Е.А. СТЕПАНОВ, И.К. КОРНЕЕВ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

ВЫСШЕЕ ОБРАЗОВАНИЕ
серия основана в 1996 г.

АННОТАЦИЯ

Е.А. СТЕПАНОВ, И.К. КОРНЕЕВ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ УЧЕБНОЕ ПОСОБИЕ

Рекомендовано в качестве учебного пособия для студентов высших учебных заведений, обучающихся по специальности «Документоведение и документационное обеспечение управления»
Москва ИНФРА-М 2001
УДК 65.012.8(075.8)
ББК 73я73
С79
С79 Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации: Учеб. пособие. — М.: ИНФРА-М, 2001. — 304 с. — (Серия «Высшее образование»).
ISBN 5-16-000491-2

В учебном пособии рассматриваются вопросы обеспечения информационной безопасности и защиты информации в офисной деятельности и предпринимательских структурах различного типа, работы, с персоналом, обладающим сведениями ограниченного распространения, функционирования защищенного документооборота и специализированной технологической системы обработки и хранения конфиденциальных документов. Излагаются вопросы защиты информации при проведении переговоров и совещании, приеме посетителей, защиты персональных данных в кадровой службе, а также направления разработки нормативно-методической документации комплексной системы защиты информации фирмы. В приложении дается терминологический справочник основных понятий в изучаемой области и главные операционные технологические схемы обработки и хранения конфиденциальных документов.
Предназначено для студентов, обучающихся по специальности «Документоведение и документационное обеспечение управления», а также студентов других специальностей, изучающих офисные технологии и работу с документами, слушателей центров, институтов и факультетов повышения квалификации, руководящих работников и специалистов, практических работников.

ББК 73я73
ISBN 5-16-000491-2

Степанов Евгений Анатольевич
Корнеев Игорь Константинович
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ОФИСЕ
Редактор Л.В. Бобылева
Корректор М. В. Литвинова
Компьютерная верстка Т. В. Доронина
Оформление серии Е.А. Доний
ЛР № 070824 от 21.01.93
Подписано в печать 20.12.2000. Формат 60x88/16. Печать офсетная. Усл. печ. л. 18,62. Тираж 6 000 экз. Заказ № 2911.
Издательский Дом «ИНФРА-М» 127214, Москва, Дмитровское ш., 107. Тел.: (095) 485-70-63; 485-71-77. Факс: (095) 485-53-18. Робофакс: (095) 485-54-44. E-mail: books@infra-m.ru http://www.infra-m.ru
Отпечатано с оригинал макета в Тульской типографии. 300600, г. Тула, пр. Ленина, 109.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Учебное пособие предназначено для всех, интересующихся вопросами практического решения проблем информационной безопасности офисной и предпринимательской деятельности. В настоящее время, несмотря на актуальность и практическую значимость этих проблем, не существует достаточно полной и современной учебной литературы в указанной области.

Цель учебного пособия — помочь в овладении теоретическими и практическими вопросами обеспечения информационной безопасности офисной деятельности в предпринимательских структурах различных типов, в том числе в малом бизнесе, и освоении системных комплексных методов защиты ценных производственных и коммерческих информационных ресурсов от различных видов угроз в процессе формирования, обработки, использования и хранения информации. Вопросы защиты информации рассматриваются в широком диапазоне современных проблем и затрагивают организационные и технологические сферы защиты как документированной информации (на бумажных и технических носителях), циркулирующей в традиционном или электронном документообороте, так и недокументированной информации.

В современной российской рыночной экономике обязательным условием успеха предпринимателя в бизнесе, получения прибыли и сохранения в целостности созданной им организационной структуры является обеспечение экономической безопасности его деятельности. Одной из главных составных частей экономической безопасности является информационная безопасность. Проблемы информационной безопасности становятся все более сложными и практически значимыми в связи с массовым переходом информационных технологий в управлении на безбумажную автоматизированную основу. Информационная безопасность носит концептуальный характер и предполагает решение комплекса задач поддержания безопасности информационных ресурсов фирмы.

Под безопасностью информационных ресурсов (информации) понимается защищенность информации во времени и пространстве от любых объективных и субъективных угроз (опасностей), возникающих в обычных условиях функционирования фирмы и условиях экстремальных ситуаций: стихийных бедствий, других неуправляемых событий, пассивных и активных попыток злоумышленника создать потенциальную или реальную угрозу несанкционированного доступа к документам, делам, базам данных. Необходимый уровень безопасности информационных ресурсов определяется в процессе различных аналитических исследований, которые предопределяют структуру и требуемую эффективность системы защиты этих ресурсов с учетом финансовых возможностей фирмы.

В решении проблемы информационной безопасности значительное место занимает построение эффективной системы организации работы с персоналом, обладающим конфиденциальной информацией. В предпринимательских структурах персонал обычно включает в себя всех сотрудников данной фирмы, в том числе и руководителей.

Персонал генерирует новые идеи, новшества, открытия и изобретения, которые продвигают научно-технический прогресс, повышают благосостояние сотрудников фирмы и являются полезными не только для фирмы в целом, но и для каждого отдельного сотрудника. Каждый сотрудник объективно заинтересован в сохранении в тайне тех новшеств, которые повышают прибыли и престиж фирмы. Несмотря на это персонал, к сожалению, является в то же время основным источником утраты (разглашения, утечки) ценной и конфиденциальной информации.

Никакая, даже самая совершенная в организационном плане и великолепно оснащенная технически система защиты информации не может соперничать с изобретательностью и хитростью человека, задумавшего украсть или уничтожить ценную информацию. Обычный секретарь руководителя фирмы имеет возможность нанести фирме такой значительный ущерб, что окажется под вопросом само ее существование. Многие специалисты по защите информации считают, что при правильной организации работы с персоналом защита информации фирмы сразу обеспечивается не менее чем, на 80%, без применения каких-либо дополнительных методов и средств защиты.

Обеспечение безопасности информации в информационных системах от случайных или преднамеренных воздействий персонала, направленных на неправомерное использование, уничтожение, модификацию тех иди иных данных, изменение степени доступности ценных сведений в машинной и внемашинной сферах предполагает наличие надежной защиты ценных для предпринимателя документов, прежде всего конфиденциальных документов. Необходимый уровень защищенности документированной информации достигается в

значительной степени за счет использования в обработке традиционных, машиночитаемых и электронных конфиденциальных документов эффективной для конкретной фирмы специализированной традиционной или автоматизированной технологической системы, позволяющей решать задачи не только документационного обеспечения управленческой и производственной деятельности, но и сохранности носителей и конфиденциальности информации.

В целях лучшего усвоения в учебное пособие включен раздел со структурированным материалом для углубленного самостоятельного изучения вопросов обеспечения информационной безопасности в офисной деятельности.

По полноте рассматриваемого материала и всестороннему освещению широкого комплекса вопросов информационной безопасности предпринимательской деятельности учебное пособие ориентировано на широкий круг читателей. Оно может быть использовано студентами вузов различного профиля, слушателями институтов и факультетов повышения квалификации, а также практическими работниками служб безопасности коммерческих структур.

1. ОРГАНИЗАЦИЯ ОФИСНОЙ ДЕЯТЕЛЬНОСТИ

1.1. Офисная деятельность как особый вид управленческой деятельности

Для определения содержания понятия «офисная деятельность» необходимо обратиться к рассмотрению категорий, так или иначе связанных с определяемым понятием. Исходным здесь является «система управления», основными образующими понятиями — «система» и «управление». При всей важности этих понятий до сих пор они не имеют общепринятых формальных определений.

Понятие «система» широко используется в научной литературе по различным отраслям знания. Каждый автор, определяя это понятие, подчеркивает ту сторону, те аспекты, которые его интересуют и которые он исследует. Тем не менее можно сформулировать ряд общих условий, которым должен удовлетворять объект, чтобы он рассматривался в качестве системы.

Прежде всего, это целостность объекта. Любое образование, любое множество объектов может быть названо системой, если его рассмотрение как целого оправдано с какой-либо точки зрения и может помочь исследователю ответить на поставленный вопрос, решить сформулированную задачу. Естественно, что временем существования такой системы является время, в течение которого ставится и решается задача. Объект, образующий систему, продолжает существовать и дальше, но в соответствии с новыми задачами изучения он будет образовывать уже другую систему. Таким образом, всегда необходимо определить **цель изучения, критерий, обусловливающий существование данного объекта как целого**. Наличие такого критерия является вторым необходимым условием рассмотрения объекта как системы.

Третье условие — рассматриваемый объект должен быть **частью, подсистемой некоторой большей системы**, что позволяет определить, с какими другими объектами и каким образом он взаимодействует. Последнее, четвертое, условие, необходимое для рассмотрения объекта как системы, — **возможность разбиения его на части, на подсистемы**. Это позволяет выяснить, какие связи и взаимодействия между составляющими объект элементами обеспечивают его единство, существование как целого.

Для иллюстрации рассмотренного подхода к определению сущности понятия «система» обратимся к объектам производственного и экономического характера.

Все известные нам производственные и экономические объекты в процессе своего функционирования выступают как целостные образования (международные и региональные экономические объединения, национальная экономика, отрасль промышленности, производственное объединение, торговая фирма, промышленное предприятие, цех, производственный участок и т.п.), с четко определенными границами (физическими, юридическими и др.).

Существование производственных и экономических объектов как целостных образований определяется прежде всего их назначением, которое заключается в конечном счете в удовлетворении материальных потребностей общества, причем для каждого конкретного объекта определены конкретные виды производимой продукции и оказываемых услуг.

Каждый производственный и экономический объект входит в качестве элемента в другую систему экономического и производственного характера, что определяет состав и виды

его взаимодействий с окружающей средой, среди которых можно выделить материальные, энергетические, информационные и т.п.

В свою очередь, каждый производственный и экономический объект состоит из множества различных элементов, взаимодействие которых и обеспечивает его существование и выполнение им своего назначения в рамках общества.

Таким образом, выполняются все перечисленные условия рассмотрения объекта как системы. Следовательно, все производственные и экономические объекты являются системами.

Понятие «управление», так же как и понятие «система», до сих пор не имеет общепринятого определения, тем не менее, в большинстве случаев можно выделить процессы управления. Если проанализировать все случаи, выяснится, что процессы управления связаны с изменениями, происходящими в системе в результате ее взаимодействия с окружающей средой. Поскольку всякая реальная система является открытой, т.е. взаимодействует с внешней средой, в ней происходят изменения, которые могут иметь две крайние, противоположные друг другу формы — это деградация (разрушение системы) и развитие (усложнение системы, накопление ею информации). Вместе с тем возможно и временное равновесие между системой и средой, благодаря которому система в течение известного времени либо остается относительно неизменной, либо испытывает лишь обратимые изменения, не нарушающие ее целостности. Количественной характеристикой организованности системы является энтропия, большее значение которой соответствует меньшему уровню сложности и организации системы. Для сохранения целостности системы необходимы процессы, препятствующие увеличению энтропии. Это и есть процессы управления, общим для которых является их антиэнтропийный характер. В этой связи процесс управления по своей сути является антиподом процессу дезорганизации. Он позволяет в зависимости от особенностей конкретных систем стабилизировать систему, сохранить ее качественную определенность, поддержать ее динамическое равновесие со средой, обеспечить совершенствование системы и достижение того или иного полезного эффекта. Короче говоря, **управление — это поддержание энтропии системы на неизменном уровне.**

Как уже отмечалось, любая реальная система взаимодействует с внешней средой, в результате чего в ней происходят изменения различного рода, выражающиеся в протекании некоторого процесса. Этот процесс изменения системы и вызывает необходимость управления. Таким образом, **в основе любой системы управления лежит процесс, требующий управления.**

Однако не всякое протекание процесса требует управления, а лишь то, которое ведет к увеличению энтропии. Поэтому необходимо связать характер изменений, лежащих в основе процесса, с критерием качества системы, т.е. нужно определить цель управления. В этом смысле **системы управления обладают целенаправленностью.**

Далее, поскольку осуществление процессов управления выделяется в обособленную функцию, то на ее выполнении специализируются некоторые элементы системы. В этой связи **системы управления обладают определенной структурой**, а именно — состоят из **управляемого процесса и управляющей части.** Данное положение принципиально, поскольку существуют объекты, которые сохраняют свою качественную определенность и без явно выраженной управляющей компоненты. Как правило, это достаточно простые физические объекты (камень, стул и т.п.), которые в дальнейшем нами рассматриваться не будут.

Управляющая часть воздействует на управляемый процесс, чтобы в соответствии с целью управления обеспечить сохранение качественной определенности всей системы. Чтобы управляющая часть могла осуществлять управление, ей нужно сопоставлять фактическое состояние управляемого процесса с целью управления, таким образом и управляемый процесс воздействует на управляющую часть. Воздействие обеих частей структуры друг на друга осуществляется в виде передачи информации, поэтому **в системе управления всегда присутствует замкнутый информационный контур** (рис. 1).

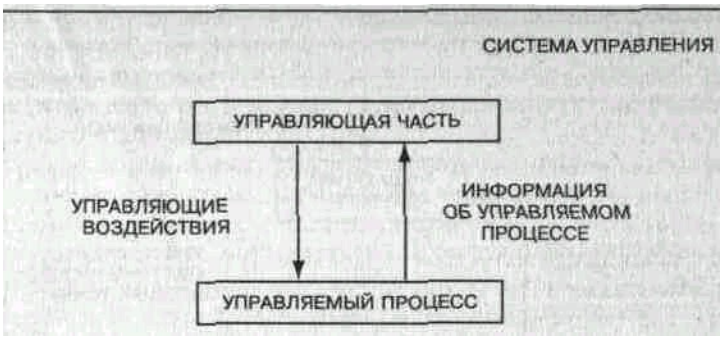

Рис. 1

Представленная на рис. 1 схема носит общий характер и справедлива для любой системы управления.

Управляющая часть, в свою очередь, включает ряд элементов:

- измерительные;
- исполнительные;
- решающие.

Каждый из них выполняет определенную функцию в реализации процесса управления, и между собой они связаны информационными связями. Эти элементы связаны между собой и с внешней средой посредством передачи информации:

- о целях управления;
- о состоянии управляемого процесса;
- об управляющих воздействиях.

На рис. 2 представлена схема системы управления с учетом состава элементов управляющей части.

Управляемый процесс может иметь довольно сложную структуру, обусловливаемую конкретными особенностями его протекания, и состоять из подпроцессов, относительно автономных и различным образом взаимодействующих друг с другом. Автономность подпроцессов выражается в их определенной локализации во времени и пространстве, в наличии собственных критериев качества функционирования и определяет, таким образом, собственные управляющие части.

Сложная конфигурация управляемого процесса порождает и соответствующее усложнение управляющей части системы управления, приводя к появлению дополнительных координирующих элементов, зачастую нескольких уровней. Можно говорить об относительной самостоятельности управляющей части уже со своими

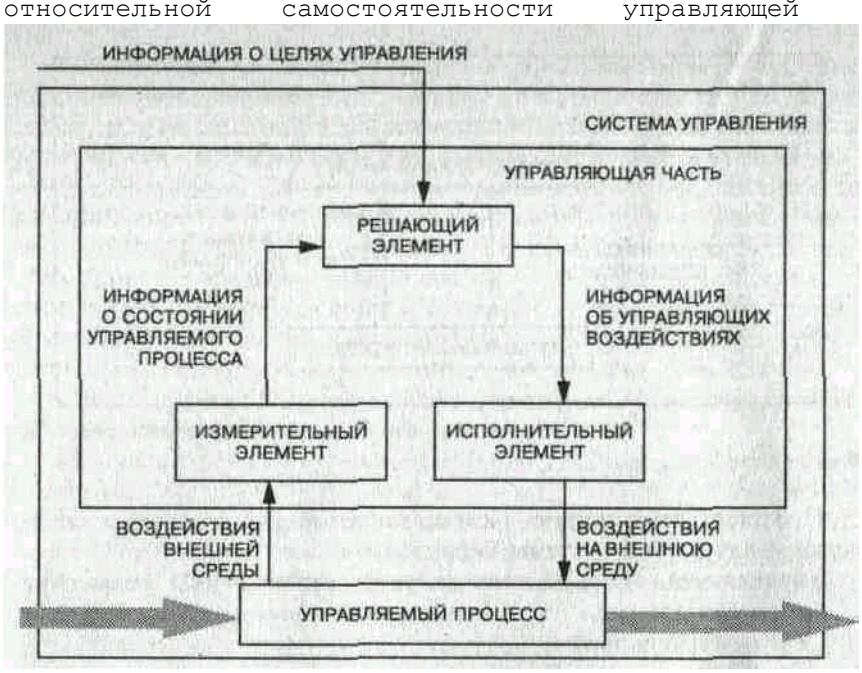

Рис. 2

критериями функционирования, сложной структурой, принципами и законами внутреннего

существования, т.е. речь идет скорее об управляющей системе. А это означает, что функционирование такой системы определяет соответствующий и отличный от других (порождаемых управляемым процессом) специфический вид деятельности — **управленческую деятельность.**

Исходя из рассмотренных положений можно определить управленческую деятельность как определенным образом организованную в пространстве и времени совокупность действий множества людей (персонала), реализация которых в рамках управляющей системы обеспечивает реализацию функций управляемого процесса, а следовательно, и достижение целей системы управления в целом.

Данное определение предполагает наличие следующих характеристик управленческой деятельности:

• управленческая деятельность осуществляется в течение определенного временного интервала (времени существования системы управления);

• управленческая деятельность осуществляется в определенных пространственных границах, как правило, определяемых местом размещения управляющей системы;

• управленческая деятельность реализуется людьми, для которых она является основным видом деятельности;

• содержание управленческой деятельности определяется задачами, решение которых приводит к негэнтропийному протеканию управляемого процесса.

Проблемы организации управленческой деятельности во многом сводятся к проблемам выработки и реализации управленческих решений, связанных с непосредственным воздействием на управляемый процесс. Соответствующие теоретико-методологические и практические разработки велись и ведутся именно в указанной области. Но, имея в виду сложность самой управляющей системы, ее относительно самостоятельное существование, наличие внутренних, порой противоречивых особенностей реализации различных функций, необходимо указать и на необходимость управления самой управленческой деятельностью, которое является особой ее разновидностью.

Как уже отмечалось, управленческая деятельность в том смысле, в котором мы ее определили, пространственно локализована рамками физического размещения управляющей системы. Указанное физическое размещение в различное время и в различных местах реализовывалось по-разному: приказы в Древней Руси, коллегии в Петровской России, министерства и ведомства в современном обществе, заводоуправления на промышленных предприятиях, деканаты на факультетах высших учебных заведений и т.п. Для обозначения указанных объектов в настоящее время существует обобщенное название — **офис.** В соответствии с изложенными выше представлениями о системах управления под **офисом** понимается физическая реализация условий выполнения управленческой деятельности в рамках управляющей системы, а обеспечение его функционирования, т.е. управление самой управленческой деятельностью — **офисной деятельностью.**

1.2. Структура и функции офисной деятельности

Исходя из того, что для достаточно сложных управляемых процессов (а к таковым относятся социальные и экономические процессы и явления) управляющая часть рассматривается как управляющая система, ее саму следует принимать за систему правления, в которой управляемым процессом является реализуемая в рамках офиса управленческая деятельность. И тогда, как следует из предыдущего рассмотрения, **офисная деятельность** — это определенным образом организованная в пространстве и времени совокупность действий множества людей (персонала), реализация которых обеспечивает условия эффективного выполнения управленческой деятельности для конкретной системы управления.

Это определение предполагает наличие следующих структурных характеристик офисной деятельности:

• офисная деятельность осуществляется в пространственных границах, определяемых совокупностью параметров размещения офиса:
количеством мест локализации (одно или несколько), их иерархической соподчиненностью (центральный или филиал) и прочими показателями функционирования офиса в пространстве;

• офисная деятельность осуществляется в течение определенного временного интервала, т.е. обладает совокупностью временных параметров: моментами начала и окончания осуществления, чередованием периодов с различными интенсивностями своей реализации, прочими показателями функционирования офиса во времени;

• офисная деятельность реализуется людьми, для которых она полностью или частично является основным видом деятельности, что характеризуется составом соответствующего персонала, его квалификацией и стажем, распределением прав и обязанностей и т.п.;
• содержание офисной деятельности определяется задачами обеспечения условий для эффективной реализации управленческой деятельности — управляемого по отношению к офисной деятельности процесса.

Раскрытие перечисленных характеристик офисной деятельности необходимо осуществить прежде всего через содержание управленческой деятельности, которая в существенной своей части сводится к выработке и принятию управленческих решений.

Категория «управленческое решение» имеет многоаспектное содержание. В широком смысле термин «управленческое решение» можно понимать как концентрированное выражение процесса управления на его заключительной стадии, как команду, подлежащую выполнению, поступающую от управляющей части системы к управляемому процессу. Отметим три связанных между собой содержательных проявления управленческого решения(СМ.Сноску *):
• во-первых, управленческое решение — это вид деятельности, протекающий в управляющей части системы и связанный с подготовкой, нахождением, выбором и принятием определенных вариантов действий;
• во-вторых, управленческое решение — это вариант воздействия управляющей части системы на управляемый процесс, формула воздействия, т.е. описание предполагаемых действий управ-

___
Сноска *. * См. Теория управления социалистическим производством: Учебник / Под ред. О.В.Козловой. - М.: Экономика, 1979.

___
ляющей части системы по отношению к объекту управления (управляемому процессу);
• в-третьих, управленческое решение — это организационно-практическая деятельность по реализации выбранного воздействия.

Первое проявление управленческого решения отражает в основном сущность управленческой деятельности, второе — ее результат, а третье — обеспечение эффективной реализации этого результата, т.е. определенным образом обусловливает содержание офисной деятельности.

Управленческое решение принимается тогда, когда выявлена та или иная управленческая проблема, проблемная ситуация, т.е. когда при наличии данного, существующего состояния управляемого объекта (процесса) возникает необходимость другого, поскольку сохранение данного состояния мешает нормальному его функционированию, совершенствованию и развитию(СМ.Сноску *).

Выявив проблему, важно всесторонне ее исследовать, получить ответы на следующие вопросы:
• каковы причины и условия ее возникновения;
• какова ее важность, значимость;
• какой характер решения необходим в данной проблемной ситуации;
• каковы ее возможные последствия;
• каково отношение к проблеме людей;
• где может быть принято решение (в данной системе или вне ее);
• есть ли ресурсы для решения проблемы;
• кто из людей способен к решению;
• какая информация необходима и т.д.

При подготовке решения необходимо также выявить и учесть ограничения, в рамках которых будет реализовываться цель, решаться задача. Эти ограничения могут быть внутренними (для предприятия, например, это производительность оборудования, наличие и квалификация специалистов и рабочих, наличие информации и т.д.) и внешними (сроки решения задачи, финансы, технические нормы, плановые показатели, отлаженность связей с поставщиками и т.д.).

Процесс подготовки и выработки решений сложен, он включает в себя ряд этапов и стадий, которые связаны с выполнением различных действий, операций, со специфическими формами управленческой деятельности.

Вопрос о том, сколько и каких стадий имеется в процессе подготовки и принятия решений, каково конкретное содержание

___
Сноска *. * См. Оптнер С.Л. Системный анализ для решения деловых и промышленных проблем. - М.: Советское радио, 1969.

___
управленческой деятельности на этих стадиях, — спорный и неодинаково решаемый различными исследователями и специалистами(СМ.Сноску *).
Однако ясно одно: сколько бы этапов ни выделялось, основным, исходным в подготовке решений является процесс сбора и переработки информации о состоянии системы и окружающей ее среды. В процессе переработки информации, ее анализа и обобщения выявляется сущность данной управленческой ситуации. Ситуация сопоставляется с целью, стоящей перед системой, а расхождение между реальным положением вещей и целью позволяет определить проблему, ради которой принимается решение. В дальнейшем этот процесс предполагает тщательный анализ проблемы, постановку задач и целей, точную формулировку проблемы, разработку и оценку альтернатив, выявление и оценку возможных последствий, разработку плана реализации решения, выбор людей, путей и средств реализации. В достаточно общем виде процесс выработки и принятия решений может быть структурирован так, как это представлено на рис.3.

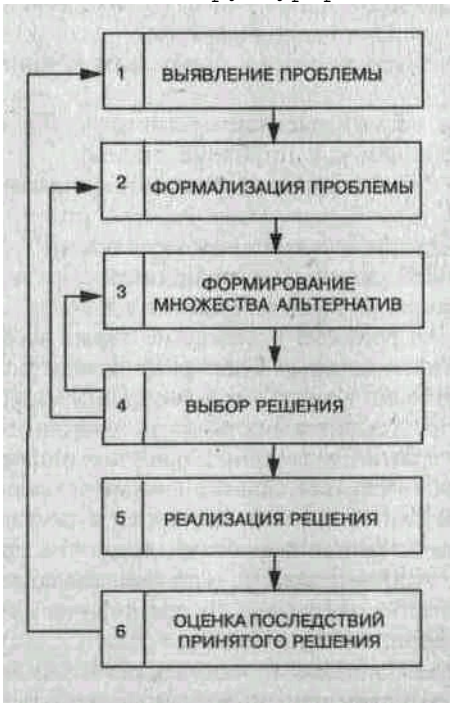

Рис. 3

___
Сноска *. Сравнительный анализ различных вариантов дан в работе: Афанасьев В.Г. Человек в управлении обществом. -.М.: Политиздат, 1977.

___
Рассмотрим содержание отдельных этапов процесса выработки и принятия управленческих решений.
На первом этапе (выявление проблемы) на основании сопоставления фактического и желаемого (или заданного) состояний управляемого объекта определяется необходимость оказания на него управляющих воздействий, порождающая соответствующую управленческую проблему. Конкретное содержание деятельности на этом этапе определяется постановкой задачи принятия решений, в которой должны быть сформулированы ответы на следующие вопросы:
• какую управленческую проблему нужно решить;
• в каких условиях нужно решить;
• когда ее нужно решать;
• какими силами и средствами будет решаться проблема.
Результатом здесь, как правило, является содержательное описание проблемной ситуации.

На втором этапе (формализация проблемы) производится анализ проблемной ситуации, в ходе которого конкретизируются:

• цели, достигаемые при решении проблемы;
• ограничения при реализации действий по устранению проблемной ситуации;
• возможные методы и средства решения задачи.

Это означает, что поставленная содержательно управленческая задача как некоторая проблемная ситуация на данном этапе приводится к некоторому структурированному виду, позволяющему с некоторой определенностью либо применить для решения задачи уже известные методы, либо осуществить поиск или разработку новых методов.

На третьем этапе (формирование множества альтернатив) на основе структуризованной задачи принятия решений и применения определенных методов ее анализа и обработки формируют различные варианты решения задачи. Следует отметить, что даже единственный выработанный вариант управленческого решения не является таковым, так как он имеет альтернативу — отсутствие каких либо воздействий на управляемый объект.

На четвертом этапе (выбор решения) на основе определенных правил (предпочтений) из ранее сформированного множества вариантов выбирается один единственный, который и воплощается в виде управленческого решения. При оценке различных вариантов решений — необходимой основы выбора — может возникнуть необходимость корректировки как множества альтернатив, так и структуризации (формализации) самой задачи принятия решений, что приведет к возврату на соответствующие этапы процесса выработки и принятия решений.

Описанные этапы осуществляются в рамках решающего элемента управляющей системы.

На пятом этапе выполнение принятого управленческого решения возложено на исполнительный элемент.

На шестом этапе оценка состояния управляемого объекта как результата реализации решения возложена на измерительный элемент.

Сопоставляя содержание понятия «управленческое решение» и отдельных этапов процесса его выработки и принятия можно прийти к выводу, что для эффективного управления необходимы соответствующее информационное обеспечение (поиск, сбор, хранение и представление информации на различных этапах) и соответствующим образом организованные процедуры реализации управленческого решения. Именно это и составляет основное содержание офисной деятельности.

Теперь перейдем к рассмотрению перечисленных структурных компонентов офисной деятельности (пространственные, временные и кадровые характеристики).

Поскольку характеристики управляемого процесса существенным образом определяют свойства управляющей системы, а следовательно, и характер протекания офисной деятельности, имеет смысл рассмотреть его возможные конфигурации.

1. Управляемый процесс характеризуется относительной простотой и целостностью, т.е. не разбивается на такие подпроцессы, которые требуют отдельных управляющих частей (обработка деталей на отдельном производственном участке цеха машиностроительного предприятия, строительство жилого дома, лечебный процесс в стоматологическом кабинете и т.п.) — **элементарный управляемый процесс.**

2. Управляемый процесс состоит из небольшого количества взаимодействующих однородных подпроцессов, локализованных на относительно ограниченном пространстве и имеющих собственные управляющие части (производственный процесс в цехе машиностроительного предприятия, учебный процесс на факультете высшего учебного заведения, эксплуатация жилых домов на территории одного домоуправления и т.п.) **— локализованный управляемый процесс с однородными элементами.**

3. Управляемый процесс состоит из взаимодействующих разнородных подпроцессов, локализованных на относительно ограниченном пространстве и имеющих собственные управляющие части (производство разнообразной продукции на промышленном предприятии с различными производственными цехами и обеспечивающими службами, лечебные процесс в клинической больнице, постановочный процесс в театре и т.п.) **— локализованный управляемый процесс с разнородными элементами.**

4. Управляемый процесс состоит из относительно автономных однородных подпроцессов, распределенных в пространстве и имеющих собственные управляющие части (торговля в сети магазинов, учебный процесс в многофилиальном институте заочного образования и т.п.) — **распределенный управляемый процесс с однородными элементами.**

5. Управляемый процесс состоит из относительно автономных разнородных подпроцессов, распределенных в пространстве и имеющих собственные управляющие части (производство разнообразной продукции в рамках производственного объединения, производство одного вида продукции в рамках объединения специализированных предприятий, городское хозяйство и т.п.) — **распределенный управляемый процесс с разнородными элементами.**
6. Управляемый процесс со сложной структурой и имеющий глобальный характер (производственная деятельность межнациональных корпораций, деятельность органов государственного управления и т.п.) — **глобальный управляемый процесс.**
Пространственные характеристики офисной деятельности существенным образом определяются содержанием, масштабами и характером протекания процесса, являющегося управляемым по отношению к той управляющей системе, деятельность которой обеспечивается, и практически совпадают с аналогичными характеристиками управленческой деятельности.
Для элементарных управляемых процессов управляющая часть пространственно реализуется в виде относительно изолированного, рабочего места непосредственно в рамках управляемого процесса (например, конторка мастера на производственном участке машиностроительного завода или вагончик прораба на строительстве какого-либо объекта).
Для локализованных управляемых процессов с однородными элементами управляющая часть имеет по меньшей мере двухуровневую структуру, где на нижнем уровне представлены независимые друг от друга управляющие части элементарных однородных подпроцессов, а на верхнем — координирующая их работу управляющая подсистема, обеспечивающая целенаправленное функционирование управляемого процесса в целом. Так, управленческая деятельность для цеха машиностроительного завода организована в рамках нескольких функционально ориентированных бюро, размещенных рядом с производственными участками, но изолированных от них.
Для локализованных управляемых процессов с разнородными элементами управляющая часть (или скорее система) также может иметь двухуровневую структуру, но в отличие от предыдущего случая на нижнем уровне разнородные управляемые подпроцессы имеют различные управляющие части, что порождает более сложную по своему строению управляющую систему на верхнем уровне. Пример — управляющая система на крупном машиностроительном предприятии, включающая в себя заводоуправление достаточно сложной структуры и службы управления цехами и производствами, которые в свою очередь стоят над элементарными управляемыми процессами с их управляющими частями (что позволяет говорить скорее не о двух-, а о трехуровневой системе).
Распределенные управляемые процессы с однородными элементами с точки зрения функциональной структуры имеют то же строение управляющей части, что и аналогичные локализованные управляемые процессы, но пространственная распределенность предполагает большую автономию управляющих частей однородных подпроцессов от управляющей системы верхнего уровня, которая существует и функционирует уже практически вне управляемого процесса в целом, как это имеет место, например, в сети продажи автомобильного топлива, где помимо бензоколонок в различных районах города имеется центральная контора, осуществляющая общее руководство.
Похожую структуру управляющей системы имеют распределенные управляемые процессы с разнородными элементами, но здесь именно разнородность подпроцессов порождает очень высокую степень автономности соответствующих управляющих частей, что приводит к еще более сложной структуре управляющих компонентов верхнего уровня, к появлению в них нескольких подуровней управления, что характерно для крупных региональных (например, городских или областных) служб коммунального хозяйства или войсковых организаций типа военных округов.
Предельный уровень сложности имеют глобальные управляемые процессы, порождающие соответствующие управляющие системы с зачастую уникальными структурами, например органы государственного управления в различных странах или аппарат управления разных международных организаций.
В пространственной организации управленческая и офисная деятельность имеют идентичные характеристики, поскольку в этом отношении они объективно неразделимы. Так же, как и пространственные характеристики, временные параметры офисной деятельности в значительной степени определяются организацией управляемого процесса во времени (в дальнейшем рассмотрении мы будем опираться на уже приведенную

классификацию управляемых процессов). Элементарные управляемые процессы с точки зрения их организации во времени существенным образом подразделяются на две категорий: с непрерывным и дискретным функционированием.

Непрерывные управляемые процессы требуют и непрерывного управления, т.е. управленческая деятельность, связанная с ними, должна осуществляться постоянно. К такого рода процессам относятся производства в химической, металлургической, энергетической отраслях промышленности. В данном случае определить временные характеристики управленческой деятельности можно следующим образом: управленческая деятельность осуществляется с относительно неизменной интенсивностью в течение всего периода функционирования управляемого процесса без перерывов.

Дискретные управляемые процессы функционируют в течение четко выделенных временных интервалов с определенными моментами начала и окончания, что позволяет осуществлять управление ими не непрерывно, а в рамках упомянутых интервалов. При этом в различных интервалах интенсивность управленческой деятельности может быть различной (пример — работа производственного участка машиностроительного цеха в дневную и ночную смены). Поэтому здесь временные характеристики управленческой деятельности можно определить следующим образом; управленческая деятельность осуществляется в рамках явно выраженных интервалов времени с четко определенными моментами начала и окончания, причем в различных интервалах ее интенсивность различна (включая и нулевую), а вся последовательность этих интервалов укладывается в общую длительность функционирования управляемого процесса.

Что касается более сложных видов управляемых процессов, то они представляют собой различные комбинации элементарных процессов, порождая те или иные уже рассмотренные конструкции управляющих систем, что в зависимости от типа подпроцессов (непрерывных или дискретных) создает и соответствующие наборы временных характеристик управленческой деятельности. Следует отметить, что по объективным причинам преобладают характеристики, связанные с дискретными процессами.

Временные характеристики офисной деятельности, так же как и ее пространственные параметры, неразрывно связаны с характеристиками управленческой деятельности, но полной идентичности здесь не наблюдается, особенно для дискретных процессов. В рамках отдельных интервалов функционирования управленческая и офисная деятельность могут иметь разную интенсивность, что порождает различную их временную структуру при идентичной пространственной организации. Например, в ночное время подавляющее большинство служб управления городского хозяйства не функционирует (а следовательно, имеют практически нулевую интенсивность в смысле офисной деятельности), но их дежурные подразделения осуществляют оперативную работу, определяя ненулевую интенсивность собственно управленческой деятельности, оставляя многие (неоперативные) решения и их оформление на дневное время с ненулевой интенсивностью офисной деятельности.

Кадровые характеристики офисной деятельности определяются свойствами персонала, ее осуществляющего. Здесь можно выделить следующие параметры:

- количество специалистов;
- состав специалистов;
- уровень специализации;
- уровень квалификации;
- стаж работы;
- общие параметры, характеризующие работу с кадрами. Количество специалистов, осуществляющих офисную деятельность, полностью определяется объемом и масштабами управленческой деятельности, которая, в свою очередь, зависит от сложности управляемого процесса. По мере перехода от элементарных управляемых процессов к глобальным с повышением уровня сложности управляющих систем число таких специалистов увеличивается, с необходимостью ставя задачи специализации, кооперации и определения необходимой квалификации при осуществлении офисной деятельности.

Состав специалистов, выполняющих задачи в рамках офисной деятельности, определяется необходимым ее объемом в конкретных пространственных и временных конфигурациях управленческой деятельности соответствующими нормативными документами (квалификационными справочниками) и может включать в себя как собственно управленческий персонал (лиц, принимающих и готовящих решения), так и персонал, обеспечивающий информационную и организационную поддержку процесса выработки и

принятия решения.
Определение состава специалистов тесно связано с уровнем их специализации на офисной деятельности. Так, собственно управленческий персонал может полностью осуществлять управленческую и офисную деятельность (как это имеет место для элементарных управляемых процессов, где указанный персонал воплощается в одном человеке — мастер, бригадир и т.п.), может быть полностью освобожден от офисной деятельности (менеджеры высшего уровня и государственные руководители), может наряду с основной (управленческой) деятельностью выполнять некоторые задачи офисной деятельности. В двух последних случаях необходимы специалисты, для которых осуществление офисной деятельности является основной работой. Это секретари, помощники, референты, офис-менеджеры, специалисты по информационному обеспечению и т.п.
Квалификация офисного персонала определяется прежде всего наличием соответствующей профессиональной подготовки. Эта подготовка может иметь различные формы:
• получение среднего специального образования (секретари-референты; техники, осуществляющие эксплуатацию различных информационных систем, и т.п.);
• получение высшего образования (референты; руководители служб документационного и информационного обеспечения; инженеры, осуществляющие эксплуатацию различных информационных систем, и т.п.);
• подготовка и переподготовка на различных краткосрочных курсах (секретари; персонал служб документационного и информационного обеспечения и т.п.).
Кроме того, фактическая квалификация, помимо уровня профессиональной подготовки, существенным образом зависит от стажа офисной работы, что определяет знание конкретной обстановки и практические навыки обеспечения конкретной управленческой деятельности.

1.3. Проблемы организации офисной деятельности

Рассмотрение структуры и функций офисной деятельности указывает на наличие существенно разнородных и довольно многочисленных, но взаимосвязанных компонентов и процессов. Эффективная реализация офисной деятельности предполагает обеспечение функционирования этих компонентов и процессов как таковых, так и их совокупности. Такая задача, в общем, достаточно распространена (по крайней мере в рамках системного подхода) и содержательно связана с понятием «организация».
Отметим, в частности, что понятие «организация» имеет такой же многозначный характер, как и понятия «система» и «управление», рассмотренные выше. Наиболее полным, на наш взгляд, является определение, данное в Советском энциклопедическом словаре (1986):
«ОРГАНИЗАЦИЯ (франц. organisation, от позднелат. organize — сообщаю стройный вид, устраиваю), 1) внутренняя упорядоченность, согласованность, взаимодействие более или менее дифференцированных и автономных частей целого, обусловленные его строением. 2) Совокупность процессов или действий, ведущих к образованию и совершенствованию взаимосвязей между частями целого.
3) Объединение людей, совместно реализующих программу или цель и действующих на основе определенных правил и процедур.
Применяется к биологическим, социальным и некоторым техническим объектам, фиксируя динамические закономерности, т.е. относящиеся к функционированию, поведению и взаимодействию частей; обычно соотносится с понятиями структуры, системы, управления».
Возникает вопрос, какое из приведенных значений является первичным, определяющим. На наш взгляд, таковым является второе (организация как деятельность), в то время как первое определяет организацию как результат определенного рода деятельности (а именно в смысле второго значения). Что касается третьего значения, то оно лишь подчеркивает первичность второго в том смысле, что определяет форму существования и функционирования группы людей по реализации организации в смысле деятельности.
Организация как деятельность предполагает:
• определение цели, задачи (или задач);
• разработку системы мероприятий для реализации цели и разделения задачи на отдельные виды работ;
• интеграцию отдельных работ в соответствующих подразделениях, которые могли бы их координировать различными средствами, включая и формальную иерархическую структуру;

• мотивацию, взаимодействие, поведение, взгляды персонала, которые отчасти определяются мероприятиями, направленными на реализацию поставленных целей, а отчасти носят личный, случайный характер; • принятие решений, коммуникации, информационные потоки, контроль, поощрение и наказание, имеющие решающее значение для обеспечения выполнения поставленных целей;
• единую организационную систему, которая понимается не как особый, дополнительный признак, а как внутренняя согласованность, которая должна быть достигнута между всеми перечисленными элементами. Представленное раскрытие содержания организации как деятельности весьма широко и неявно содержит компоненты организации как результата деятельности. Поэтому необходима определенная конкретизация с точки зрения организации офисной деятельности.

Цели, задачи офисной деятельности определяются ее содержанием как процесса, обеспечивающего эффективную реализацию управленческой деятельности в рамках конкретной системы управления. Как было показано выше, в основном это информационное обеспечение управленческой деятельности и реализации принятых решений.

Разработка системы мероприятий для реализации цели и разделения задач на отдельные виды работ применительно к только что определенным целям и задачам офисной деятельности предполагает определение всего состава конкретных функций информационного обслуживания управленческой деятельности в рамках ее конкретных пространственных и временных характеристик, выделения соответствующих задач, работ, процедур и операций с учетом последовательности их выполнения и взаимосвязей.

Интеграция отдельных работ в соответствующих подразделениях осуществляется с учетом прежде всего пространственных характеристик управленческой деятельности и предполагает распределение выявленной совокупности задач, работ, процедур и операций по соответствующим пространственным компонентам (структурным подразделениям) с последующей их концентрацией и интеграцией с целью эффективной реализации.

Мотивация, взаимодействие, поведение, взгляды персонала определяются в соответствии с кадровыми характеристиками требуемой офисной деятельности и во многом зависят от необходимой квалификационной поддержки выявленного состава задач, работ, процедур и операций информационного обслуживания управленческой деятельности.

Принятие решений, коммуникации, информационные потоки, контроль, поощрение и наказание — эта составляющая, на первый взгляд, относится к собственно процессу принятия управленческих решений для воздействия на управляемый процесс, но поскольку мы приняли положение о том, что офисная деятельность есть во многом процесс управления управленческой деятельностью, то перечисленные элементы организации должны иметь место и разрабатываться соответствующим образом.

Единая организационная система офисной деятельности предполагает сведение воедино всех перечисленных компонентов ее организации в рамках функционирования офиса во всех его проявлениях.

2. ОСНОВНЫЕ НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ

2.1. Информационные ресурсы и конфиденциальность информации

В соответствии с действующим Федеральным законом «Об информации, информатизации и защите информации» от 25.01.95 информационные ресурсы предприятия, организации, учреждения, банка, компании и других государственных и негосударственных предпринимательских структур (далее по тексту — фирмы) включают в себя отдельные документы и отдельные массивы документов (дела), документы и комплексы документов в информационных системах (библиотеках, архивах, фондах, банках данных компьютеров и других информационных системах) на любых носителях, в том числе обеспечивающих работу вычислительной и организационной техники.

Информационные ресурсы (информация) являются объектами отношений физических и юридических лиц между собой и с государством. В совокупности они составляют информационные ресурсы России и защищаются законом наряду с другими видами ресурсов. Документирование информации (создание официального документа) является обязательным условием включения информации в информационные ресурсы. Следует учитывать, что документ может быть не только и даже не столько управленческим

(деловым), имеющим в большинстве случаев текстовую, табличную или анкетную форму. Значительно большие объемы наиболее ценных документов представлены в изобразительной форме: конструкторские документы, картографические, научно-технические, документы на фотографических, магнитных и иных носителях.

По принадлежности к тому или иному виду собственности информационные ресурсы могут быть государственными или негосударственными и как элемент состава имущества находиться в собственности граждан, органов государственной власти, исполнительных органов, органов местного самоуправления, государственных учреждений, организаций и предприятий, общественных объединений, предпринимательских структур.

В соответствии с интересами обеспечения национальной безопасности и степенью ценности для государства, а также правовыми, экономическими и другими интересами предпринимательских структур информационные ресурсы могут быть: а) открытыми, т.е. общедоступными, используемыми в работе без специального разрешения, публикуемыми в средствах массовой информации, оглашаемыми на конференциях, в выступлениях и интервью; б) ограниченного доступа и использования, т.е. содержащими сведения, составляющие тот или иной вид тайны и подлежащие защите, охране, наблюдению и контролю.

Запрещается относить к информации ограниченного доступа:

• законодательные и другие нормативные акты, устанавливающие правовой статус органов государственной власти, исполнительных органов, органов местного самоуправления, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;

• документы, содержащие информацию о чрезвычайных ситуациях, экологическую, метеорологическую, демографическую, санитарно-эпидемиологическую и другую информацию, необходимую для обеспечения безопасного функционирования населенных пунктов, производственных объектов, безопасности граждан и населения в целом;

• документы, содержащие информацию о деятельности органов государственной власти, исполнительных органов и органов местного самоуправления, об использовании бюджетных средств и других государственных и местных ресурсов, о состоянии экономики и потребностях населения, **за** исключением сведений, относящихся к государственной тайне;

• документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах органов государственной власти, исполнительных органов, органов местного самоуправления, организаций, общественных объединений, представляющие общественный интерес или необходимые для реализации прав, свобод и обязанностей граждан.

Накопители информационных ресурсов называются источниками (обладателями) информации. Они представляют собой пассивные концентраторы этой информации и включают в себя:

• публикации о фирме и ее разработках;

• рекламные издания, выставочные материалы, документацию;

• персонал фирмы и окружающих фирму людей;

• физические поля, волны, излучения, сопровождающие работу вычислительной и другой офисной техники, различных приборов и средств связи.

Источники содержат информацию как открытого, так и ограниченного доступа. Причем информация того и другого рода находится в едином информационном пространстве и разделить ее без тщательного содержательного анализа часто не представляется возможным. Например, систематизированная совокупность открытой информации может в комплексе содержать сведения ограниченного доступа.

Документация как источник информации ограниченного доступа включает:

• документацию, содержащую ценные сведения, ноу-хау;

• комплексы обычной деловой и научно-технической документации, содержащей общеизвестные сведения, организационно-правовые и распорядительные документы;

• рабочие записи сотрудников, их служебные дневники, личные рабочие планы, переписку по производственным вопросам;

• личные архивы сотрудников фирмы.

В каждой из указанных групп могут быть:

• документы на традиционных бумажных носителях (листах бумаги, ватмане, фотобумаге и т.п.);

• документы на технических носителях (магнитных, фотопленочных и т.п.);

• электронные документы, банки электронных документов,
изображения документов на экране дисплея (видеограммы). При выполнении управленческих и производственных действий любая информация источника всегда распространяется во внешней среде. Тем самым увеличивается число опасных источников разглашения или утечки информации ограниченного доступа, источников, подлежащих учету и контролю.
Каналы распространения информации носят объективный характер, отличаются активностью и включают в себя:
• деловые, управленческие, торговые, научные и другие коммуникативные регламентированные связи;
• информационные сети;
• естественные технические каналы излучения, создания фона. Канал распространения информации представляет собой путь перемещения сведений из одного источника в другой в санкционированном (разрешенном, законном) режиме или в силу объективных закономерностей. Например: обсуждение важного вопроса на закрытом совещании, запись на бумаге содержания изобретения, переговоры с потенциальным партнером, работа на ЭВМ и т.д.
Следовательно, информационные ресурсы фирмы представляют собой динамичную категорию, что проявляется прежде всего в процессе документирования информации, объективном возникновении и расширении состава источников и каналов ее распространения.
Документированные информационные ресурсы, которые используются предпринимателем в бизнесе и управлении фирмой, являются его собственной или частной информацией, представляющей для него значительную ценность. Эта информация составляет интеллектуальную собственность предпринимателя.
Ценность информации может быть стоимостной категорией и характеризовать конкретный размер прибыли при ее использовании или размер убытков при ее утрате. Информация часто становится ценной ввиду ее правового значения для фирмы или развития бизнеса, например: учредительные документы, программы и планы, договоры с партнерами и посредниками и т.д. Ценность может проявляться в ее перспективном научном, техническом или технологическом значении.
Обычно выделяется два вида информации, интеллектуально ценной для предпринимателя:
• **техническая, технологическая:** методы изготовления продукции, программное обеспечение, производственные показатели, химические формулы, рецептуры, результаты испытаний опытных образцов, данные контроля качества и т.п.;
• **деловая:** стоимостные показатели, результаты исследования рынка, списки клиентов, экономические прогнозы, стратегия действий на рынке и т.п.
Ценная информация охраняется нормами права (патентного, авторского, смежных прав и др.), товарным знаком или защищается включением ее в категорию информации, составляющей тайну фирмы.
Процесс выявления и регламентации реального состава ценной информации, составляющей тайну фирмы, является основополагающей частью системы защиты информации. Состав этих сведений фиксируется в специальном **перечне**, закрепляющем факт отнесения их к защищаемой информации и определяющем период (срок) конфиденциальности (т.е. недоступности для всех) этих сведений, уровень (гриф) их конфиденциальности, список сотрудников фирмы, которым дано право использовать эти сведения в работе. В основе перечня лежит типовой состав защищаемых сведений фирм данного профиля. Перечень является постоянным рабочим материалом руководства фирмы, служб безопасности и конфиденциальной документации. Он представляет собой классифицированный список типовой и конкретной ценной информации о проводимых работах, производимой продукции, научных и деловых идеях, технологических новшествах. В перечень включаются действительно ценные сведения («изюминки») о каждой работе фирмы. Следует отметить, что нельзя ограничивать доступ к информации, относящейся к новой продукции, но не имеющей ценности.
Дополнительно может составляться **перечень документов**, в которых защищаемая информация отражается (документируется). В перечень включаются также документы, не содержащие указанную информацию, но представляющие ценность для фирмы и подлежащие охране. Часто обычный открытый правовой акт важно сохранить в целостности и безопасности от похитителя или стихийного бедствия. Перечни формируются

индивидуально каждой фирмой в соответствии с рекомендациями специальной комиссии и утверждаются первым руководителем фирмы. Эта комиссия регулярно вносит текущие изменения в перечни в соответствии с динамикой выполнения фирмой конкретных работ.
При заключении любого договора (контракта) стороны должны брать на себя взаимные письменные обязательства по защите конфиденциальной информации другой стороны и документов, полученных при переговорах, исполнении условий договора.
Производственная или коммерческая ценность информации, как правило, недолговечна и определяется временем, необходимым конкуренту для выработки той же идеи или ее хищения и воспроизводства, а также временем до патентования, опубликования и перехода в число общеизвестных.
Документированная информация ограниченного доступа всегда принадлежит к одному из видов тайны — государственной или негосударственной. В соответствии с этим документы делятся на секретные и несекретные. Обязательным признаком (критерием принадлежности) секретного документа является наличие в нем сведений, составляющих в соответствии с законодательством государственную тайну. Несекретные документы, включающие сведения, относимые к негосударственной тайне (служебной, коммерческой, банковской, профессиональной, производственной и др.), или содержащие персональные данные граждан, именуются конфиденциальными.
Несмотря на то, что конфиденциальность является синонимом секретности, термин широко используется исключительно для обозначения информационных ресурсов ограниченного доступа, не отнесенных к государственной тайне. Конфиденциальность отражает ограничение, которое накладывает собственник информации на доступ к ней других лиц, т.е. собственник устанавливает правовой режим этой информации в соответствии с законом. Вместе с тем в соответствии с постановлением Правительства «О перечне сведений, которые не могут составлять коммерческую тайну» от 05.12.91 к конфиденциальным документам нельзя относить учредительные документы, уставы предпринимательских структур, финансовую документацию, сведения о заработной плате персонала и другую документированную информацию, необходимую правоохранительным и налоговым государственным органам.
Под конфиденциальным (закрытым, защищаемым) документом
понимается необходимым образом оформленный носитель документированной информации, содержащий сведения ограниченного доступа или использования, которые составляют интеллектуальную собственность юридического или физического лица. Конфиденциальные документы не следует называть служебными или ставить на них гриф секретности, так как конфиденциальные и секретные документы отражают различные виды тайны.
Конфиденциальные документы включают в себя:
• в государственных структурах — служебную информацию ограниченного распространения, именуемую в чиновничьем обиходе информацией для служебного пользования, т.е. информацией, отнесенной к служебной тайне, а также документы, имеющие рабочий характер и не подлежащие публикации в открытой печати (проекты документов, сопутствующие материалы и др.);
• в предпринимательских структурах и направлениях подобной деятельности — сведения, которые их собственник или владелец в соответствии с законодательством имеет право отнести к коммерческой (предпринимательской) тайне, тайне фирмы, тайне мастерства;
• независимо от принадлежности — любые персональные (личные) данные о гражданах, а также сведения, содержащие профессиональную тайну, технические и технологические новшества (до их патентования), тайну предприятий связи, сферы обслуживания и т.п.
Особенностью конфиденциального документа является то, что он представляет собой одновременно:
• массовый носитель ценной, защищаемой информации;
• основной источник накопления и объективного распространения этой информации, а также ее неправомерного разглашения или утечки; • обязательный объект защиты.
Конфиденциальность документов всегда имеет значительный разброс по срокам ограничения свободного доступа к ним персонала фирмы (от нескольких часов до значительного числа лет). Следует учитывать, что основная масса конфиденциальных документов после окончания их исполнения или работы с ними теряет свою ценность и конфиденциальность. Например, переписка до заключения контракта может иметь гриф конфиденциальности, но после его подписания этот гриф с письменного разрешения первого руководителя фирмы снимается.

Исполненные документы, сохранившие конфиденциальный характер и ценность для деятельности фирмы, формируются в дела в соответствии с номенклатурой дел. Период нахождения конфиденциальных документов в делах может быть кратковременным или долговременным в зависимости от ценности информации, содержащейся в документах дела. Период конфиденциальности документов определяется по указанному выше перечню конфиденциальных сведений и зависит от специфики деятельности фирмы. Например, производственные, научно-исследовательские фирмы обладают более ценными документами, чем торговые, посреднические и др.

Документы долговременного периода конфиденциальности (программы и планы развития бизнеса, технологическая документация ноу-хау, изобретения и др.) имеют усложненный вариант обработки и хранения, обеспечивающий безопасность информации и ее носителя. Документы кратковременного периода конфиденциальности, имеющие оперативное значение для деятельности фирмы, обрабатываются и хранятся по упрощенной схеме и могут не выделяться из технологической системы обработки открытых документов при наличии в этой системе минимальных защитных, контрольных и аналитических элементов.

Следовательно, конфиденциальные документы характеризуются специфическими особенностями, которые отражают их сущность как носителей информации ограниченного доступа и определяют построение системы защиты этой информации.

2.2. Угрозы конфиденциальной информации

Все информационные ресурсы фирмы постоянно подвергаются объективным и субъективным угрозам утраты носителя или ценности информации.

Под угрозой или опасностью утраты информации понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление неблагоприятных возможностей внешних или внутренних источников угрозы создавать критические ситуации, события, оказывать дестабилизирующее воздействие на защищаемую информацию, документы и базы данных.

Риск угрозы любым (открытым и ограниченного доступа) информационным ресурсам создают стихийные бедствия, экстремальные ситуации, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица. К угрозам, создаваемым этими лицами, относятся: несанкционированное уничтожение документов, ускорение угасания (старения) текста или изображения, подмена или изъятие документов, фальсификация текста или его части и др.

Для информационных ресурсов ограниченного доступа диапазон угроз, предполагающих утрату информации (разглашение, утечку) или утерю носителя, значительно шире в результате того, что к этим документам проявляется повышенный интерес со стороны различного рода злоумышленников. В отличие от объективного распространения утрата информации влечет за собой незаконный переход конфиденциальных сведений, документов к субъекту, не имеющему права владения ими и использования в своих целях.

Под злоумышленником понимается лицо, действующее в интересах конкурента, противника или в личных корыстных интересах (агентов иностранных спецслужб, промышленного и экономического шпионажа, криминальных структур, отдельных преступных элементов, лиц, сотрудничающих со злоумышленником, психически больных лиц и т.п.).

Основной угрозой безопасности информационных ресурсов ограниченного распространения является несанкционированный (незаконный, неразрешенный) доступ злоумышленника или постороннего лица к документированной информации и как результат — овладение информацией и противоправное ее использование или совершение иных действий. Целью и результатом несанкционированного доступа может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, подмена и т.п.

Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности фирмы (работники коммунальных служб, экстремальной помощи, прохожие и др.), посетители фирмы, работники других организационных структур, а также сотрудники данной фирмы, не обладающие правом доступа в определенные помещения, к конкретному документу, информации, базе данных. Каждое из указанных лиц может быть злоумышленником или его сообщником, агентом, но может и не быть им.

Обязательным условием успешного осуществления попытки несанкционированного доступа к информационным ресурсам ограниченного доступа является интерес к ним со стороны конкурентов, определенных лиц, служб и организаций. При отсутствии такого интереса угроза информации не возникает даже в том случае, если создались предпосылки для

ознакомления с ней постороннего лица. Основным виновником несанкционированного доступа к информационным ресурсам является, как правило, персонал, работающий с документами, информацией и базами данных. При этом надо иметь в виду, что утрата информации происходит в большинстве случаев не в результате преднамеренных действий, а из-за невнимательности и безответственности персонала.

Следовательно, утрата информационных ресурсов ограниченного доступа может наступить:

• при наличии интереса конкурента, учреждений, фирм или лиц к конкретной информации;

• при возникновении риска угрозы, организованной злоумышленником или при случайно сложившихся обстоятельствах;

• при наличии условий, позволяющих злоумышленнику осуществить необходимые действия и овладеть информацией. Эти условия могут включать:

• отсутствие системной аналитической и контрольной работы по выявлению и изучению угроз, каналов и степени риска нарушений безопасности информационных ресурсов;

• неэффективную систему защиты информации или отсутствие этой системы;

• непрофессионально организованную технологию обработки и хранения конфиденциальных документов;

• неупорядоченный подбор персонала и текучесть кадров, сложный психологический климат в коллективе;

• отсутствие системы обучения сотрудников правилам защиты информации ограниченного доступа;

• отсутствие контроля со стороны руководства фирмы за соблюдением персоналом требований нормативных документов по работе с информационными ресурсами ограниченного доступа;

• бесконтрольное посещение помещений фирмы посторонними лицами.

Следует всегда помнить, что факт документирования резко увеличивает риск угрозы информации. Великие мастера прошлого никогда не записывали секреты своего искусства, а передавали их устно сыну, ученику. Поэтому тайна изготовления многих уникальных предметов того времени так и не раскрыта до наших дней.

Угрозы сохранности, целостности и конфиденциальности информационных ресурсов ограниченного доступа практически реализуются через риск образования канала несанкционированного получения (добывания) кем-то ценной информации и документов. Этот канал представляет собой совокупность незащищенных или слабо защищенных фирмой направлений возможной утраты конфиденциальной информации, которые злоумышленник использует для получения необходимых сведений, преднамеренного незаконного доступа к защищаемой информации.

Каждая конкретная фирма обладает своим набором каналов несанкционированного доступа к информации, что зависит от множества моментов — профиля деятельности, объемов защищаемой информации, профессионального уровня персонала, местоположения здания и т.п.

Функционирование канала несанкционированного доступа к информации обязательно влечет за собой утрату информации, исчезновение носителя информации.

В том случае, когда речь идет об утрате информации по вине персонала, используется термин «разглашение (огласка) информации». Человек может разглашать информацию устно, письменно, с помощью жестов, мимики, условных сигналов, лично, через посредников, по каналам связи и т.д. Термин «утечка информации», хотя и используется наиболее широко, однако в большей степени относится, по нашему мнению, к утрате информации за счет ее перехвата с помощью технических средств разведки, по техническим каналам.

Утрата информации характеризуется двумя условиями: информация переходит а) непосредственно к заинтересованному лицу — конкуренту, злоумышленнику или б) к случайному, третьему лицу. Под третьим лицом в данном случае понимается любое постороннее лицо, получившее информацию во владение в силу обстоятельств или безответственности персонала, не обладающее правом владения ею и, что очень важно, не заинтересованное в этой информации. Однако от третьего лица информация может легко перейти к злоумышленнику.

Переход информации к третьему лицу представляется достаточно частым явлением, и его можно назвать непреднамеренным, стихийным, хотя при этом факт разглашения

информации, нарушения ее безопасности имеет место.
Непреднамеренный переход информации к третьему лицу возникает в результате:
• утери или неправильного уничтожения документа, пакета с документами, дела, конфиденциальных записей;
• игнорирования или умышленного невыполнения сотрудником требований по защите документированной информации;
• излишней разговорчивости сотрудников при отсутствии злоумышленника (с коллегами по работе, родственниками, друзьями, иными лицами в местах общего пользования, транспорте и т.п.);
• работы с документами ограниченного доступа при посторонних лицах, несанкционированной передачи их другому сотруднику;
• использования сведений ограниченного доступа в открытых документации, публикациях, интервью, личных записях, дневниках и т.п.;
• отсутствия маркировки (грифования) информации и документов ограниченного доступа (в том числе документов на технических носителях);
• наличия в документах излишней информации ограниченного доступа;
• самовольного копирования сотрудником документов в служебных или коллекционных целях.
В отличие от третьего лица злоумышленник или его сообщник целенаправленно охотятся за конкретной информацией и преднамеренно, противоправно устанавливают контакт с источником этой информации или преобразуют канал ее объективного распространения в канал ее разглашения или утечки. Такие каналы всегда являются тайной злоумышленника.
Каналы несанкционированного доступа могут быть двух типов: организационные и технические. Обеспечиваются они легальными и нелегальными методами. Организационные каналы разглашения информации отличаются большим разнообразием видов и основаны на установлении разнообразных, в том числе законных, взаимоотношений злоумышленника с фирмой или ее сотрудником для последующего несанкционированного доступа к интересующей информации.
Основными видами организационных каналов могут быть:
• поступление злоумышленника на работу в фирму, как правило, на техническую или вспомогательную должность (оператором ЭВМ, секретарем, дворником, охранником, шофером и т.п.);
• участие в работе фирмы в качестве партнера, посредника, клиента, использование разнообразных обманных способов;
• поиск злоумышленником сообщника (инициативного помощника), работающего в интересующей его фирме, который становится его соучастником;
•'установление злоумышленником доверительных взаимоотношений с сотрудником учреждения, фирмы или посетителем, сотрудником другого учреждения, обладающим интересующими злоумышленника сведениями;
• использование коммуникативных связей фирмы — участие в переговорах, совещаниях, переписке с фирмой и др.;
• использование ошибочных действий персонала или умышленное провоцирование злоумышленником этих действий;
• тайное или по фиктивным документам проникновение в здание фирмы и помещения, криминальный, силовой доступ к информации, т.е. кража документов, дискет, дисков, компьютеров, шантаж и склонение к сотрудничеству отдельных сотрудников, подкуп сотрудников, создание экстремальных ситуаций и т.п.;
• получение нужной информации от третьего (случайного) лица.
Организационные каналы отбираются или формируются злоумышленником индивидуально в соответствии с его профессиональным умением, конкретной ситуацией, и прогнозировать их крайне сложно. Обнаружение организационных каналов требует проведения серьезной поисковой и аналитической работы.
Широкие возможности несанкционированного получения подобных сведений создает техническое обеспечение офисных технологий. Любая управленческая деятельность всегда связана с обсуждением ценной информации в кабинетах или по линиям связи, проведением расчетов и анализа ситуаций на ЭВМ, изготовлением, размножением документов и т.п.
Технические каналы утечки информации возникают при использовании злоумышленником

специальных технических средств промышленного шпионажа, позволяющих получать защищаемую информацию без непосредственного контакта с персоналом фирмы, документами, делами и базами данных. Технический канал представляет собой физический путь утечки информации от источника или канала объективного распространения информации к злоумышленнику. Канал возникает при анализе злоумышленником физических полей и излучений, появляющихся в процессе работы вычислительной и другой офисной техники, при перехвате информации, имеющей звуковую, зрительную или иную форму отображения. Основными техническими каналами являются: акустический, визуально-оптический, электромагнитный и др. Это каналы прогнозируемые, носят стандартный характер и перекрываются стандартными средствами противодействия. Обычным и профессионально грамотным является творческое сочетание в действиях злоумышленника каналов обоих типов, например установление доверительных отношений с сотрудником фирмы и перехват информации по техническим каналам с помощью этого сотрудника. Вариантов и сочетаний каналов может быть множество. Изобретательность грамотного злоумышленника не знает предела, поэтому риск утраты информации всегда достаточно велик. При эффективной системе защиты информации фирмы злоумышленник разрушает отдельные элементы защиты и формирует необходимый ему канал получения информации.

В целях практической реализации поставленных задач злоумышленник определяет не только каналы несанкционированного доступа к информации фирмы, но и совокупность методов получения этой информации.

Легальные методы входят в содержание понятий «невинного Шпионажа» и «разведки в бизнесе», отличаются правовой безопасностью и, как правило, предопределяют возникновение интереса к конкурирующей фирме. В соответствии с этим может появиться Необходимость использования каналов несанкционированного доступа к требуемой информации. В основе «невинного шпионажа» Лежит кропотливая аналитическая работа специалистов-экспертов над опубликованными и общедоступными материалами конкурирующей фирмы. Одновременно изучается продукция фирмы, рекламные издания, сведения, полученные в процессе официальных и неофициальных бесед и переговоров с сотрудниками фирмы, материалы пресс-конференций, презентаций фирмы и продукции, Научных симпозиумов и семинаров, сведения, получаемые из информационных сетей. Легальные методы дают злоумышленнику Основную массу интересующей его информации и позволяют определить состав отсутствующих сведений, которые предстоит добыть нелегальными методами.

Нелегальные методы получения ценной информации всегда носят незаконный характер и используются в целях доступа к защищаемой информации, которую невозможно получить легальными методами. В основе нелегального получения информации лежит поиск злоумышленником существующих в фирме и наиболее эффективных в конкретных условиях незащищенных организационных и технических каналов несанкционированного доступа к информации, формирование таких каналов при их отсутствии и реализация плана практического комплексного использования этих каналов.

Нелегальные методы предполагают: воровство, продуманный Обман, подслушивание разговоров, подделку идентифицирующих документов, взяточничество, инсценирование или организацию экстремальных ситуаций, использование различных криминальных приемов и т.д. В процессе реализации нелегальных методов часто образуется агентурный канал добывания ценной информации. К нелегальным методам относятся также: перехват информации, объективно распространяемой по техническим каналам, визуальное наблюдение за помещениями фирмы и персоналом, анализ продуктов и объектов, содержащих следы защищаемой информации, анализ архитектурных особенностей объектов защиты, анализ отходов производства, мусора, выносимого из офиса.

В результате эффективного использования каналов несанкционированного доступа к информации ограниченного доступа и разнообразных методов ее добывания злоумышленник получает:

• подлинник или официальную копию документа (бумажного, машиночитаемого, электронного), содержащего информацию ограниченного доступа;

• несанкционированно сделанную копию этого документа (рукописную или изготовленную с помощью копировального аппарата, фототехники, компьютера и т.п.);

• диктофонную, магнитофонную, видеокассету с записью текста документа, переговоров, совещания;

• письменное или устное изложение за пределами фирмы содержания документа, ознакомление с которым осуществлялось санкционированно или тайно;
• устное изложение текста документа по телефону, переговорному устройству, специальной радиосвязи и т.п.;
• аналог документа, переданного по факсимильной связи или электронной почте;
• речевую или визуальную запись текста документа, выполненную с помощью технических средств разведки (радиозакладок, встроенных микрофонов и видеокамер, микрофотоаппаратов, фотографирования с большого расстояния). Получение ценных документов или информации ограниченного доступа может быть единичным явлением или регулярным процессом, протекающим на протяжении относительно длительного времени.
Следовательно, любые информационные ресурсы фирмы являются весьма уязвимой категорией и при интересе, возникшем к ним со стороны злоумышленника, опасность их утраты становится достаточно реальной.

2.3. Система защиты конфиденциальной информации

Практической реализацией политики (концепции) информационной безопасности фирмы является технологическая система защиты информации. Защита информации представляет собой жестко регламентированный и динамический технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности ценных информационных ресурсов и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности фирмы.
Система защиты информации — рациональная совокупность направлений, методов, средств и мероприятий, снижающих уязвимость информации и препятствующих несанкционированному доступу к информации, ее разглашению или утечке. Главными требованиями к организации эффективного функционирования системы являются: персональная ответственность руководителей и сотрудников за сохранность носителя и конфиденциальность информации, регламентация состава конфиденциальных сведений и документов, подлежащих защите, регламентация порядка доступа персонала к конфиденциальным сведениям и документам, наличие специализированной службы безопасности, обеспечивающей практическую реализацию системы защиты и нормативно-методического обеспечения деятельности этой службы.
Собственники информационных ресурсов, в том числе государственные учреждения, организации и предприятия, самостоятельно определяют (за исключением информации, отнесенной к государственной тайне) необходимую степень защищенности ресурсов и тип системы, способы и средства защиты, исходя из ценности информации. Ценность информации и требуемая надежность ее защиты находятся в прямой зависимости. Важно, что структура системы защиты должна охватывать не только электронные информационные системы, а весь управленческий комплекс фирмы в единстве его реальных функциональных и производственных подразделений, традиционных документационных процессов. Отказаться от бумажных документов и часто рутинной, исторически сложившейся управленческой технологии не всегда представляется возможным, особенно если вопрос стоит о безопасности ценной, конфиденциальной информации.
Основной характеристикой системы является ее комплексность, т.е. наличие в ней обязательных элементов, охватывающих все направления защиты информации. Соотношение элементов и их содержания обеспечивают индивидуальность построения системы защиты информации конкретной фирмы и гарантируют неповторимость системы, трудность ее преодоления. Конкретную систему защиты можно представить в виде кирпичной стены, состоящей из множества разнообразных элементов (кирпичиков). Элементами системы являются: правовой, организационный, инженерно-технический, программно-аппаратный и криптографический.
Правовой элемент системы защиты информации основывается на нормах информационного права и предполагает юридическое закрепление взаимоотношений фирмы и государства по поводу правомерности использования системы защиты информации, фирмы и персонала по поводу обязанности персонала соблюдать установленные собственником информации ограничительные и технологические меры защитного характера, а также ответственности персонала за нарушение порядка защиты информации. Этот элемент включает:
• наличие в организационных документах фирмы, правилах внутреннего трудового распорядка, контрактах, заключаемых с сотрудниками, в должностных и рабочих инструкциях положений и обязательств по защите конфиденциальной информации;

• формулирование и доведение до сведения всех сотрудников фирмы (в том числе не связанных с конфиденциальной информацией) положения о правовой ответственности за разглашение конфиденциальной информации, несанкционированное уничтожение или фальсификацию документов;
• разъяснение лицам, принимаемым на работу, положения о добровольности принимаемых ими на себя ограничений, связанных с выполнением обязанностей по защите информации.
Организационный элемент системы защиты информации содержит меры управленческого, ограничительного (режимного) и технологического характера, определяющие основы и содержание системы защиты, побуждающие персонал соблюдать правила защиты конфиденциальной информации фирмы. Эти меры связаны с установлением режима конфиденциальности в фирме. Элемент включает в себя регламентацию:
• формирования и организации деятельности службы безопасности и службы конфиденциальной документации (или менеджера по безопасности, или референта первого руководителя), обеспечения деятельности этих служб (сотрудника) нормативно-методическими документами по Организации и технологии защиты информации;
• составления и регулярного обновления состава (перечня, списка, матрицы) защищаемой информации фирмы, составления и ведения перечня (описи) защищаемых бумажных, машиночитаемых и электронных документов фирмы;
• разрешительной системы (иерархической схемы) разграничения доступа персонала к защищаемой информации;
• методов отбора персонала для работы с защищаемой информацией, методики обучения и инструктирования сотрудников;
• направлений и методов воспитательной работы с персоналом, контроля соблюдения сотрудниками порядка защиты информации;
• технологии защиты, обработки и хранения бумажных, машиночитаемых и электронных документов фирмы (делопроизводственной, автоматизированной и смешанной технологий); внемашинной технологии защиты электронных документов;
• порядка защиты ценной информации фирмы от случайных или умышленных несанкционированных действий персонала;
• ведения всех видов аналитической работы;
• порядка защиты информации при проведении совещаний, заседаний, переговоров, приеме посетителей, работе с представителями рекламных агентств, средств массовой информации;
• оборудования и аттестации помещений и рабочих зон, выделенных для работы с конфиденциальной информацией, лицензирования технических систем и средств защиты информации и охраны, сертификации информационных систем, предназначенных для обработки защищаемой информации;
• пропускного режима на территории, в здании и помещениях фирмы, идентификации персонала и посетителей;
• системы охраны территории, здания, помещений, оборудования, транспорта и персонала фирмы;
• действий персонала в экстремальных ситуациях;
• организационных вопросов приобретения, установки и эксплуатации технических средств защиты информации и охраны;
• организационных вопросов защиты персональных компьютеров, информационных систем, локальных сетей;
• работы по управлению системой защиты информации;
• критериев и порядка проведения оценочных мероприятий по установлению степени эффективности системы защиты информации.
Элемент организационной защиты является стержнем, основной частью рассматриваемой комплексной системы. По мнению большинства специалистов, меры организационной защиты информации составляют 50—60% в структуре большинства систем защиты информации. Это связано с рядом факторов и также с тем, что важной составной частью организационной защиты информации является подбор, расстановка и обучение персонала, который будет реализовывать на практике систему защиты информации. Сознательность, обученность и ответственность персонала можно с полным правом назвать краеугольным камнем любой даже самой технически совершенной системы защиты информации. Организационные меры защиты отражаются в нормативно-методических документах службы безопасности, службы конфиденциальной документации учреждения или

фирмы. В этой связи часто используется единое название двух рассмотренных выше элементов системы защиты — «элемент организационно-правовой защиты информации».
Инженерно-технический элемент системы защиты информации предназначен для пассивного и активного противодействия средствам технической разведки и формирования рубежей охраны территории, здания, помещений и оборудования с помощью комплексов технических средств. При защите информационных систем этот элемент имеет весьма важное значение, хотя стоимость средств технической защиты и охраны велика. Элемент включает в себя:
• сооружения физической (инженерной) защиты от проникновения посторонних лиц на территорию, в здание и помещения (заборы, решетки, стальные двери, кодовые замки, идентификаторы, сейфы и др.);
• средства защиты технических каналов утечки информации, возникающих при работе ЭВМ, средств связи, копировальных аппаратов, принтеров, факсов и других приборов и офисного оборудования, при проведении совещаний, заседаний, беседах с посетителями и сотрудниками, диктовке документов и т.п.;
• средства защиты помещений от визуальных способов технической разведки;
• средства обеспечения охраны территории, здания и помещений (средства наблюдения, оповещения, сигнализирования, информирования и идентификации);
• средства противопожарной охраны;
• средства обнаружения приборов и устройств технической разведки (подслушивающих и передающих устройств, тайно установленной миниатюрной звукозаписывающей и телевизионной аппаратуры и т.п.);
• технические средства контроля, предотвращающие вынос персоналом из помещения специально маркированных предметов, документов, дискет, книг и т.п. Программно-аппаратный элемент системы защиты информации предназначен для защиты ценной информации, обрабатываемой и хранящейся в компьютерах, серверах и рабочих станциях локальных сетей и различных информационных системах. Однако фрагменты этой защиты могут применяться как сопутствующие средства в инженерно-технической и организационной защите. Элемент включает в себя:
• автономные программы, обеспечивающие защиту информации и контроль степени ее защищенности;
• программы защиты информации, работающие в комплексе с программами обработки информации;
• программы защиты информации, работающие в комплексе с техническими (аппаратными) устройствами защиты информации (прерывающими работу ЭВМ при нарушении системы доступа, стирающие данные при несанкционированном входе в базу данных и др.);
Криптографический элемент системы защиты информации предназначен для защиты конфиденциальной информации методами криптографии. Элемент включает:
• регламентацию использования различных криптографических методов в ЭВМ и локальных сетях;
• определение условий и методов криптографирования текста документа при передаче его по незащищенным каналам почтовой, телеграфной, телетайпной, факсимильной и электронной связи;
• регламентацию использования средств криптографирования переговоров по незащищенным каналам телефонной и радиосвязи;
• регламентацию доступа к базам данных, файлам, электронным документам персональными паролями, идентифицирующими командами и другими методами;
• регламентацию доступа персонала в выделенные помещения с помощью идентифицирующих кодов, шифров.
Составные части криптографической защиты, коды, пароли и другие ее атрибуты разрабатываются и меняются специализированной организацией. Применение пользователями собственных систем шифровки не допускается.
В каждом элементе защиты могут быть реализованы на практике только отдельные составные части в зависимости от поставленных задач защиты в крупных и некрупных фирмах различного профиля, малом бизнесе. Структура системы, состав и содержание элементов, их взаимосвязь зависят от объема и ценности защищаемой информации, характера возникающих угроз безопасности информации, требуемой надежности защиты и стоимости системы. Например, в некрупной фирме с небольшим объемом защищаемой информации можно ограничиться регламентацией технологии обработки и хранения

документов, доступа персонала к документам и делам. Можно дополнительно выделить в отдельную группу и маркировать ценные бумажные, машиночитаемые и электронные документы, вести их опись, установить порядок подписания сотрудниками обязательства о неразглашении тайны фирмы, организовывать регулярное обучение и инструктирование сотрудников, вести аналитическую и контрольную работу. Применение простейших методов защиты, как правило, дает значительный эффект.

В крупных производственных и исследовательских фирмах с множеством информационных систем и значительными объемами защищаемых сведений формируется многоуровневая система защиты информации, характеризующаяся иерархическим доступом к информации. Однако эти системы, как и простейшие методы защиты, не должны создавать сотрудникам серьезные неудобства в работе, т.е. они должны быть «прозрачными».

Содержание составных частей элементов, методы и средства защиты информации в рамках любой системы защиты должны регулярно изменяться с целью предотвращения их раскрытия заинтересованным лицом. Конкретная система защиты информации фирмы всегда является строго конфиденциальной, секретной. При практическом использовании системы следует помнить, что лица, проектирующие и модернизирующие систему, контролирующие и анализирующие ее работу не могут быть пользователями этой системы.

Следовательно, безопасность информации в современных условиях компьютеризации информационных процессов имеет принципиальное значение для предотвращения незаконного и часто преступного использования ценных сведений. Задачи обеспечения безопасности информации реализуются комплексной системой защиты информации, которая по своему назначению способна решить множество проблем, возникающих в процессе работы с конфиденциальной информацией и документами. Основным условием безопасности информационных ресурсов ограниченного доступа от различных видов угроз является прежде всего организация в фирме аналитических исследований, построенных на современном научном уровне и позволяющих иметь постоянные сведения об эффективности системы защиты и направлениях ее совершенствования в соответствии с возникающими ситуационными проблемами.

3. АНАЛИТИЧЕСКАЯ РАБОТА В СФЕРЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ

3.1. Понятие информационно-аналитической работы

Аналитические методы обработки информации очень важны и успешно используются большинством фирм. Не в последнюю очередь в аналитической обработке нуждаются сведения, получаемые и используемые службой безопасности фирмы. Такие сведения отрывочны, противоречивы, зачастую недостоверны, но именно на их основе принимаются жизненно важные для фирмы решения. Информационно-аналитическая деятельность службы безопасности фирмы представляет собой системное получение, анализ и накопление информации с элементами прогнозирования по вопросам, относящимся к безопасности фирмы, и на этой основе консультирование и подготовка рекомендаций руководству о правомерной защите от противоправных посягательств. Служба безопасности проводит аналитическую работу не только с целью предотвратить утрату собственной информации, но и с целью получения информации о конкурентах. Являясь ядром такого понятия, как «разведка в бизнесе», аналитическая обработка информации позволяет получать по различным оценкам от 80 до 90% необходимой информации при использовании только открытых источников.

Руководитель каждой фирмы имеет собственный взгляд на построение, направления работы и структуру информационно-аналитической службы (ИАС). На основе многолетнего опыта работы в этой области как отечественных, так и зарубежных специалистов сформировалось мнение, что в силу определенных причин наиболее эффективно такие службы функционируют как ядро службы безопасности. В первую очередь это объясняется тем, что основным потребителем аналитически обработанных данных является сама служба безопасности как подразделение, наиболее нуждающееся в аналитически обработанных данных, работающее на опережение и прогнозирование событий. Кроме того, в ходе аналитической работы очень часто используются (или могут быть получены) конфиденциальные сведения, что также подтверждает рациональность размещения ИАС в службе безопасности. Даже не являющиеся конфиденциальными аналитически обработанные данные представляют собой наиболее ценные информационные ресурсы фирмы.

В настоящее время ИАС фирмы рассматривается как основной поставщик аналитически

обработанной информации для нужд всех подразделений фирмы. Основной задачей ИАС становится информационно-аналитическое обеспечение принятия решений по вопросам прежде всего основной деятельности. Таким образом, сотрудники фирмы или его подразделений могут заказать аналитический отчет по интересующему вопросу для принятия более рационального и взвешенного решения. В этой связи очень важной проблемой становится обеспечение информационной безопасности аналитически обработанных данных, представляющих собой ценный информационный ресурс фирмы наряду с другими конфиденциальными сведениями. Процесс заказа аналитического отчета должен быть четко регламентирован, чтобы только сотрудники определенного уровня имели право давать задания ИАС фирмы. Все заказы на аналитические исследования должны фиксироваться, причем темы исследований и авторы заказов на них должны тщательно регламентироваться. Доступ к аналитически обработанным данным должен быть строго ограничен.

Защита информации внутри ИАС представляет собой крайне сложную задачу, так как специфика аналитической работы в ряде случаев вступает в прямое противоречие с нормами защиты информации. Например, обеспечение такого важного принципа, как дробление информации в работе реальных ИАС, в большинстве случаев практически невозможно, так как это тормозит работу всей системы ИАС, где сотрудники должны иметь представление обо всей картине событий. Сокрытие какой-либо информации от сотрудников ИАС может привести их к ложным выводам, а фирму — к принятию неверных решений, а следовательно, и к убыткам. ИАС, являясь ядром службы безопасности фирмы, не имеет и не должна иметь властных функций. Такое положение исключает намеренное искажение обрабатываемой информации и позволяет работать «на стыках» по пограничным вопросам.

Функции ИАС:

• обеспечить своевременное поступление надежной и всесторонней информации по интересующим вопросам;

• описать сценарии действий конкурентов, которые могут затрагивать текущие интересы фирмы;

• осуществлять постоянный мониторинг событий во внешней конкурентной среде и на рынке, которые могут иметь значение для интересов фирмы;

• обеспечить безопасность собственных информационных ресурсов;

• обеспечить эффективность и исключить дублирование при сборе, анализе и распространении информации.

Следовательно, ИАС все в большей степени становится важным и функционально емким подразделением любой фирмы и, как правило, входит в состав службы безопасности. В последнее время специалисты все чаще сходятся во мнении, что в ИАС должна быть сосредоточена вся работа по прогнозированию ситуаций, а также формированию соответствующих информационных комплексов, необходимых для эффективного и взвешенного принятия решений.

3.2. Направления аналитической работы

Направления аналитической работы определяются каждой фирмой самостоятельно и отражают области ее интересов. К основным направлениям аналитической работы, разрабатываемым на многих фирмах, можно отнести: анализ объекта защиты, анализ угроз, анализ каналов несанкционированного доступа к информации, анализ комплексной безопасности фирмы, анализ нарушений режима конфиденциальности, анализ подозрений утраты конфиденциальной информации и т.д.

Можно выделить моменты, общие для всех ИАС. Направления аналитической работы, ведущейся ИАС фирмы, могут быть постоянными, периодическими и разовыми. Постоянные направления аналитической работы являются наиболее важными. Периодические и разовые направления аналитической работы характеризуются своей жесткой зависимостью от постоянных направлений. Промежутки времени, через которые проводятся исследования в области периодических направлений аналитической работы, всецело зависят от результатов анализа по постоянным направлениям. Разовые направления аналитической работы не только жестко зависят, от постоянной аналитической работы, но и в подавляющем большинстве случаев являются следствием результатов таких исследований.

В концептуальном отношении ИАС должна представлять собой единую систему анализа, контроля и прогнозирования внешней и внутренней ситуации. Все направления аналитической работы должны быть связаны определенной логикой взаимодействия.

Результаты исследований в одном направлении должны влиять на ход других исследований таким образом, чтобы результаты постоянных направлений аналитической работы инициировали проведение периодических и разовых исследований, а результаты последних не выпали из внимания специалистов по постоянным направлениям.
Следовательно, ИАС должна быть единой и взаимосвязанной структурой обеспечения фирм достоверной и аналитически обработанной информацией, направленной на информационную поддержку принятия эффективных решений по всем направлениям безопасности бизнеса.
Каждая фирма ведет индивидуальные направления аналитической работы и самостоятельно решает, следует ли разрабатывать их постоянно, периодически или только по мере надобности. Более того, каждая фирма имеет свои специфические области интересов, в рамках которых проводит аналитические исследования. Направления аналитической работы могут быть различными, но логика взаимодействия и система связей между направлениями исследований должны сохраняться. Принципиально важными представляются ключевые направления, работа по которым ведется постоянно. Как указывалось выше, наиболее сложными для обнаружения являются организационные каналы несанкционированного доступа к защищаемой информации фирмы, связанные с так называемым человеческим фактором. Например, трудно обнаружить инициативное сотрудничество злоумышленника с сотрудником фирмы — секретарем-референтом, экспертом, оператором ЭВМ и др. В основе поиска и обнаружения таких каналов лежит постоянная аналитическая работа, которая должна носить превентивный характер и использовать в качестве инструмента учетный аппарат, предназначенный для фиксирования (протоколирования) необходимых для анализа сведений. В данном случае аналитическая работа представляет собой комплексное исследование различной целевой направленности в целях выявления, структуризации и изучения опасных объективных и субъективных, потенциальных и реальных ситуаций, которые могут создать риск для экономической и информационной безопасности фирмы, ее деятельности или персонала, привести к материальным, финансовым или иным убыткам, падению престижа фирмы или ее продукции.
Результаты аналитической работы показывают степень безопасности интеллектуальной собственности, условий функционирования фирмы и являются основой для построения и совершенствования системы защиты традиционных и электронных информационных ресурсов, формирования рубежей охраны территории, здания, помещений, оборудования, продукции и персонала фирмы. Аналитическое исследование позволяет выработать способы пассивного и активного противодействия злоумышленнику в организационных и технических каналах, разработать и систематически совершенствовать систему защиты информации, определять ее структуру и стоимость в соответствии с реальными опасностями, угрожающими ценным информационным ресурсам фирмы.
Обнаружение действующего или предполагаемого канала несанкционированного доступа к информации, а также предотвращение его появления возможны только при наличии постоянного контроля и анализа объекта защиты, уровня безопасности информационных ресурсов в источнике и канале распространения информации. Уязвимым является любой элемент информационных ресурсов и информационных систем. Другие пути носят случайный характер ожидания ошибки в тайных действиях злоумышленника.
Обнаружение канала или каналов несанкционированного доступа к ценной информации фирмы входит в число постоянных направлений аналитической работы и в общем виде включает в себя:
• анализ источников конфиденциальной информации;
• анализ каналов объективного распространения информации;
• аналитическую работу с источником угрозы информации.

Аналитическое исследование источников конфиденциальной информации предусматривает:

• выявление и классификацию существующих и возможных конкурентов и соперников фирмы, криминальных структур и отдельных преступных элементов, интересующихся фирмой;
• выявление и классификацию максимально возможного числа источников конфиденциальной информации фирмы;
• выявление, классификацию и ведение перечня (учетного аппарата) реального состава циркулирующей в фирме конфиденциальной информации (в разрезе источников, обеспечиваемых функций и видов работы, с указанием носителей — документов, дискет, файлов и т.д.);

• изучение данных учета осведомленности сотрудников в тайне фирмы в разрезе каждого руководителя и сотрудника (в том числе технического и вспомогательного), т.е. изучение степени и динамики реального владения (в том числе случайного) сотрудниками конфиденциальной информацией;
• изучение состава конфиденциальной информации в разрезе документов, т.е. изучение правильности расчленения тайны (конфиденциальной информации) между документами и определение избыточности ценной информации в документах;
• учет и изучение выявленных внутренних и внешних, потенциальных и реальных (пассивных и активных) угроз каждому отдельному источнику информации, контроль процесса формирования канала несанкционированного доступа к информации;
• ведение и анализ полноты перечня защитных мер, предпринятых по каждому источнику, и защитных мер, которые могут быть использованы при активных действиях злоумышленника, заблаговременное противодействие злоумышленнику.
Обязательному учету подлежат все санкционированные и несанкционированные обращения сотрудников фирмы к конфиденциальной информации, документам, делам и базам данных.
По отношению к каналам объективного (естественного) распространения защищаемой информации (управленческие и производственные действия, функциональные связи персонала, информационные сети, технические каналы излучения информации и т.п.) применяются следующие аналитические действия и меры превентивного контроля:
• выявление и классификация реального максимального состава каналов объективного распространения конфиденциальной информации в фирме;
• изучение составных элементов каждого канала с целью нахождения опасных участков, способствующих возникновению канала несанкционированного доступа к информации;
• исследование и обобщение способов и сферы распространения информации в каждом канале;
• изучение (учет) состава конфиденциальной информации, циркулирующей в каждом канале;
• изучение (учет) состава конфиденциальной информации, циркулирующей между источниками;
• изучение сферы распространения информации при коммуникативных связях фирмы (по конкурентам, средствам массовой информации, выставкам и ярмаркам, рекламным изданиям и т.п.);
• контроль и перекрытие каналов несанкционированного ознакомления с информацией ограниченного доступа для третьих лиц, случайных, посторонних людей;
• исследование состава и эффективности методов защиты, предпринятых по каждому каналу, и дополнительных мер противодействия злоумышленнику при активных угрозах, экстремальных ситуациях.
Анализ угроз является одним из самых важных разделов аналитической работы и представляет собой ответ на вопрос, от чего или кого следует защищать определенные ранее объекты защиты. Источники угрозы конфиденциальной информации — объективные и субъективные события, явления, факторы, действия и обстоятельства, содержащие опасность для ценной информации. К объективным источникам можно отнести: экстремальные ситуации, несовершенство технических средств и др. Субъективные источники связаны с человеческим фактором и включают: злоумышленников различного рода, посторонних лиц, посетителей, неквалифицированный или безответственный персонал, психически неполноценных людей, сотрудников, обиженных руководством фирмы и др. Источники угрозы могут быть внешними и внутренними. Внешние источники находятся вне фирмы и представлены чрезвычайными событиями, а также организационными структурами и физическими лицами, проявляющими определенный интерес к фирме. Внутренние источники угрозы связаны с фатальными событиями в здании фирмы, а также с персоналом. Однако наличие источника угрозы само по себе не является угрозой. Угроза реализуется в действиях.
Аналитическая работа с источником угрозы конфиденциальной информации предусматривает:
• выявление и классификацию максимального состава источников угрозы конфиденциальной информации;
• учет и изучение каждого отдельного субъективного внутреннего и внешнего источника, степени его опасности (анализ риска) при реализации угрозы;
• разработку превентивных мероприятий по локализации и ликвидации объективных

угроз.
В области внешних источников угрозы аналитическая работа связана с маркетинговыми исследованиями, которые регулярно ведет любая фирма. Анализ внутренних источников угрозы имеет целью выявление и изучение недобросовестных интересов и злоумышленных устремлений отдельных сотрудников фирмы и партнеров. В процессе анализа источников выявляются факты получения злоумышленником секретов фирмы, факты сотрудничества персонала фирмы с конкурентами или наличия в составе сотрудников фирмы злоумышленника.
Контрольная и аналитическая работа проводится при потенциальных и пассивных угрозах источникам и каналом распространения информации. При активной угрозе одновременно осуществляется заранее спланированное, продуманное и решительное противодействие злоумышленнику. При несколько упрощенной схеме целью проведения анализа угроз можно считать выявление фигуры противника и его планов по дестабилизирующему воздействию на фирму. В ряде случаев более эффективно проводить анализ не от выявления и рассмотрения всех объектов защиты и каналов распространения информации, а от выявления лица (лиц), которое заинтересовано в реализации каких-либо угроз как конфиденциальной информации, сотрудникам, так и фирме в целом, т.е. от выявления злоумышленника. Этот метод позволяет не только более четко спрогнозировать дальнейшие действия этого лица, но и оценить границы его действий и материальные возможности. Сначала нужно выяснить, кто является злоумышленником и что ему нужно, затем, исходя из имеющихся у него средств и возможностей, будет гораздо легче спрогнозировать, как именно он попытается достигнуть своей цели. Однако не следует забывать и о том, что достаточно серьезную угрозу могут представлять и субъекты (объекты), не заинтересованные в нанесении ущерба фирме.
Следовательно, наличие, ведение и результаты постоянной аналитической работы определяют необходимость, структуру и содержание системы защиты информации, степень ее требуемой эффективности и направления совершенствования. При отсутствии в фирме серьезной аналитической работы становится практически невозможным выявление и контроль каналов несанкционированного доступа к ценной, конфиденциальной информации фирмы.
Сотрудники ИАС фирмы должны учитывать все каналы несанкционированного доступа к конфиденциальной информации, выявлять, определять наиболее вероятные из них и контролировать их. С этой целью сотрудники ИАС должны принимать непосредственное участие в мероприятиях, в ходе которых имеется вероятность возникновения, указанных каналов доступа к конфиденциальной информации фирмы. Так, целесообразным является предварительная оценка аналитиками подготовленных к публикации материалов о фирме, выставочных проспектов, рекламных изданий и т.п., их участие в презентациях, выставках, собраниях акционеров, переговорах, а также собеседованиях и тестированиях кандидатов на должности. Последнее является одной из основных и наиболее важных обязанностей ИАС, так как именно на этом этапе можно с определенной долей вероятности перекрыть один из основных организационных каналов — поступление злоумышленника на работу в фирму. В состав ИАС должны входить профессиональные психологи — специалисты по проведению опросов и тестов среди персонала.
Аналитически обработанные сведения вносятся в электронную базу данных. Аналитические отчеты по каждому направлению представляются с определенной периодичностью. В любой момент времени по требованию руководства ИАС должна быть в состоянии представить сводный обзор по всем направлениям. При выявлении каких-либо подозрений, угроз, пробелов в защите и т.п. сразу же ставятся в известность руководители, а аналитический отчет готовится в кратчайшие сроки.
Не менее важными являются и так называемые периодические направления аналитической работы, которые проводятся через определенные промежутки времени с целью контроля эффективности и возможности внесения улучшений в действующую в фирме систему защиты информации. К такому виду направлений аналитической работы прежде всего относится анализ степени безопасности фирмы. Очевидно, что постоянная и каждодневная аналитическая работа по данному направлению не имеет смысла. Вполне достаточно проводить анализ через определенные, специально установленные промежутки времени. Это направление аналитической работы находится в прямой зависимости от анализа состава угроз — постоянного направления аналитической работы. Именно результаты аналитической работы по выявлению угроз позволяют установить рациональную

периодичность анализа эффективности структуры действующей системы безопасности фирмы. Так, при появлении дополнительных угроз, аналитическую работу (и следовательно, проверки, контрольные мероприятия и т.п.) следует проводить более часто.

Необходимо также периодически проводить анализ нарушений режима конфиденциальности, причем это направление относится также и к разовым направлениям. Рассматриваемые в рамках периодического направления аналитической работы нарушения режима безопасности за определенный период времени анализируются с целью выявления вызвавших их причин и выработки мер для их устранения. Частота проведения исследований такого рода также напрямую зависит от результатов исследований по другим направлениям.

Разовые направления аналитических исследований также являются очень важными в силу того факта, что чаще всего бывают вызваны чрезвычайными обстоятельствами, происшествиями, неожиданно появившимися проблемами и т.п., требуют проведения исследований в кратчайшие сроки. Типичным примером разового направления аналитической работы является проверка подозрения утраты конфиденциальной информации фирмы и злоумышленных действий, а также анализ нарушения режима конфиденциальности в фирме. Последнее направление включается также и в подсистему периодических направлений. Тем не менее факт каждого нарушения режима конфиденциальности должен сразу же расследоваться и анализироваться.

Следовательно, все направления аналитической работы независимо от их типа, в том числе имеющие разовый характер, должны быть связаны в единую систему, позволяющую эффективно принимать решения, предотвращать угрозы и прогнозировать развитие событий — работать на опережение.

3.3. Этапы аналитической работы

Ведение аналитической работы возможно только при наличии необходимой информации, поэтому в первую очередь нужно определить, какая, именно информация будет необходима аналитикам для работы, где можно ее получить и какой из источников можно при этом использовать. Как правило, получение информации не относится специалистами непосредственно к аналитической работе, тем не менее, определение круга исходной информации, а также мест и способов ее получения должно решаться непосредственно сотрудниками ИАС.

Интерпретация информации является первым этапом предварительного анализа. Под интерпретацией подразумевается выявление истинного значения той или иной информации. В первую очередь это относится к вербальной информации, так как очень часто то или иное высказывание бывает понято превратно. Это происходит, когда фраза вырвана из контекста либо неправильно понята иностранная речь, интонация, жесты, сленг и т.п. При возникновении такой ситуации в помощь аналитикам целесообразно пригласить знающего специалиста, который сможет правильно интерпретировать то или иное сообщение.

В интерпретации нуждаются не только слова, но и действия. Зачастую факт, внешне подозрительный, на самом деле может иметь абсолютно положительный характер, а многие по сути угрожающие факты могут иногда выглядеть как неопасные.

Язык, используемый для описания информации, может допускать неоднозначность ее понимания. Это создает определенные трудности при интерпретации вербальной информации, но в этом случае истинный смысл можно понять из контекста. Информация, которая хранится в персональных компьютерах, как правило, лишена контекста, поэтому ошибочная интерпретация становится гораздо более вероятной. Западные специалисты определяют цену информации через те действия, которые могут быть предприняты в результате знания этой информации.

Вся информация подразделяется на факты, личные мнения и аналитически обработанные данные. Смешивание или неправильное определение этих различных по своей сути видов информации может приводить к ошибкам в интерпретации и, как следствие, к принятию неправильных решений. Следовательно, процесс интерпретации требует максимальной осторожности и тщательности. В каждом конкретном случае необходимо выявить истинный смысл поступившей информации. Здесь аналитики сталкиваются с такой проблемой, как выделение не относящейся к делу информации.

Выделение посторонней информации составляет следующий этап предварительного анализа. Этот процесс является одним из самых сложных и ответственных моментов во

всей процедуре. Избыток информации, так же как и ее недостаток, представляет собой серьезную проблему и затрудняет проведение аналитической работы. Тактика выделения нескольких ключевых деталей гораздо более эффективна, чем разбрасывание между многими разрозненными данными. Вместе с тем именно на этом этапе существует опасность отбросить важную информацию. Как правило, это может произойти в случае неправильной интерпретации сведений на предыдущем этапе. Кроме того, аналитики могут стремиться сохранить не относящуюся напрямую к делу информацию в надежде, что она может пригодиться в будущем. Такая информация должна заноситься в банк данных ИАС таким образом, чтобы впоследствии ее можно было легко найти. С созданием такого информационного фонда и его постоянным пополнением задача поиска и сбора исходной информации для анализа будет значительно облегчена. Тем не менее избыток информации представляет собой серьезную проблему, так как значительно замедляет ведение аналитической работы, старение же и обесценивание информации может происходить очень быстро. Кроме того, избыток не относящейся к делу информации является для руководителя ИАС сигналом того, что поиск и сбор информации организованы неэффективно.

Оценка информации составляет следующий этап. Под оценкой понимается метод ранжирования источников информации, самой информации и способов ее получения. Как правило, пользуются системой оценок информации, при которой аналитик может выразить свою точку зрения относительно надежности и достоверности полученных сведений, хотя очевидным недостатком данной системы будет определенная субъективность оценок. Например:

Оценка источника:

• надежный источник;
• обычно надежный источник;
• довольно надежный источник;
• не всегда надежный источник;
• ненадежный источник;
• источник неустановленной надежности. Оценка информации:
• подтвержденная другими фактами;
• вероятно правдивая (75%);
• возможно правдивая (50%);
• сомнительная (25%);
• неправдоподобная;
• достоверность не поддается определению. Оценка способа получения информации источником;
• получил информацию сам (сам видел, слышал и т.п.);
• получил информацию через постоянный источник (через информатора, открытые источники и т.п.);
• получил информацию через разовый источник (случайно подслушанный разговор, слухи и т.п.).

На этапе оценки необходимо установить, насколько информация может соответствовать истине. При этом нужно учитывать, что можно получить не соответствующую истине информацию следующих типов:

• дезинформацию, доведенную до сведения источника;
• преднамеренно или непреднамеренно искаженную источником;
• произвольно или непроизвольно измененную в ходе передачи.

При намеренной дезинформации применяется заведомая ложь, полуправда, а также правдивые сведения, которые в данном контексте подтолкнут воспринимающих информацию лиц к ложным выводам.

Искажения, возникающие в процессе передачи исходных данных, могут происходить по многим причинам:

• передача только части сообщения;
• пересказ услышанного своими словами;
• факты, искаженные чьим-либо субъективным восприятием. Для своевременного выявления искаженной информации, а также для успешной борьбы с вероятной дезинформацией необходимо различать факты и мнения, учитывать субъективные характеристики источника и его предполагаемое отношение к выдаваемому сообщению. Следует четко осознавать, способен ли источник по своему положению иметь доступ к

сообщаемым фактам. В качестве страховочных мер всегда нужно иметь дублирующие источники, использовать дублирующие каналы связи и стараться исключать все лишние промежуточные звенья передачи информации. Кроме того, необходимо помнить, что особенно легко воспринимается та дезинформация, которая хорошо соответствует принятой ранее версии, т.е. та, которую предполагают или желают получить.

Следующим этапом является построение предварительных версий, объясняющих место основных полученных фактов в цепи событий. Первым шагом является составление списка сведений, приготовленных для анализа. Это необходимо для дальнейшего ранжирования их по степени важности, кроме того, это является некой гарантией того, что сведения не выпадут из поля зрения и о них не забудут. Далее необходимо выделить ключевые моменты, отделить их от менее важных, не играющих главной роли в данной ситуации. Полученные сведения должны быть четко классифицированы по степени достоверности источника, самих сведений и способа их получения. Самые свежие и полные сведения должны рассматриваться в первую очередь. В перечне сведений, приготовленных для анализа, наиболее важные сведения специально помечаются. Материалы с пометками «источник неустановленной надежности» и «достоверность не поддается определению» откладываются и не участвуют в анализе без крайней необходимости.

Затем необходимо выявить все возможные гипотезы, которые могут объяснять ключевые события, и, расположив их по степени вероятности, поочередно проверять на стыкуемость со всеми данными. Если обнаружено значительное расхождение какой-либо предварительной гипотезы с полученными сведениями, причем последние имеют достаточно высокие оценки достоверности, то следует переходить к следующей гипотезе. Таким образом, выбираются наиболее вероятные предположения. На этом этапе возникает одна из самых серьезных проблем аналитической работы — противоречия в сведениях. Для ее преодоления необходимо сравнить оценки информации и источника, даты получения спорных сведений. Решающее же значение имеет интуиция, знания и опыт самого сотрудника, проводящего анализ. Конфликты в информации должны быть устранены в процессе анализа, для их разрешения собирается дополнительная информация, что соответствует следующему этапу аналитической работы. Если решение, которое будет принято на основе аналитически обработанной информации, является очень важным и нет возможности получить дополнительную информацию для устранения противоречий, то окончательный выбор возлагается на лиц, ответственных за принятие решения. Тем не менее общая доля таких ситуаций должна сводиться к минимуму, так как это свидетельствует о неудовлетворительной работе ИАС.

Следующим этапом является определение потребности в дополнительной уточняющей информации, а также выяснение, какая именно информация необходима и почему. На этом этапе выявляются пробелы в информации. Часть пробелов может быть быстро установлена, так как является результатом недостаточного исследования, другая же часть пробелов в информации может и не быть обнаружена аналитиком, потому что упущена на этапе сбора самих сведений. Очевидно, что второй вид пробелов в информации является гораздо более опасным.

Необходимо четко различать понятия «неполная информация» и «пробел в информации». Неполная информация означает отсутствие не имеющих особой важности сведений, что является естественным, так как никогда нельзя получить абсолютно все сведения. Более того, такая информация была бы избыточной и осложнила бы анализ. Пробел же в информации подразумевает отсутствие сведений, являющихся ключевыми в данной ситуации или необходимыми для устранения противоречий. Такие сведения крайне важны для проведения анализа.

Выявив пробелы в информации, нужно определить их важность для дальнейшего анализа. Нельзя до бесконечности откладывать составление аналитического отчета под предлогом того, что в информации выявлены пробелы. На определенном этапе следует признать, что для решения задачи собрано достаточно данных. Кроме того, имеют значение факторы времени и денег, потому что решение проблемы ограничено тем и другим. Сотрудники ИАС должны стремиться к решению поставленной задачи имеющимися средствами и в разумные сроки.

На основе выполнения предыдущих этапов приступают к подготовке аналитических отчетов по определенному вопросу, выработке конкретных выводов и предложений. Подготовка отчетов является основной обязанностью аналитика, а готовый отчет представляет собой результат функционирования системы аналитической работы. Отчеты

могут быть представлены в различных формах. Наиболее часто отчет составляется в письменном виде, но он также может быть устным, иллюстрируемым графиками, таблицами, диаграммами и т.п. Если сроки жестко ограничены, отчет излагается устно, в форме вопросов и ответов.

В зарубежной литературе выделяют три основных вида аналитических отчетов. Первый вид называют тактическим (оперативным) отчетом. К этому типу относятся экстренные отчеты по какому-либо вопросу небольшого объема, которые необходимы для срочного принятия решения. При этом аналитика редко знакомят с причиной или целью данного задания. Такие отчеты составляются по разовым направлениям аналитической работы. Второй вид составляют стратегические отчеты. Они содержат более полную информацию и менее ограничены сроками. В них включается подробная предыстория данной проблемы и прогноз ее дальнейшего развития, причем для построения реалистичной гипотезы анализируется вся предшествующая информация поданной теме. Отчеты такого типа соответствуют постоянным направлениям аналитической работы. Третий вид представлен периодическими отчетами, основной отличительной особенностью которых является то, что они готовятся по графику. Интервалы между сроками предоставления составляют дни, недели или месяцы. Как правило, такой вид отчетов готовится по проблемам, являющимся объектом постоянного пристального внимания со стороны ИАС фирмы. Этот вид может соответствовать как периодическим, так и постоянным направлениям аналитической работы.

Все письменные отчеты должны содержать глубокий анализ и быть представлены в регламентированной (типовой, унифицированной) форме. Потребителями аналитических отчетов являются ответственные за планирование и принятие решений лица, которые вправе предъявлять определенные требования к содержанию и оформлению отчетов. Аналитический отчет должен быть четко, логично и грамотно составлен. Кроме того, отчет должен абсолютно соответствовать месту сотрудника — потребителя информации в разрешительной системе доступа к конфиденциальной информации: по степени конфиденциальности используемых в отчете сведений, профилю профессиональных знаний сотрудника и деловой необходимости информации для конкретной работы. Нужно учитывать также и то, что внешний вид отчета обязательно будет влиять на восприятие содержащейся в нем информации.

За рубежом используется, как правило, следующая форма изложения данных аналитического отчета:

1) Заключение. Здесь должны содержаться ответы на вопросы, какова степень важности полученной информации, ее значение для принятия конкретных решений, идет ли речь о каких-либо угрозах, подозрениях, выявленных негативных факторах и т.п., какое отношение имеет предмет отчета к другим областям аналитической работы. Факты и сведения, на основе которых получены результаты анализа, не должны смешиваться с самими результатами.

2) Рекомендации. Должны быть указаны конкретные направления дальнейших действий службы безопасности и других структурных подразделений предприятия для улучшения системы безопасности, предотвращения утраты информации, принятия наиболее эффективных решений и т.п.

3) **Обобщение информации.** Изложение самой существенной информации без излишней детализации.

4) Источники и надежность информации. Должны быть указаны предполагаемые оценки надежности данных и источника на момент написания отчета, так как для принятия решений необходимо оценить надежность материалов, являющихся их базой.

5) Основные и альтернативные гипотезы. Обязательно должны указываться рассмотренные в ходе анализа наиболее вероятные гипотезы, что помогает принимать более взвешенные и адекватные решения, а также позволяет еще раз оценить правильность выбранной гипотезы.

6) Недостающая информация. Четко указывается, какая именно дополнительная информация необходима для подтверждения окончательной гипотезы и принятия решения. Описанная структурная схема проведения аналитического исследования позволяет предоставить в распоряжение пользователя, принимающего решение, структурированный массив ценной информации, отражающей с определенной степенью достоверности сложившуюся ситуацию с обеспечением безопасности информационных ресурсов фирмы.

3.4. Методы аналитической работы

Основным назначением всех аналитических методов является обработка полученных сведений, установление взаимосвязи между фактами, выявление значения этих связей и выработка конкретных предложений на основе достоверной и полной, аналитически обработанной информации. Существует широкий спектр специальных методов анализа: графические, табличные, матричные и т.п., например, диаграммы связи и матрицы участников, схемы потоков данных, временные графики, графики анализа визуальных наблюдений VIA (visual investigative analysis) и графики оценки результатов PERT (program evaluation review technique). Тем не менее следует отметить, что у каждого аналитика есть свой собственный метод анализа, который может быть как комбинацией вышеперечисленных методов, так и сугубо индивидуальным, уникальным методом аналитической работы.

С помощью диаграмм связей выявляется наличие связи между субъектами, вовлеченными в конкретную ситуацию, подвергающуюся анализу, а также области общения, соприкосновения этих субъектов. На диаграмме связей отмечают как наиболее прочные, так и вспомогательные связи между субъектами. Анализируются все связи без исключения, так как в ходе развития событий и получения дополнительной информации вспомогательные связи могут выступить на первый план. Для большей наглядности следует. также указывать на диаграмме связи должностей (для физических лиц) или род деятельности (для юридических лиц).

Матрицы связей отражают частоту взаимодействия субъектов за определенный период времени. Такой метод анализа дополняет диаграммы связей, позволяет оценить характер взаимодействий между субъектами через частоту таких взаимодействий. При использовании этого метода анализа до его начала необходимо отделить маловажные и не имеющие отношения к делу, пусть даже частые, взаимодействия субъектов.

Схемы потоков информации позволяют оценить то, каким образом происходят события. С их помощью можно анализировать пути движения информации среди субъектов анализа, т.е. оценивать положение каждого субъекта в общей группе и выявлять неустановленные связи между субъектами, используя определенную, специально подготовленную информацию как индикатор. Метод применим для отображения, например, физических процессов, взаимодействия юридических и физических лиц.

Временные графики используются для регистрации событий. Такая форма представления данных помогает не только эффективнее анализировать события, но и более рационально планировать меры противодействия.

Графики анализа визуальных наблюдений VIA являются составной частью графиков оценки результатов PERT. Оба графика составляются по принципу разбивки сложной операции на составные элементы. Такой принцип позволяет наглядно отражать ход событий. В зарубежных странах графики VIA и PERT применяются для анализа тяжких преступлений и террористической деятельности, для повышения эффективности работы предприятий, а также аналитиками служб безопасности для нужд ИАС фирм. В обоих графиках принята одна и та же система символов: события представлены треугольниками и кругами, причем треугольники отмечают начало и конец события, а также наиболее важные моменты операции. Отличием этих типов графиков является то, что график VIA представляет собой схему визуальных наблюдений в процессе одиночного события, а график PERT отражает общий ход событий, является более общим методом анализа. Графики VIA и PERT могут иметь различную степень детализации событий. С их помощью легко вычленить определенную схему в действиях субъектов, что значительно облегчит процесс построения версий. Графики PERT широко применяются при таком широко распространенном методе анализа, как изучение реальных дел с целью поиска аналогий. Такой метод позволяет определить возможные сценарии, по которым события реально развивались в предшествующий период. Основная идея этого метода состоит в том, что все события рано или поздно повторяются в силу схожести целей, средств и обстоятельств. Разбор и анализ ситуаций, имевших место в прошлом, позволяет на раннем этапе выявить подлинный характер происходящего за счет совпадения с типичными схемами.

В настоящее время в работе ИАС широко используются возможности современной вычислительной техники. Это относится не только к созданию баз данных по тематике аналитической работы, но и непосредственно к процессу анализа. Статистический анализ в подавляющем большинстве случаев не выполняется вручную, для этого должны применяться специальные пакеты программ статистической обработки данных,

предназначенные для аналитической работы. Такие программы используются зарубежными специалистами при анализе уже достаточно длительное время и с большим успехом.
В последнее время для аналитической работы все чаще применяются так называемые экспертные системы (expert systems), которые, являясь практическим приложением искусственного интеллекта, оказывают огромную помощь при анализе, а в ряде случаев могут даже заменить собой аналитика. Они представляют собой класс компьютерных программ, которые выдают советы, проводят анализ, выполняют классификацию, дают консультации и ставят диагноз. Экспертные системы не только выполняют все эти функции, но и на каждом шаге могут объяснить аналитику причину той или иной рекомендации и последовательность анализа. Широкое использование таких систем в зарубежных странах объясняется тем фактом, что аналитические задачи, как и все задачи, требующие дедуктивных рассуждений, решаются компьютером не хуже, чем человеком, а в ряде случаев — быстрее и надежнее. В отличие от человека-аналитика у экспертных систем нет предубеждений, они не делают поспешных выводов, не поддаются влиянию внешних факторов. Такие системы работают систематизированно, рассматривая все детали, выбирая наилучшую альтернативу из всех возможных. Несомненным преимуществом экспертных систем является и то, что, будучи введены в машину один раз, знания сохраняются навсегда, как бы обширны они ни были.
Теоретически экспертные системы по мере своего развития и расширения проходят три стадии:
1) ассистент — система освобождает человека-аналитика от рутинной и однообразной аналитической работы, позволяя заниматься только самыми важными и ответственными вопросами;
2) коллега — система участвует в решении проблемы на равных с человеком, общение с системой представляет собой постоянный диалог;
3) эксперт — уровень знаний системы во много раз превосходит уровень знаний человека, так как знания системы представляют собой постоянно пополняемую совокупность знаний многих ведущих экспертов в этой области.
Реально в настоящее время применяются экспертные системы первого уровня — облегчающие работу аналитика. Такие системы накапливают знания и опыт наиболее квалифицированных экспертов-аналитиков. С помощью этих знаний пользователь с обычной квалификацией может решать различные аналитические задачи столь же успешно, как и сами эксперты. Это происходит за счет того, что система в своей работе воспроизводит ту же схему рассуждений, что и человек-эксперт при анализе проблемы.
Второй уровень экспертных систем пока не достигнут в силу больших практических трудностей.
Третий уровень экспертных систем пока существует лишь в проекте.
Экспертные системы позволяют копировать и распространять знания, делая уникальный опыт нескольких экспертов-аналитиков доступным широким кругам рядовых специалистов. То есть такие системы имитируют деятельность человека-эксперта. Однако эти системы имеют существенные недостатки — большинство экспертных систем не вполне пригодны для применения конечным пользователем, они рассчитаны в первую очередь на использование теми экспертами, которые создавали их базы знаний. Пользователь экспертной системы не только должен иметь определенные навыки работы с такими системами, но и представлять себе логику ее построения. К недостаткам можно отнести и то, что приведение знаний, полученных от эксперта, к виду, обеспечивающему их эффективную машинную реализацию, все еще остается достаточно сложной задачей. Экспертные системы еще не способны самообучаться, не обладают интуицией и здравым смыслом, которые использует человек-аналитик при отсутствии формальных методов решения или аналогов таких задач.
Эти недостатки планируется устранить в экспертных системах второго поколения (система-коллега). Они смогут не просто повторять ход рассуждений экспертов, а стать полноценными помощниками и советчиками для аналитика. Такие экспертные системы будут проводить анализ нецифровых данных, выдвигать и отбрасывать гипотезы, оценивать достоверность фактов, самостоятельно пополнять свои знания, контролировать их непротиворечивость, делать заключения на основе прецедентов и, может быть, даже порождать решения новых, ранее не рассматривавшихся задач.
Следовательно, в распоряжении сотрудников ИАС предприятия находится множество методов ведения аналитической работы, среди которых они могут выбрать наиболее

эффективный с их точки зрения метод, либо пользоваться своим собственным, уникальным методом. В работу ИАС предприятий также должны широко внедряться современные компьютерные технологии как в форме современных баз данных и новейших статистических программ, так и в форме практического применения искусственного интеллекта — экспертных систем.

4. ОСОБЕННОСТИ РАБОТЫ С ПЕРСОНАЛОМ, ВЛАДЕЮЩИМ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИЕЙ

4.1. Персонал как основная опасность утраты конфиденциальной информации

В основе системы защиты информации лежит человеческий фактор, предполагающий преданность персонала интересам фирмы, и осознанное соблюдение им установленных правил защиты информации. Если отдельный сотрудник не оправдает доверия, то никакая эффективная система защиты не сможет гарантировать безопасность информации и предотвратить ее разглашение.

В решении проблемы информационной безопасности значительное место занимает выбор эффективных методов работы с персоналом, обладающим конфиденциальной информацией. Персонал генерирует новые идеи, новшества, открытия и изобретения, которые ускоряют научно-технический прогресс, повышают благосостояние сотрудников фирмы и являются полезными не только для фирмы в целом, но и для каждого отдельного сотрудника. Поэтому любой сотрудник объективно заинтересован сохранять в тайне те новшества, которые повышают прибыли и престиж фирмы.

Несмотря на это персонал, к сожалению, является в то же время основным источником утраты ценной и конфиденциальной информации. Объясняется это тем, что с точки зрения психологических особенностей персонал — явление сложное, каждый из сотрудников всегда индивидуален, трудно предсказуем и мотивации его поведения часто противоречивы и не отвечают требованиям сложившейся жизненной ситуации. Это определяет особую значимость решения проблемы тщательного изучения персонала в структурах, связанных с необходимостью заботиться о сохранении в тайне тех или иных сведений, документов и баз данных. Трудности в работе с персоналом и сложности в подборе достойных во всех отношениях людей испытывает любая фирма, которая использует в работе достаточные объемы конфиденциальных сведений.

В современных предпринимательских структурах практически каждый основной сотрудник становится носителем ценных сведений, которые представляют интерес для конкурентов и криминальных структур. В контексте безопасности кадровая политика имеет профилактическую роль по отношению к такому типу угрозы, как неблагонадежность отдельных сотрудников. Вопросы управления персоналом, работа которого связана с обработкой, хранением и использованием конфиденциальных сведений, документов и баз данных, в настоящее время все в большей степени в концептуальном и практическом аспектах включаются в число главных при решении проблем информационной безопасности.

Информационная безопасность понимается как защищенность информации на любых носителях от случайных и преднамеренных несанкционированных воздействий естественного и искусственного свойства, направленных на уничтожение, разрушение, видоизменение тех или иных данных, изменение степени доступности ценных сведений. Помимо профессиональных способностей сотрудники, связанные с секретами фирмы, должны обладать высокими моральными качествами, порядочностью, исполнительностью и ответственностью. Они добровольно соглашаются на определенные ограничения в использовании информационных ресурсов и вырабатывают в себе самодисциплину, самоконтроль действий, поступков и высказываний. Зарубежные специалисты считают, что сохранность конфиденциальной информации на 80% зависит от правильного подбора, расстановки и воспитания персонала фирмы.

Повышение ответственности персонала за выполняемую работу, сохранность ценных сведений, активное участие в принятии управленческих решений требует нового содержания при оценке таких критериев, как образование, профессионализм, личная культура, моральные качества и этика работников. Люди рассматриваются как самый ценный ресурс фирмы и решают, с одной стороны, производственные и коммерческие задачи, а с другой — получают во владение ценные и конфиденциальные сведения фирмы и обеспечивают их правильное использование и сохранность.

Работа с персоналом подразумевает целенаправленную деятельность руководства фирмы и

трудового коллектива, направленную на наиболее полное использование трудовых и творческих способностей каждого члена коллектива, воспитание в нем фирменной гордости, препятствующей возникновению желания нанести вред организации, стать соучастником в недобросовестной конкуренции или криминальных действиях.
Человеческий фактор должен постоянно учитываться в долговременной стратегии фирмы и ее текущей деятельности, являться основным элементом построения действенной и эффективной системы защиты информационных ресурсов.
Организационные мероприятия по работе с персоналом, получающим доступ к конфиденциальной информации, можно разделить на несколько групп:
• проведение усложненных аналитических процедур при приеме и увольнении сотрудников;
• документирование добровольного согласия лица не разглашать конфиденциальные сведения и соблюдать правила обеспечения безопасности информации;
• Инструктирование и обучение сотрудников практическим действиям по защите информации;
А контроль за выполнением персоналом требований по защите информации, стимулирование ответственного отношения к сохранению конфиденциальных сведений.
Сложности в работе с персоналом определяются:
• большой ценой решения о допуске лица к тайне предприятия;
• наличием в фирме, как правило, небольшого контингента сотрудников, служебные обязанности которых связаны с использованием конфиденциальных сведений (руководители, ответственные исполнители, сотрудники службы конфиденциальной документации);
• разбиением тайны на отдельные элементы, каждый из которых известен определенным сотрудникам в соответствии с направлением их деятельности.
Персонал является основным и самым трудно контролируемым источником ценной и конфиденциальной информации.
Источник, который мы именуем «Персонал и окружающие фирму люди», включает в себя:
• всех сотрудников данной фирмы, ее персонал;
• сотрудников других фирм — посредников, изготовителей комплектующих деталей, торговых фирм, рекламных агентств и т.п.);
• сотрудников государственных учреждений, к которым фирма обращается в соответствии с законом — налоговых и иных инспекций, муниципальных органов, правоохранительных органов и т.д.;
• журналистов средств массовой информации, сотрудничающих с фирмой;
• посетителей фирмы, работников коммунальных служб, почтовых служащих, работников служб экстремальной помощи и т.д.;
• посторонних лиц, работающих или проживающих рядом со зданием или помещениями фирмы, уличных прохожих;
• родственников, знакомых и друзей всех указанных выше лиц. Перечисленные лица в той или иной мере являются или могут стать в силу обстоятельств источниками конфиденциальных сведений. Каждый из источников, особенно ставший им случайно, может стать опасным для фирмы в результате несанкционированного разглашения (оглашения) защищаемых сведений.
Наиболее осведомлены в секретах фирмы первый руководитель, его основной заместитель, их референты и секретари, работники службы конфиденциальной документации.
Следовательно, персонал фирмы, владеющий ценной и конфиденциальной информацией, работающий с конфиденциальными делами и базами данных, является наиболее осведомленным и часто достаточно доступным источником для злоумышленника, желающего получить необходимые ему сведения. Причем овладение требуемой информацией происходит в значительном числе случает в результате безответственности и необученности персонала, его недостаточно высоких личных и моральных качеств.

4.2. Методы добывания ценной информации у персонала

Прежде всего, можно выделить так называемое осознанное сотрудничество работника фирмы со злоумышленником. К такому сотрудничеству можно отнести:
• инициативное сотрудничество работника фирмы с целью мести руководству или коллективу фирмы, а также по причине подкупа, регулярной оплаты постоянных услуг, и психической неустойчивости;

• формирование сообщества — злоумышленник и его сообщник, помощник, работающий на основе убеждения в справедливости взглядов злоумышленника, дружеских и иных отношений, взаимопомощи и т.п.
• сотрудничество на основе личного убеждения работника в противоправных действиях руководства фирмы или их моральном разложении;
• склонение (принуждение, побуждение) к сотрудничеству путем обманных действий, изменения взглядов или моральных принципов путем убеждения, вымогательства, шантажа, использования отрицательных черт характера, физического насилия.
Наиболее частым, достаточно опасным и трудно выявляемым является использование сотрудника фирмы для неосознанного сотрудничества:
• переманивание ценных и осведомленных специалистов обещанием лучшего материального вознаграждения, лучшими условиями труда и иными преимуществами («кража мозгов»);
• ложная инициатива в приеме сотрудника на высокооплачиваемую работу в конкурирующую фирму, выведывание в процессе собеседования необходимых конфиденциальных сведений и затем отказ в приеме;
• выведывание ценной информации у сотрудника фирмы с помощью подготовленной системы вопросов на научных конференциях, встречах с прессой, на выставках, в личных беседах в служебной и неслужебной обстановке;
• подслушивание и записывание на диктофон разговоров сотрудников фирмы в служебных и неслужебных помещениях, в процессе переговоров и приеме посетителей, в транспорте, на банкетах, в домашней обстановке, при общении с друзьями и знакомыми;
• прослушивание служебных и личных телефонов сотрудников фирмы; перехват телексов, телеграмм, факсов, сообщений по электронной почте, вскрытие и ознакомление со служебной и личной корреспонденцией руководства фирмы сотрудников (иногда при содействии секретаря);
• получение злоумышленником от сотрудника нужной информации, когда сотрудник находится в состоянии алкогольного опьянения, под действием наркотиков, психотропных препаратов, внушений, гипноза, приведения злоумышленником сотрудника в бессознательное состояние, не позволяющее адекватно оценивать свои действия и легко меняющее убеждение.
От персонала информация легко переходит к злоумышленнику по причине:
• слабого знания персоналом требований и правил защиты информации;
• злостного или безответственного невыполнения сотрудником этих правил;
• использования экстремальных ситуаций в помещениях фирмы и происшествий с персоналом: пожара (или инсценирования пожара), нападения, плохого самочувствия сотрудника в транспорте, отключения электропитания в помещении фирмы и т.п.;
• ошибочных или безответственных действий персонала. Ошибочные и безответственные действия персонала обычно подразделяют на две группы:
• не провоцированные злоумышленником: взятие конфиденциальных документов на дом, оставление без надзора документа или загруженного компьютера, выбрасывание в мусорную корзину черновиков и копий конфиденциальных документов, использование конфиденциальной информации в открытых публикациях, ошибочная выдача конфиденциального документа сотруднику, не имеющему к нему доступа, и т.п.;
• провоцированные злоумышленником: предоставление конфиденциальной информации на ложные социологические и другие опросы, прохождение сотрудником ложного анкетирования, обман сотрудника, выдающего документы, проход злоумышленника или его сообщника в режимное помещение, на территорию фирмы по фиктивным документам, общение сотрудника с легендированным злоумышленником по поводу сведений, составляющих тайну, и т.п.
Результативность обмана зависит от подготовки, интуиции и сообразительности сотрудников, которых провоцируют на ошибочные действия. Сотрудники должны быть обучены и готовы к противодействию подобным действиям злоумышленника или его сообщников, посторонних лиц.
Хорошие деловые отношения обычно складываются у злоумышленника с сотрудниками, которые обижены на руководство фирмы или структурного подразделения, незаслуженно забыты при выдвижении на должность или повышение оклада, не получившими материального или морального поощрения за успехи в работе, испортившими отношения с коллективом или неформальным лидером коллектива. Неустойчивый и сложный психологический климат в коллективе фирмы является надежной основой для успешной

работы даже не очень опытного злоумышленника и его помощников.
Личные и бытовые затруднения сотрудников, на которые не обращает внимание руководство фирмы, также являются хорошей почвой для работы с ним злоумышленника. Например: временные материальные затруднения, жилищные проблемы, тяжелые заболевания близких людей, трудности с детьми, шантаж криминальных элементов и т.п. Чаще всего злоумышленник выявляет сотрудников, обладающих человеческими слабостями, которые можно развивать и использовать с пользой для его дела. Например: болтливость сотрудников, амбициозность, легкомыслие, стремление к развлечениями, любовь к незаработанным деньгам и другие качества, которые формируют безответственность и ведут к разглашению тайны фирмы.
В этом случае злоумышленник с успехом использует лесть, обещания, подарки, установление дружеских и близких отношений, одалживание денег и т.п. Он играет также на естественном стремлении сотрудника показаться более компетентным, осведомленным и значимым в делах фирмы, особенно если этот сотрудник находится в состоянии алкогольного опьянения или под действием наркотика, психотропного препарата. Но наиболее частой причиной разглашения секретов фирмы является обычная глупость сотрудника или его неумение оценивать ситуацию, незнание методов эффективного противодействия злоумышленнику, т.е. плохой подбор персонала и его необученность.
В результате незнания правил защиты информации конфиденциальная информация несанкционированно разглашается на общедоступных научных семинарах, выставках, официальных и неофициальных встречах и презентациях, особенно коллегам по профессии и журналистам. Очень опасны лица, уволенные из фирмы и владеющие ее конфиденциальной информацией.
Следовательно, даже поверхностный анализ некоторых способов добывания конфиденциальной информации, которые используют злоумышленники при содействии персонала, показывает, что система защиты секретов фирмы должна прежде всего основываться на тщательном отборе персонала, анализе его личных и моральных качеств, обучении сотрудников правилам защиты информации и противодействия злоумышленникам, создании в фирме здорового психологического климата, воспитании у сотрудников фирменной гордости.

4.3. Особенности приема и перевода сотрудников на работу, связанную с владением конфиденциальной информацией

Процессу приема сотрудника на работу предшествует ряд подготовительных этапов, которые позволяют составить точное представление о том, какой специалист и какой квалификации действительно нужен для данной должности, какими деловыми, моральными и личными качествами он должен обладать. Особенно это касается должностей, связанных с владением конфиденциальной информацией. Можно выделить следующие этапы:
• предварительно сформулировать, какие функции должен выполнять сотрудник, каков круг его ответственности, какие качества, знания и уровень квалификации необходимо иметь претенденту;
• составить перечень ценных и конфиденциальных сведений, с которыми будет работать специалист;
• составить перечень форм поощрения и стимулирования, которые может получать сотрудник;
• составить другие перечни вопросов, которые необходимо будет решать специалисту, перечни его личных качеств, возрастных, профессиональных и иных характеристик;
• составить описание должности — документ аналогичный по структуре должностной инструкции, который определяет требования к кандидату на должность (но это документ — вспомогательный).
Выполнение указанных этапов облегчит процедуру подбора кандидатов и сделает отбор их более обоснованным и объективным. Кандидаты предварительно знакомятся с указанными выше документами, что делает собеседование с ними более целенаправленным и конкретным. Кроме того, ознакомившись с документами, кандидат может отказаться от предлагаемой работы. Описание вакантной должности имеет для работодателя примерно такое же значение, как и резюме для кандидата.
Поиск кандидата на вновь создаваемую или вакантную должность в фирме не должен носить бессистемный характер. Случайный человек, пришедший с улицы, в определенной степени таит опасность для фирмы как с точки зрения его профессиональной

пригодности, так и личных, моральных качеств. Особую опасность подобный метод подбора представляет для должностей, связанных с владением конфиденциальной информацией или материальными ценностями. Случайные претенденты на должность обычно рассылают или разносят по предприятиям, учреждениям и фирмам свое резюме. Им не важно, где работать, их просто интересует работа по данной специальности.
С другой стороны, случайный человек не всегда плох и поэтому данный метод при подборе персонала является наиболее распространенным и объективно завоевал право на существование. Но дело в том, что он не Должен быть единственным.
Помимо пассивного ожидания прихода нужного человека, существует ряд эффективных направлений активного поиска кандидатов на вакантную должность или рабочее место. К числу основных направлений можно отнести следующие:
1. Поиск, кандидатов внутри фирмы, особенно если речь идет о руководителе или специалисте высокого уровня. Этот метод дает возможность продвигать перспективных работников по служебной лестнице и заинтересовывать их работой, воспитывать преданность делам фирмы. Можно приглашать на должность лицо, ранее работавшее в фирме и хорошо себя зарекомендовавшее.
Перераспределение персонала в соответствии с его склонностями и способностями всегда дает большой положительный эффект в улучшении работы фирмы и обеспечении ее информационной безопасности. Но надо учитывать, что поддерживается коллективом только такое продвижение по службе, которое определяется высокими деловыми качествами работника. Не может получить одобрения персонала выдвижение плохого работника, в частности по принципу личных связей или знакомства.
Большим преимуществом этого метода является то, что о кандидате достаточно много известно всему коллективу и судить о профессиональных, моральных и личных качествах, соответствии предлагаемой должности можно на основании достаточно обширного опыта.
Метод имеет недостаток, который состоит в том, что без притока новых людей коллектив теряет свои новаторские качества. Новые люди — это новые идеи, предложения и перспективы развития. Тем не менее этот метод является наилучшим и наиболее надежным при подборе кандидата на должность, связанную с владением ценной и конфиденциальной информацией.
2. Поиск кандидатов среди студентов и выпускников учебных заведений, установление связей с подразделениями вузов, занятыми трудоустройством выпускников. Можно иметь достаточно полную информацию о профессиональных и личных качествах студентов. Очень эффективно вести поиск (даже на средних курсах) наиболее способных студентов, привлекать их в процессе учебы к работе в организации, отплачивать их труд и, может быть, финансировать обучение в вузе, платить стипендию. Коллектив фирмы должен регулярно омолаживаться. Это лекарство от застоя идей, путь к успеху.
3. Обращение в государственные и частные бюро, агентства по найму рабочей силы, биржи труда, организации по трудоустройству лиц, уволенных по сокращению штатов, трудоустройству молодежи, бывших военнослужащих и т.п. Подобные агентства предлагают требуемый контингент работников на имеющиеся рабочие места, ведут целенаправленный поиск необходимого специалиста высокой квалификации, организуют переподготовку специалистов по индивидуальным заказам.
При обращении в агентство необходимо составить перечень служебных обязанностей и требований к нужному работнику, без указания конфиденциальных сведений, с которыми будет связана работа.
4. Рекомендации работающих в фирме сотрудников. Обычно такие рекомендации отличаются ответственным и взвешенным характером, так как с рекомендуемыми людьми сотрудникам придется работать вместе.
Указанные направления поиска кандидатов на должности, связанные с владением конфиденциальной информацией, как правило, позволяют выбрать необходимых работников из ряда лиц, изъявивших желание занять вакантную должность.
Технологическая цепочка приема сотрудников, работа которых связана с владением ценной и (или) конфиденциальной информацией, включает следующие процедуры:
• подбор предполагаемого кандидата (кандидатов) для приема на работу или перевода, получение резюме;
• изучение резюме (и личного дела, если кандидат работает на фирме) руководством фирмы, структурного подразделения и службой персонала, вызов для беседы подходящих

кандидатов;
• информирование кандидатов, работающих в фирме, об их будущих должностных обязанностях, связанных с владением тайной фирмы;
• знакомство (предварительное собеседование) руководства фирмы, структурного подразделения и службы персонала с кандидатами, не работающими в фирме; беседа с ними, уточнение отдельных положений резюме; ответы на вопросы о будущей работе; изучение полученных от кандидата рекомендательных писем;
• заполнение кандидатами, не работающими в фирме, и представление в отдел кадров заявления о приеме, автобиографии, личного листка по учету кадров (с цветной фотокарточкой), копий документов об образовании, наличии ученых степей, ученых и почетных званий, передача в отдел кадров рекомендательных писем и при наличии характеристик;
• обновление материалов личного дела работающего в фирме сотрудника; получение представления о переводе на новую должность от руководителя структурного подразделения;
• собеседование кандидатов с работником отдела кадров по представленным документам, при необходимости подтверждение тех или иных сведений представлением дополнительных документов;
• опрос сотрудником отдела кадров авторитетных для фирмы лиц, лично знающих кандидата на должность, протоколирование опроса;
• собеседование экспертов с кандидатами с целью определения их личных и моральных качеств, а для неработающих в фирме сотрудников дополнительно — профессиональных способностей; рассмотрение медицинской справки;
• при необходимости — тестирование и анкетирование кандидатов;
• по совокупности собранных материалов и их анализа принятие решения руководством фирмы об отборе единственного претендента и возможности предложить ему работу, связанную с владением тайной фирмы;
• заключительное собеседование с претендентом на должность, получение от него принципиального согласия на работу с конфиденциальной информацией;
• в случае согласия — подписание претендентом обязательства о неразглашении тайны фирмы, в частности, сообщаемых ему конфиденциальных сведений; информирование претендента о характере конфиденциальной информации, с которой он будет работать, наличии системы защиты этой информации и тех ограничениях, которые придется учитывать работнику в служебной и неслужебной обстановке;
• беседа-инструктаж руководителя структурного подразделения, руководителя службы безопасности и сотрудника службы персонала с претендентом на должность; ознакомление претендента с должностной инструкцией, рабочими технологическими инструкциями, инструкцией по обеспечению информационной безопасности фирмы и другими аналогичными материалами;
• составление проекта контракта, содержащего пункт об обязанности работника не разглашать конфиденциальные сведения фирмы;
• подписание контракта о временной работе без права доступа к конфиденциальной информации;
• составление и подписание приказа о приеме на работу с испытательным сроком (или на временную работу);
• заведение личного дела на вновь принятого сотрудника;
• заполнение на сотрудника необходимых учетных форм, в том числе личной карточки формы Т-2;
• внесение фамилии сотрудника в первичные учетные бухгалтерские документы;
• внесение соответствующей записи в трудовую книжку сотрудника;
• изучение личных, моральных и профессиональных качеств сотрудника в течение испытательного срока;
• обучение сотрудника правилам работы с конфиденциальной информацией и документами, инструктажи, проверка знаний;
• анализ результатов работы сотрудника в течение испытательного срока, составление нового контракта о длительной работе и издание соответствующего приказа или отказ сотрудника в работе;
• оформление допуска сотрудника к конфиденциальной информации и документам.
Предоставленный комплект документов, из которых в дальнейшем будет сформировано

личное дело сотрудника, является предметом тщательного изучения руководителями фирмы, структурного подразделения, коллегиального органа управления и службы персонала при решении вопроса о назначении данного лица на должность.
Изучение документов не должно носить формально-бюрократический характер и быть единственным критерием в решении вопроса о назначении данного лица на должность. Изучение документов следует сочетать с объективным анализом нескольких личностей, претендующих на должность, сопоставлением результатов собеседований, тестирования, опросов и т.п. Все это в совокупности позволит на конкурсной или неконкурсной основе правильно провести отбор именно того претендента на должность, который более всего отвечает составленным ранее требованиям.
Предоставленные кандидатом персональные документы тщательно проверяются на достоверность: соответствие фамилий, имен и отчеств, других персональных данных, наличие необходимых отметок и записей, идентичность фотокарточки и личности гражданина (на фотографии очки, парик — только при постоянной носке), соответствие формы бланка годам их использования, отсутствие незаверенных подчисток, исправлений, попыток замены листов, фотографий, соответствие и качество печатей и т.п. При каких-то сомнениях кандидата просят представить дубликаты испорченных документов, заверить исправления. Сведения, включенные в характеристики, рекомендательные письма, списки научных трудов и изобретений, выданные и заверенные другими учреждениями, могут быть проверены Путем обращения в эти учреждения. Документы, явно недостоверные, могут быть возвращены гражданину, и одновременно ему отказывается в рассмотрении вопроса о приеме на работу без объяснения причины отказа. Сведения, указываемые в резюме, не проверяются.
Заявление о назначении (переводе) на должность, личный листок по учету кадров, автобиография пишутся или заполняются гражданином собственноручно, без использования пишущей машинки или принтера.
Все записи, сделанные в личном листке по учету кадров, и текст автобиографии сравниваются сотрудником отдела кадров с персональными документами. Неподтвержденные записи, на которых настаивает гражданин, дополняются записью сотрудника отдела кадров «со слов гражданина». Исправления в указанных документах не допускаются.
Копии с аттестатов, дипломов, свидетельств, грамот и т.п., которые приобщаются к документам для решения вопроса о приеме на работу, снимаются с помощью копировальной техники в отделе кадров и заверяются сотрудником отдела. Копии, принесенные гражданином, внимательно сличаются с подлинником и также заверяются этим сотрудником. Нотариального заверения копий не требуется. Запрещается заверение копий с копии.
Паспорт, военный билет, дипломы, аттестаты и другие подобные персональные документы после работы с ними сотрудника отдела кадров возвращаются гражданину (кроме трудовой книжки).
При подборе персонала для работы с ценной или конфиденциальной информацией следует в первую очередь обращать внимание на личные и моральные качества кандидатов на должность, их порядочность и лишь затем — на их профессиональные знания, умения и навыки.
Важно уже на первых этапах отбора исключить те кандидатуры, которые по формальным признакам явно не соответствуют требованиям, предъявляемым к будущему сотруднику.
Собеседования с кандидатами на должность преследуют следующие цели:
• выявить реальную причину желания работать в данной фирме;
• выявить возможных злоумышленников или попытаться увидеть слабости кандидата как человека, которые могут провоцировать преступные действия;
• убедиться, что кандидат не намерен использовать в работе секреты фирмы, в которой он раньше работал;
• убедиться в добровольном согласии кандидата соблюдать правила защиты информации и иметь определенные ограничения в профессиональной и личной жизни. Вопросники для собеседования составляются таким образом, чтобы выяснить:
• причины увольнения кандидата с прежнего места работы;
• источник информации о вакансии в данной фирме — кто подсказал, кто рекомендовал и т.п.;
• работал ли кандидат ранее с конфиденциальной информацией, подписывал ли

обязательство о ее неразглашении;
• возникшие сомнения, появившиеся в связи с изучением документов кандидата;
• отношения в семье, уровень благосостояния кандидата, жилищные условия, культурный уровень и т.п.
Ответы кандидата фиксируются, и те из них, которые вызвали сомнения, уточняются путем опроса знающих кандидата лиц, путем тестирования и другими способами (если это необходимо).
При приеме на работу, связанную с информацией особой предпринимательской важности, для сбора полных сведений о кандидате могут привлекаться работники частных детективных агентств.
Одной из главных задач собеседования и тестирования является выявление несоответствия мотиваций в различных логических группах вопросов. Например: несоответствие — хочет получать большую зарплату, но раньше он получал столько же, работал близко от дома, а хочет работать в фирме, находящейся на значительном расстоянии, и т.п.
С точки зрения безопасности психологический отбор преследует следующие цели:
• выявление имевших ранее место судимостей, преступных связей, криминальных наклонностей;
• определение возможных преступных склонностей, предрасположенности кандидата к совершению противоправных действий, дерзких и необдуманных поступков в случае формирования в его окружении определенных обстоятельств;
• установление факторов, свидетельствующих о морально-психологической ненадежности, неустойчивости, уязвимости кандидата и т.д.
По мнению многих специалистов-психологов, основные личные качества, которыми должен обладать потенциальный сотрудник, включают:
• порядочность, честность, принципиальность и добросовестность;
• исполнительность, дисциплинированность;
• эмоциональная устойчивость (самообладание);
• стремление к успеху и порядку в работе;
• самоконтроль в поступках и действиях;
• правильная самооценка собственных возможностей и способностей;
• умеренная склонность к риску;
• умение хранить секреты;
• тренированное внимание;
• хорошая память, способности к сравнительной оценке фактов и т.д. Личные качества, не способствующие сохранению секретов:
• эмоциональная неуравновешенность;
• разочарование в себе и своих способностях;
• отчуждение от коллег по работе;
• недовольство своим служебным положением;
• ущемленное самолюбие;
• крайне эгоистическое поведение;
• отсутствие достаточного благоразумия;
• нежелание и неспособность защищать информацию;
• нечестность;
• финансовая безответственность;
• употребление наркотиков;
• отрицательное воздействие алкоголя, приводящее к болтливости, необдуманным поступкам и т.д.
Не следует думать, что психологический отбор полностью заменяет прежние, достаточно надежные кадровые процедуры (анализ документов, собеседование, опросы сослуживцев и лиц, знающих кандидата, оперативная проверка в правоохранительных органах и т.д.). Только при умелом сочетании традиционных и психологических кадровых методов анализа можно с определенной степенью достоверности прогнозировать поведение сотрудников в различных, в том числе экстремальных, ситуациях.
Обычно отобранным для работы считается кандидат, у которого результаты анализа документов, собеседований, проверок, тестов и психологического изучения не противоречат друг другу, и не содержат данных, которые препятствовали бы приему на работу.

Материалы проверок и анализа кандидатов на должность (в том числе вопросники и протоколы собеседований, заполненные тесты, а также используемые виды тестов и «ключи» к тестам, тестовые нормы, инструкции по проведению и интерпретации и другие подобные материалы) являются строго конфиденциальной информацией.
Обязательство о неразглашении конфиденциальной информации и сохранении тайны фирмы претендент подписывает до того, как ему будет сообщен состав ценных сведений, с которыми ему предстоит работать, и порядок защиты этих сведений.
Обязательство (подписка, соглашение) о неразглашении конфиденциальных сведений представляет собой правовой документ, которым претендент добровольно и письменно дает согласие на ограничение его прав в отношении использования конфиденциальной информации. Одновременно в обязательстве претендент предупреждается об ответственности за разглашение этой информации.
Например:
Договорное обязательство. Обязуюсь:
1. В период оформления на работу и работы в _____ не разглашать сведения, составляющие ее коммерческую тайну, которые мне будут доверены или станут известны при исполнении обязанностей, собеседованиях, инструктировании и обучении.
2. Беспрекословно и аккуратно выполнять относящиеся ко мне требования приказов, инструкций и положений по защите коммерческой тайны, с которой я ознакомлен.
3. Не сообщать устно, письменно или иным способом кому бы то ни было сведений, составляющих тайну.
4. В случае отказа от работы, окончания работы или увольнения не разглашать и не использовать для себя и других лиц сведений, составляющих тайну _____.
Я предупрежден, что в случае нарушения данного обязательства должен возместить причиненный _____ ущерб или буду привлечен к дисциплинарной (вплоть до увольнения) или другой ответственности в соответствии с действующим законодательством.
Проинструктировал (подпись). Подпись лица, принимающего обязательство. Дата.
Текст обязательства может заканчиваться фразой об ознакомлении лица с его содержанием и добровольном согласии выполнять все пункты.
Многие американские фирмы включают в соглашение (обязательство) следующие пункты:
• детальное изложение принципов определения конкретных сведений, составляющих тайну фирмы;
• краткое изложение порядка охраны конфиденциальных сведений;
• изложение мер, которые должен принимать сам работник для обеспечения сохранности этих сведений;
• перечень административных наказаний, которым может быть подвергнут работник, разгласивший сведения, составляющие тайну фирмы (увольнение, понижение в должности, перевод на другую работу и т.п.).
Хорошо, если обязательство содержит пункт о том что сотрудник не будет использовать в своей деятельности информацию, принадлежащую на правах собственности фирме, в которой он ранее работал. Подобные обязательства подписывают не только претенденты на работу в данной фирме, но и все лица, тем или иным образом участвующие в работе фирмы и потенциально имеющие возможность узнать элементы тайны фирмы, например акционеры, поставщики, сотрудники работающих с фирмой рекламных и торговых структур, эксперты и т.п. Подписание обязательства о неразглашении тайны фирмы следует предусмотреть для служащих фирмы, которые не имеют непосредственного отношения к закрытым сведениям, однако имеют возможность ознакомиться с ними при исполнении служебных обязанностей (шоферы, дворники, уборщицы, сотрудники охраны и др.).
Считается, что обязательство о неразглашении тайны фирмы не дает полной гарантии сохранения этих сведений, однако, как показывает практика, существенно снижают риск разглашения персоналом или иными лицами этих сведений, риск незаконного их использования, а также число попыток конкурентов внедрить на фирму свою агентуру.
После подписания обязательства и проведения беседы-инструктажа с претендентом заключается трудовой договор (контракт). В контракте должен быть пункт об обязанности работника не разглашать сведения, составляющие тайну фирмы, а также конфиденциальные сведения партнеров и клиентов, об обязательстве соблюдать правила защиты конфиденциальных сведений. Может быть пункт о собственности фирмы на результаты работы сотрудника, на сделанные им изобретения и открытия и согласие

сотрудника на публикацию этих достижений только с разрешения руководства фирмы. Часто содержится пункт об обязанности сотрудника сообщать в службу безопасности о всех попытках посторонних лиц получить у него конфиденциальную информацию. В обязательном порядке включается пункт об обязанности сотрудника немедленно сообщать непосредственному руководителю и службе безопасности об утере носителей конфиденциальной информации, документов, дел, конфиденциальных материалов, изделий и т.п.

В заключительной части указывается степень ответственности за разглашение тайны фирмы или несоблюдение правил защиты информации. Обычно это расторжение трудового договора, при необходимости — последующее судебное разбирательство.

Отличительной особенностью индивидуальных трудовых соглашений от трудовых договоров (контрактов) в части сохранения коммерческой тайны является то, что в трудовых соглашениях должны быть указаны конкретные сведения, составляющие предпринимательскую тайну фирмы и доверенные сотруднику в связи с выполнением им работы, а также конкретные меры со стороны сотрудника по обеспечению сохранения этих сведений.

После подписания приказа о приеме на работу в отделе кадров формируется личное дело сотрудника, включающее стандартный набор документов.

Материалы, связанные с профессиональным и психологическим анализом данного работника (протоколы собеседований, тесты, протоколы бесед и опросов и т.п.) подшиваются в дело кадровой службы «Материалы по приему сотрудников на работу», но не в личное дело сотрудника. Дело с материалами имеет гриф конфиденциальности «Строго конфиденциально».

Вести какие-либо досье на сотрудников, содержащие сведения, полученные неофициальным путем, запрещается.

После получения допуска к конфиденциальной информации сотрудник в индивидуальном порядке должен быть обучен правилам работы с документами, базами данных, которые будут ему предоставлены. Результат обучения фиксируется в обязательстве или контракте. Отметка заверяется подписями руководителя службы безопасности и сотрудника.

Следовательно, усложненные процедуры приема на работу, связанную с владением конфиденциальной информацией, и проверки достоверности сведений, указанных в документах, дают возможность всесторонне оценить кандидата на должность. С другой стороны, они дают возможность руководству фирмы и самому кандидату оценить ситуацию и без спешки принять правильное решение. Методы психологического анализа, проводимые одновременно с хорошо зарекомендовавшими себя приемами анализа документов претендента на должность, позволяют сделать достаточно обоснованные выводы о пригодности данного лица для замещения вакантной должности, связанной с владением конфиденциальной информацией. Следует учитывать, что использование только психологических методов анализа личности не дает достоверного результата и может иметь лишь рекомендательный характер.

4.4. Доступ персонала к конфиденциальным сведениям, документам и базам данных

Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных является одной из центральных проблем системы защиты информации. Регламентация порядка доступа лежит в основе режима конфиденциальности проводимых фирмой работ. Важно четко и однозначно определить: кто, кого, к каким сведениям, когда и как допускает.

Режим представляет собой совокупность ограничительных правил, мероприятий, норм, обеспечивающих контролируемый доступ на определенную территорию, в помещения, к информации и документам. Любой режим базируется на так называемой разрешительной системе. Разрешительная система в общем виде предусматривает необходимость получения специального разрешения на осуществление соответствующих правовых мероприятий, например на въезд в пограничную зону, на посещение воинской части и т.п.

Разрешительная (разграничительная) система доступа в сфере коммерческой тайны представляет собой совокупность правовых норм и требований, устанавливаемых первым руководителем или коллективным органом руководства фирмой с целью обеспечения правомерного ознакомления и использования сотрудниками фирмы конфиденциальных сведений, необходимых им для выполнения служебных обязанностей.

Принципы построения разрешительной системы доступа:

• надежность, т.е. относительное исключение возможности несанкционированного доступа посторонних лиц к документам в обычных и экстремальных условиях;

• полнота охвата всех категорий исполнителей и всех категорий документов, информации на любых носителях;

• конкретность, т.е. исключение двоякого толкования и однозначность решения о доступе;

• производственная необходимость как единственный критерий доступа исполнителя к документу, а также доступа к документам представителей государственных служб;

• определенность состава и компетенции должностных лиц, дающих разрешение на доступ исполнителя к конфиденциальным сведениям, документам и базам данных, исключение возможности бесконтрольной и несанкционированной выдачи таких разрешений;

• строгая регламентация порядка работы всех категорий сотрудников фирмы с информацией, документами и базами данных. Разрешительная система решает следующие задачи:

• ограничения и регламентации состава сотрудников, функциональные обязанности которых требуют знания тайны фирмы и работы с ценными документами;

• строгого избирательного и обоснованного распределения документов и информации между сотрудниками;

• обеспечения сотрудника всем необходимым для реализации своих служебных функций (документами, делами, базами данных, информацией, техническими средствами и т.д.);

• беспрепятственного прохода сотрудника в здание фирмы, в конкретное рабочее помещение (режимную зону), к выделенному ему офисному рабочему оборудованию и компьютеру;

• исключение возможности для посторонних лиц несанкционированного ознакомления с конфиденциальной информацией в процессе работы сотрудника с документами, делами и базами данных;

• рациональное размещение рабочих мест сотрудников, при котором исключалось бы бесконтрольное использование сотрудником защищаемой информации (коллективный контроль за работой сотрудников). Разрешительная система включает в себя две составные части:

допуск сотрудника к конфиденциальной информации и непосредственный доступ этого сотрудника к конкретным сведениям.

Под допуском понимается процедура оформления права сотрудника фирмы или иного лица на доступ к сведениям (информации) ограниченного распространения и одновременно правовой акт согласия (разрешения) собственника (владельца) информации на передачу ее для работы конкретному лицу.

Оформление допуска, т.е. согласия лица на определенные ограничения в использовании информации, всегда носит добровольный характер. Наличие допуска предоставляет сотруднику формальное право работать со строго определенным кругом конфиденциальных документов, баз данных и отдельных сведений.

Как отмечалось выше, к конфиденциальной информации допускаются, как правило, лица, проработавшие в фирме определенное время и зарекомендовавшие себя с положительной стороны.

В предпринимательских структурах разрешение на допуск дает первый руководитель фирмы. Разрешение оформляется соответствующим пунктом в контракте (трудовом договоре). Допуск может оформляться приказом первого руководителя с указанием типового состава сведений, с которыми разрешается работать данному сотруднику или группе сотрудников. Допуск может носить временный характер на период выполнения определенной работы и пересматриваться при изменении профиля работы сотрудника.

Законодательством США предусмотрено, что никто не имеет права иметь допуск к засекреченной информации лишь благодаря своему чину или положению. Конечной инстанцией, решающей вопрос о необходимости допуска данному лицу, является руководитель, который распоряжается этой информацией и осуществляет за ней контроль.

Доступ — практическая реализация каждым сотрудником предоставленного ему допуском права на ознакомление и работу с определенным составом конфиденциальных сведений, документов и баз данных. Он санкционируется полномочным должностным лицом (первым руководителем, его заместителем, руководителем подразделения, службы или

направления деятельности) в отношении конкретной информации и конкретного сотрудника. Право на выдачу такого разрешения строго регламентируется.
Разрешение (санкция) на доступ к конкретной информации может быть дано при соблюдении следующих условий:
• наличие подписанного приказа первого руководителя о приеме на работу (переводе, временном замещении, изменении должностных обязанностей и т.п.) или назначении на должность, в функциональную структуру которой входит работа
• с данной, конкретной информацией;
• наличие подписанного сторонами трудового договора (контракта)» имеющего пункт о сохранении тайны фирмы и подписанного обязательства о неразглашении ставших известными конфиденциальных сведений и соблюдении правил их защиты;
• соответствие функциональных обязанностей сотрудника передаваемым ему документам и информации;
• знание сотрудником требований нормативно-методических документов по защите информации и сохранении тайны фирмы;
• наличие необходимых условий в офисе для работы с конфиденциальными документами и базами данных;
• наличие систем контроля за работой сотрудника.
Особенность информационного обслуживания потребителей конфиденциальной информации заключается в том, что вопросы определения состава необходимой им информации решаются полномочным руководителем, а не самими потребителями. Существует общее, обязательное правило: исполнители, которым документ не адресован руководителем, не только не имеют права доступа к нему, но и не должны знать о существовании такого документа и исходных данных о нем.
Структура процедуры разграничения доступа должна быть многоуровневой, иерархической. Иерархическая последовательность доступа к информации реализуется по принципу «чем выше уровень доступа, тем уже круг допущенных лиц», «чем выше ценность сведений, тем меньшее число сотрудников может их знать». В фирме может составляться схема выдачи разрешений на доступ к массовой конфиденциальной информации. Такая схема разрабатывается с учетом двух аспектов: а) выдача разрешений в зависимости от категорий документов и б) выдача разрешений в зависимости от занимаемой должности. Графы схемы: категории документов, должностные лица, дающие разрешение, категории исполнителей, кому дается разрешение. В схеме отражаются также категории документов, с которыми знакомятся определенные категории исполнителей без специального разрешения.
Может составляться матрица полномочий, в которой по горизонтали — наименования категорий документов, по вертикали — фамилии или должности сотрудников.
Всю конфиденциальную информацию фирмы может знать только первый руководитель фирмы. Конфиденциальную информацию по конкретной работе в полном объеме вправе получать лишь соответствующий заместитель первого руководителя, руководители структурных подразделений или направлений деятельности по специальному перечню, утвержденному первым руководителем.
Необходимо добиваться минимизации для персонала привилегий по доступу к информации. При сбое в системе защиты информации или обнаружении факта утраты информации должно мгновенно вводиться ограничение на доступ или прекращение доступа к любой конфиденциальной информации до окончания служебного расследования.
Разграничение доступа основывается на однозначном расчленении информации по тематическим группам, уровням конфиденциальности этих групп и пользователям, которым эта информация необходима для работы. Задачей процедуры разграничения доступа является регламентация минимальных потребностей персонала в конфиденциальных сведениях.
Это дает возможность разделить знание элементов коммерческой тайны среди как можно большего числа сотрудников. Например, желательно, чтобы целиком идею, формулу, конструкцию не знал никто, каждый знал бы лишь свою незначительную часть. Дробление информации также не позволяет конкурентам использовать ее за счет прима на работу уволенного из фирмы сотрудника.
При составлении конфиденциального документа следует учитывать, что его содержание не только определяет функциональное назначение документа, но и лежит в основе разрешительной процедуры доступа персонала к данному документу. Поэтому документ

необходимо посвящать только одной тематической группе вопросов, предназначенной, по возможности, одному конкретному исполнителю или структурному подразделению.
В соответствии с иерархической последовательностью доступа определяется структура рубежей защиты информации, которая предусматривает постепенное ужесточение защитных мер по иерархической вертикали возрастания уровня конфиденциальности сведений.
Этим обеспечивается недоступность этих сведений для случайных людей, злоумышленника и определяется необходимый уровень защищенности информации.
Разрешение на доступ к конфиденциальным сведениям строго персонифицировано, т.е. руководители несут персональную ответственность за правильность выдаваемых ими разрешений на доступ исполнителей к конфиденциальным сведениям, а лица, работающие с конфиденциальными документами, несут персональную ответственность за сохранение в тайне их содержания, сохранность носителя и соблюдение установленных правил работы с документами.
Руководитель фирмы имеет право давать разрешение на ознакомление со всеми видами конфиденциальных документов фирмы и всем категориям исполнителей и другим лицам. Однако целесообразно, чтобы первый руководитель оставлял за собой право распоряжаться только наиболее ценной информацией, делегируя право выдачи разрешений на доступ к другой информации нижестоящим руководителям. Следует иметь в виду, что чрезмерная централизация в выдаче разрешений на доступ к конфиденциальной информации неизбежно ведет к снижению оперативности в решении производственных вопросов. Излишняя децентрализация и либерализация создает условия для утраты ценных сведений.
Заместители первого руководителя по функциональным сферам (по науке, производственным вопросам, сбыту и др.) имеют право давать разрешение на ознакомление с конфиденциальными сведениями всем нижестоящим руководителям и исполнителям, но в пределах своей компетенции.
Руководителям структурных подразделений дается право разрешать доступ к конфиденциальным сведения всем работникам своих подразделений по тематике их работы. Руководитель подразделения может давать разрешение только непосредственно подчиненным ему сотрудникам. Для осуществления доступа к документам данного подразделения работника другого подразделения необходимо разрешение соответствующего заместителя руководителя фирмы.
Ответственные исполнители работ (направлений деятельности) имею право давать разрешение на доступ к конфиденциальной информации подчиненным им исполнителям и в пределах их компетенции. В небольших фирмах разрешение на доступ дает только первый руководитель.
Представителям государственных органов разрешение на доступ к конфиденциальным сведениям дает только первый руководитель фирмы. При необходимости доступа к конфиденциальным сведения представителей других фирм и предприятий руководствуются теми обязательствами, которые были закреплены в соответствующем договоре (контракте) на выполнение работ или услуг. Это касается как документированной информации, так и информации устной, визуальной и любой другой. В этом случае разрешение на доступ дает должностное лицо фирмы, включенное в специальный перечень, прилагаемый к договору и утвержденный первым руководителем.
Руководитель фирмы, вне зависимости от формы ее собственности, может устанавливать иные специальные или дополнительные правила доступа к конфиденциальным сведениям, документам, базам данных и носителям информации, конфиденциальным изделиям и продукции фирмы. Он несет за это единоличную ответственность.
Разрешение на доступ к конфиденциальной информации всегда дается полномочным руководителем только в письменном виде: резолюцией на документе, приказом, утверждающим схему именного или должностного доступа к конкретным группам информации, утвержденным руководителем списком-разрешением на обложке дела, списком ознакомления с документом и т.п.
Без дополнительного разрешения допускаются к документам: их исполнители (если они продолжают работать по той же тематике) и лица, визировавшие, подписавшие, утвердившие документ. Без специального разрешения могут допускаться также лица, указанные в тексте распорядительных документов. Если сотрудник допускается только к части документа, то в разрешении (резолюции) четко указываются конкретные пункты, разделы, страницы, приложения, с которыми он может ознакомиться. Сотрудник службы

конфиденциальной документации (КД) обязан принять необходимые меры по исключению возможности ознакомления исполнителя с другими частями документа.
Разрешение на доступ к конфиденциальным сведениям представителя другой фирмы или предприятия оформляется резолюцией полномочного должностного лица на предписании (или письме, обязательстве), представленном заинтересованным лицом. В резолюции должны быть указаны конкретные документы или сведения, к которым разрешен доступ. Одновременно указывается фамилия сотрудника фирмы, который знакомит представителя другого предприятия с этими сведениями и несет ответственность за его работу - в помещении фирмы.
Следует соблюдать правило, по которому регистрируются все лица, имеющие доступ к определенным документам, коммерческим секретам. Это позволяет на высоком уровне осуществлять информационное обеспечение аналитической работы по выявлению возможных каналов утраты информации.
При организации доступа сотрудников фирмы к конфиденциальным массивам электронных документов, базам данных необходимо помнить о его многоступенчатом характере. Можно выделить следующие главные составные части:
• доступ к персональному компьютеру, серверу или рабочей станции;
• доступ к машинным носителям информации, хранящимся вне ЭВМ;
• непосредственный доступ к базам данных и файлам.
Доступ к персональному компьютеру, серверу или рабочей станции, которые используются для обработки конфиденциальной информации, предусматривает:
• определение и регламентацию первым руководителем фирмы состава сотрудников, имеющих право доступа (входа) в помещение, в котором находится соответствующая вычислительная техника, средства связи;
• регламентацию первым руководителем временного режима нахождения этих лиц в указанных помещениях; персональное и временное протоколирование (фиксирование) руководителем подразделения или направления деятельности фирмы наличия разрешения и периода работы этих лиц в иное время (например, в вечерние часы, выходные дни и др.);
• организацию охраны этих помещений в рабочее и нерабочее время, определение правил вскрытия помещений и отключения охранных технических средств информации и сигнализирования; определение правил постановки помещений на охрану; регламентацию работы указанных технических средств в рабочее время;
• организацию контролируемого (в необходимых случаях пропускного) режима входа в указанные помещения и выхода из них;
• организацию действий охраны и персонала в экстремальных ситуациях или при авариях техники и оборудования помещений;
• организацию выноса из указанных помещений материальных ценностей, машинных и бумажных носителей информации; контроль вносимых в помещение и выносимых персоналом личных вещей.
Несмотря на то, что по окончании рабочего дня конфиденциальные сведения должны быть перенесены на гибкие носители и стерты с жесткого диска компьютера, помещения, в которых находится вычислительная техника, подлежат охране. Объясняется это тем, что, во-первых, в неохраняемый компьютер легко установить какое-либо средство промышленного шпионажа, во-вторых, злоумышленник может с помощью специальных методов восстановить стертую конфиденциальную информацию на жестком диске (произвести «уборку мусора»).
Доступ к машинным носителям конфиденциальной информации, хранящимся вне ЭВМ, предполагает:
• организацию учета и выдачи сотрудникам чистых машинных носителей информации;
• организацию ежедневной фиксируемой выдачи сотрудникам и приема от сотрудников носителей с записанной информацией (основных и резервных);
• определение и регламентацию первым руководителем состава сотрудников, имеющих право оперировать конфиденциальной информацией с помощью компьютеров, установленных на их рабочих местах, и получать в службе КД учтенные машинные носители информации;
• организацию системы закрепления за сотрудниками машинных носителей информации и контроля за сохранностью и целостностью информации, учета динамики изменения состава записанной информации;
• организацию порядка уничтожения информации на носителе, порядка и условий

физического уничтожения носителя;
• организацию хранения машинных носителей в службе КД в рабочее и нерабочее время, регламентацию порядка эвакуации носителей в экстремальных ситуациях;
• определение и регламентацию первым руководителем состава сотрудников не сдающих по объективным причинам технические носители информации на хранение в службу КД в конце рабочего дня, организацию особой охраны помещений и компьютеров этих сотрудников. Работа сотрудников службы КД и фирмы в целом с машинными носителями информации вне ЭВМ должна быть организована по аналогии с бумажными конфиденциальными документами.

Доступ к конфиденциальным базам данных и файлам является завершающим этапом доступа сотрудника фирмы к компьютеру. И если этот сотрудник — злоумышленник, то можно считать, что самые серьезные рубежи защиты охраняемой электронной информации он успешно прошел. В конечном счете он может просто унести компьютер или вынуть из него и унести жесткий диск, не «взламывая» базу данных.

Обычно доступ к базам данных и файлам подразумевает:
• определение и регламентацию первым руководителем состава сотрудников, допускаемых к работе с определенными базами данных и файлами; контроль системы доступа администратором базы данных;
• именование баз данных и файлов, фиксирование в машинной памяти имен пользователей и операторов, имеющих право доступа к ним;
• учет состава базы данных и файлов, регулярную проверку наличия, целостности и комплектности электронных документов;
• регистрацию входа в базу данных, автоматическую регистрацию имени пользователя и времени работы; сохранение первоначальной информации;
• регистрацию попытки несанкционированного входа в базу данных, регистрацию ошибочных действий пользователя, автоматическую передачу сигнала тревоги охране и автоматическое отключение компьютера;
• установление и нерегулярное по сроку изменение имен пользователей, массивов и файлов (паролей, кодов, классификаторов, ключевых слов и т.п.), особенно при частой смене персонала;
• отключение ЭВМ при нарушениях в системе регулирования доступа или сбое системы защиты информации;
• механическое (ключом или иным приспособлением) блокирование отключенной, но загруженной ЭВМ при недлительных перерывах в работе пользователя. Коды, пароли, ключевые слова, ключи, шифры, специальные программные продукты, аппаратные средства и т.п. атрибуты системы защиты информации в ЭВМ разрабатываются, меняются специализированной организацией и индивидуально доводятся до сведения каждого пользователя работником этой организации или системным администратором. Применение пользователем собственных кодов не допускается.

Следовательно, процедуры допуска и доступа сотрудников к конфиденциальной информации завершают процесс включения данного сотрудника в состав лиц, реально владеющих тайной фирмы. С этого времени большое значение приобретает текущая работа с персоналом, в распоряжении которого находятся ценные и конфиденциальные сведения.

4.5. Текущая работа с персоналом, владеющим конфиденциальной информацией

По мнению большинства специалистов по безопасности информационных систем, главное внимание должно быть обращено на персонал, постоянно работающий с конфиденциальными документами и базами данных. Основными задачами должны быть две: 1) максимально затруднить работу злоумышленнику или его сообщнику по добыванию необходимой информации, противодействовать им в пассивном или активном режиме на основе результатов аналогичных выводов и 2) не допустить установления определенных взаимоотношений злоумышленника и сотрудника фирмы, владеющего конфиденциальной информацией.

Текущая работа с персоналом, обладающим конфиденциальной информацией, включает в себя:
• обучение и систематическое инструктирование сотрудников;
• проведение регулярной воспитательной работы с персоналом, работающим с конфиденциальными сведениями и документами;
• постоянный контроль за выполнением персоналом требований по защите конфиденциальной информации;

• контрольную работу по изучению степени осведомленности персонала в области конфиденциальных работ фирмы;
• проведение служебных расследований по фактам утечки информации и нарушений персоналом требований по защите информации;
• совершенствование методики текущей работы с персоналом.

Процесс обучения сотрудников фирмы правилам защиты информации должен быть постоянным, так как система защиты требует регулярного обновления и видоизменения. Занятия не должны превращаться в редкие, необязательные и формальные собрания.

Обучение сотрудника начинается с момента проведения собеседования с ним при приеме на работу и подписания им обязательства о неразглашении тайны и кончая моментом увольнения и подписания этим лицом обязательства о недопустимости использования конфиденциальных сведений в чьих-либо целях. Обучение сотрудников может начинаться также с момента начала работы коллектива над новой идеей, оцененной в качестве фирменного секрета, работы с использованием ноу-хау и т.п. Обычная периодичность обучения для работающих сотрудников один раз в 3—5 лет, как правило, после аттестации или перезаключения контракта.

Задачи обучения включают в себя изучение:
• характера и состава конфиденциальной информации;
• возможных угроз конфиденциальным сведениям, каналов их объективного распространения и каналов утраты, методов работы злоумышленников;
• структуры системы защиты, требований и правил защиты конфиденциальной информации;
• порядка работы сотрудников с конфиденциальными сведениями, документами и базами данных;
• действий персонала в конкретных экстремальных ситуациях.

Обучение сотрудников предполагает приобретение и поддержание на высоком уровне производственных навыков работы с конфиденциальными сведениями, психологическое воспитание сотрудников и воспитание глубокой убежденности в необходимости выполнения требований по защите любой конфиденциальной информации. Персонал должен получить знания по оценке важности тех или иных сведений для упрочения престижа фирмы и ее финансовой стабильности, а значит, и для благополучия каждого сотрудника.

Методика обучения включает в себя:
• специализированные программы обучения для обеспечения лекционных курсов и практических занятий;
• проведение лекций, семинаров и собеседований как общеознакомительного плана, так и по конкретным направлениям защиты; тестирование сотрудников;
• решение ситуационных задач, связанных с выполнением необходимых требований по защите конфиденциальной информации;
• практическую ситуационную учебу по действиям персонала в экстремальных ситуациях;
• проведение деловых игр, обучающих методам противодействия замыслам злоумышленника.

Очень важно сделать процесс обучения индивидуализированным. Он должен быть конкретизирован по должностному составу сотрудников, по типовым рабочим местам и часто — по отдельным сотрудникам. В процессе обучения сотрудник должен получить только те знания, которые ему необходимы для работы. Избыточности знаний в области состава конфиденциальной информации и способов ее защиты не должно быть. Отдельно от остального персонала обучаются сотрудники службы безопасности, секретарь-референт, сотрудники, работающие с особо ценными документами, делами и изделиями.

Информация, сообщаемая в процессе обучения сотрудников, является строго конфиденциальной. Конспекты, записи сотрудники делают в специальных тетрадях, хранящихся в соответствии с общим порядком работы с конфиденциальными документами.

По окончании обучения проводится проверка усвоения сотрудниками полученных знаний. Результаты проверки фиксируются в протоколе комиссии, ведущей проверку. Целесообразно организовывать проверку знаний путем тестирования или решения ситуационной задачи. Сотрудники, не прошедшие проверку знаний, от работы с конфиденциальной информацией отстраняются.

Одновременно с обучением должны проводиться регулярные совещания-инструктажи с сотрудниками. В процессе инструктажа:
• до сведения сотрудников доводятся изменения и дополнения, внесенные в действующие

нормативно-методические документы по защите информации, приказы и указания руководства фирмы в области защиты информации и информационной безопасности;
• сотрудники информируются о конкретных угрозах информации, о каналах утечки информации, действиях злоумышленников, принятых дополнительных мерах по защите информации;
• анализируются случаи нарушения правил защиты информации сотрудниками, сообщается о фактах утраты секретов по вине сотрудников.
Инструктаж, так же как и обучение, проводится индивидуально, информация, сообщаемая на инструктажах, разглашению не подлежит. Совещания-инструктажи проводятся, как правило, по необходимости.
Следовательно, обязательной и первостепенной частью текущей работы с персоналом должно стать обучение сотрудников правилам работы с конфиденциальной информацией, документами и базами данных. Трудно говорить об эффективности работы с персоналом, если сотрудники не имеют достаточно твердых представлений о системе защиты конфиденциальной информации, методах противодействия злоумышленникам.
Обучение и инструктаж находится в тесной связи с процессом воспитания сотрудников, направленным на то, чтобы привить им устойчивые мотивационные стереотипы поведения в той или иной ситуации, связанной с обеспечением недоступности информации посторонним лицам, исключением возможности несанкционированного доступа этих лиц к ценным и конфиденциальным сведениям.
Воспитание — это процесс систематического и целенаправленного воздействия на формирование и развитие личности в целях наиболее полного использования ее профессиональных способностей, деловых, высоких моральных и иных положительных качеств для деятельности фирмы, повышения ее благополучия и конкурентоспособности. Воздействие на личность осуществляется руководством фирмы в процессе обучения и инструктажа сотрудников, коллективом фирмы в процессе решения совместных производственных и иных задач и отдельными сотрудниками фирмы в неформальной обстановке.
Воспитательный процесс тесно связан с исследованием мотиваций в поведении человека. Функция мотивации поведения, мышления и действий персонала в различных ситуациях и жизненных обстоятельствах имеет существенное значение в управлении персоналом, особенно если его деятельность связана с владением ценными и конфиденциальными сведениями.
Мотивация деятельности человека понимается как совокупность движущих сил, побуждающих человека к осуществлению определенных действий. Эти силы находятся вне или внутри человека и заставляют его осознанно, или неосознанно совершать определенные поступки. В соответствии с этим текущая или профилактическая работа с персоналом является обязательной составной частью предотвращения попыток отдельных сотрудников воспользоваться в личных целях ценной для фирмы информацией, нарушить требования обеспечения информационной безопасности фирмы. Каждый из сотрудников фирмы, работающий с закрытыми сведениями, документами и базами данных, должен находиться под постоянным наблюдением руководства и коллектива фирмы, оценивающих степень его лояльности по отношению к делам фирмы. Со своей стороны фирма обязана обеспечить любому сотруднику необходимые условия труда и отдыха, постоянно заботиться о его благополучии, повышении квалификации и поддержании на высоком уровне интереса к выполняемым обязанностям и работам. Между руководством и сотрудниками не может быть глухой стены непонимания стоящих задач. Все дела фирмы должны быть важны для коллектива в целом и для каждого отдельного сотрудника. Достигается это сложным и длительным процессом индивидуального воспитания сотрудников на основах взаимного доверия, взаимопонимания и заботы. Руководители всех рангов несут персональную ответственность за качество этой работы.
В основе воспитательной работы с персоналом фирмы должны лежать не пустые словесные увещевания о необходимости хорошо работать и грядущем благополучии для всего персонала. Дальновидные руководители серьезных фирм под воспитательной работой подразумевают прежде всего создание реально здорового психологического климата в коллективе фирмы, позволяющего объединить осознанные усилия персонала на решение стоящих перед фирмой задач и преодоление возникающих трудностей.
Здоровый психологический климат в коллективе фирмы создает трудно преодолимый барьер на пути любого злоумышленника, который пытается получить конфиденциальные

сведения.
Для сотрудника фирмы часто важен не столько оклад, который он получает, сколько та доброжелательная обстановка, которая существует в коллективе, уверенность в том, что его уважают как специалиста, ценят его упорный труд и он может надеяться на продвижение по службе. При формировании здорового психологического климата решаются следующие задачи:
• создание действенной системы стимулирования труда персонала;
• обеспечение долговременной работы в фирме каждого сотрудника;
• формирование отношения к сотрудникам как самостоятельным членам коллектива, участие персонала в выработке решений;
• справедливое участие персонала в прибылях фирмы;
• реализация на практике гибкой, нетравмируемой системы увольнений;
• расстановка кадров в соответствии с их способностями;
• главенство в отношениях руководства и сотрудников духа коллективизма.
При хорошем психологическом климате сотрудники, доброжелательно относятся к любым ограничениям, связанным с функционированием системы защиты информации, добровольно, с пониманием важности выполняют все требования этой системы.
Здоровый психологический климат должен включать в себя следующие основные элементы:
• постоянное изучение и анализ комплекса качеств каждого сотрудника фирмы, т.е. знание каждого сотрудника в отдельности, а не абстрактная воспитательная работа с коллективом;
• строгое выполнение пунктов и положений коллективного договора;
• создание реальных условий для продвижения сотрудников по службе или повышение оклада с учетом их трудовых достижений, а не по иным причинам;
• оплата фирмой обучения или переподготовки способных и ценных для фирмы сотрудников;
• строгое выполнение администрацией норм по технике безопасности и охране труда, создание наилучших условий для работы сотрудников и их отдыха;
• организация благоприятных условий для проведения отпусков и выходных дней сотрудников;
• своевременное выявление неформальных лидеров в коллективе, выдвижение их на руководящие должности или перевод в другие подразделения (при их отрицательном влиянии на коллектив — увольнение);
• заинтересованное соучастие администрации фирмы в решении сотрудниками своих личных и бытовых затруднений;
• охрана персонала, гарантия юридической и физической защиты в случае попыток криминальных действий злоумышленника по отношению к ним, их родственникам и близким людям.
Процесс обучения и воспитания сотрудников фирмы должен завершаться контролем работы персонала с конфиденциальной информацией и документами. Важен контроль защиты ценной информации от недобросовестных посягательств отдельных сотрудников.
Превентивный контроль работы персонала предполагает прежде всего наличие в фирме строгого учета степени осведомленности каждого сотрудника в фирменных секретах. В данном случае учет создает информационную базу не только для облегчения контрольной функции, но и для аналитических исследований по обнаружению каналов утраты защищаемой информации.
Следует соблюдать правило, по которому в обычном принудительном режиме регистрируются все лица, имеющие доступ к определенным документам, базам данных и носителям коммерческих секретов. Одновременно подлежат специальному (экстремальному) учету все замеченные несанкционированные или ошибочные действия персонала с документами и информацией, нарушения системы доступа к информации и правил работы с конфиденциальными документами и базами электронных данных. Подобные факты подлежат оперативному, тщательному сравнительному анализу, а результаты анализа должны докладываться непосредственно первому руководителю фирмы.
Регулярный и своевременный учет состава конфиденциальной информации, известной каждому из сотрудников фирмы, является наиболее информативной частью контрольной работы. Учитываются любые контакты любого сотрудника с конфиденциальными сведениями, в том числе санкционированные, а также случайное, несанкционированное ознакомление с информацией, к которой сотрудник не имеет доступа, в том числе

несанкционированное ознакомление с конфиденциальной информацией сотрудников, вообще не имеющих доступа к подобной информации.
Традиционная (карточная) или электронная учетная форма должна содержать ряд предметных зон, позволяющих сопоставлять функциональные обязанности сотрудника и состав конфиденциальной информации, полученной сотрудником, который должен соответствовать выполняемым видам работы. Целесообразно включить;
в учетную форму следующие зоны:
• зону штатных функциональных обязанностей сотрудника, при реализации которых используется конфиденциальная информация (по утвержденной должностной инструкции);
• зону изменений и дополнений, внесенных в функциональные обязанности сотрудника, с указанием документа-основания, его даты и фамилии руководителя, подписавшего документ;
• зону стандартного состава конфиденциальных сведений и их индексов (по перечню конфиденциальной информации), к которым допущен сотрудник в соответствии с должностной инструкцией (с указанием наименования документа о допуске, его даты, номера и фамилии руководителя, подписавшего документ);
• зону изменений и дополнений в составе конфиденциальных сведений и их индексов по перечню, к которым допускается сотрудник в связи с пересмотром его должностных обязанностей (с указанием наименований и дат документов о допуске, фамилий руководителей, подписавших документы);
• зону документированной информации (документов), с которой знакомится или работает сотрудник, с указанием наименований документов, их дат и номеров, краткого содержания, целевого использования содержащихся в документах конфиденциальных сведений и их индексов по перечню, фамилий руководителей, разрешивших работу с документами;
• зону недокументированной конфиденциальной информации, которая стала известна сотруднику, с указанием даты и цели ознакомления, фамилии руководителя, разрешившего ознакомление, состава конфиденциальных сведений и их индексов по перечню;
• зону обнаруженного несанкционированного ознакомления сотрудника с конфиденциальной информацией с указанием даты ознакомления, условий или причин ознакомления, фамилии виновного сотрудника, места ознакомления, состава конфиденциальных сведений и их индексов по перечню. Анализ осуществляется сравнением содержания записей в зонах и индексов известной сотруднику конфиденциальной информации, т.е. ведется поиск несоответствия.
Следовательно, главным фактором воспитания у сотрудников фирменной гордости, ответственного отношения к выполнению своих служебных обязанностей является прежде всего упорная работа руководства фирмы по формированию здорового психологического климата в коллективе. Работник, ответственно относящийся к своей работе и участвующий в делах и прибылях фирмы, как правило, также ответственно относится к сохранению конфиденциальности тех работ, которые ведет фирма, строго соблюдает требования информационной безопасности и защиты информации.
Основными формами контроля качества работы персонала, повышения ими своих профессиональных знаний, в том числе в части защиты информации, можно назвать следующие:
• аттестация сотрудников;
• отчеты руководителей подразделений о работе подразделений и состоянии системы защиты информации;
• регулярные проверки руководителем фирмы или службой безопасности соблюдения сотрудниками требований по защите информации;
• самоконтроль сотрудников.
Аттестация сотрудников представляется одной из наиболее эффективных форм контроля их деятельности как в профессиональной сфере, так и в сфере соблюдения информационной безопасности фирмы. Аттестация персонала — это коллективная форма оценки профессиональной пригодности сотрудника, его соответствия занимаемой должности. Аттестация проводится периодически (ежеквартально, раз в год и иные сроки).
При проведении аттестации рассматриваются следующие характеристики сотрудника: трудовая дисциплина, исполнительность, трудолюбие, ответственность,

требовательность и принципиальность, организованность в работе, качество и эффективность выполняемой работы, самостоятельность и инициатива, творческая деятельность, прогрессивность профессиональных решений, профессиональный кругозор, умение общаться с людьми, организаторские способности, преданность делу фирмы. В части соблюдения сотрудничаем требований защиты информации рассматриваются такие характеристики, как знание нормативных и инструктивных документов по защите информации, умение применять требования этих документов в практической деятельности, отсутствие нарушений в работе с конфиденциальными документами, умение общаться с посторонними лицами, не раскрывая секреты фирмы, и т.д. На основе изучения этих характеристик формируется представление о каждом сотруднике, его деловых и человеческих качествах.

По результатам аттестации издается приказ (распоряжение), в котором отражаются решения аттестационной комиссии о поощрении, переаттестации, повышении в должности или увольнении сотрудников. Аттестационная комиссия может также выносить решение об отстранении сотрудника от работы с информацией и документами, составляющими тайну фирмы.

Одна из форм контроля — заслушивание руководителей структурных подразделений и руководителя службы безопасности на совещании у первого руководителя фирмы о состоянии системы защиты информации и выполнении ее требований сотрудниками подразделений. Одновременно на совещании принимаются решения по фактам нарушения сотрудниками этой системы.

Формой контроля являются также регулярные проверки выполнения сотрудниками (в том числе хорошо работающими) правил работы с конфиденциальной информацией, документами и базами данных. Проверки проводятся руководителями структурных подразделений и направлений деятельности фирмы, заместителями первого руководителя, работниками службы безопасности. Одновременно с соблюдением сотрудником правил работы с конфиденциальными документами проверяется наличие у этого сотрудника числящихся за ним документов, носителей информации, дел, магнитных носителей информации; электронных массивов информации, изделий и иных элементов, составляющих тайну фирмы.

Проверки могут быть плановыми, внеплановыми (внезапными), Внезапные проверки проводятся при возникновении малейшего подозрения о разглашении или утечке информации.

Самоконтроль сотрудников фирмы состоит в проверке самими руководителями и исполнителями полноты и правильности выполнения ими действующих инструктивных положений, а также в немедленном информировании непосредственного руководителя и службу безопасности о фактах утери документов, утрате по какой-либо причине ценной информации, разглашении лично или другими сотрудниками сведений, составляющих тайну фирмы, нарушении сотрудниками порядка защиты информации.

При работе с персоналом фирмы следует сосредоточивать внимание не только на сотрудниках, работающих с конфиденциальной информацией. Под контролем должны находиться также лица, не имеющие доступа к тайне фирмы. Можно предполагать, что эти сотрудники могут быть посредниками в действиях злоумышленника: в проведении электронного шпионажа, создании условий для хищения документов, снятии с них копий и т.п.

Кроме того, нужно учитывать, что сотрудники фирмы, работающие с конфиденциальной информацией, вынуждены действовать в рамках требований, регламентированных инструкцией по обеспечению режима конфиденциальности. Ограничение свободы человека может приводить к стрессам, нервным срывам. Сохранение чего-то в тайне противоречит потребности человека в общении путем обмена информацией. В связи с этим психологический настрой коллектива и отдельных сотрудников всегда должен находиться в центре внимания руководства фирмы.

В случае установления фактов невыполнения сотрудниками требований по защите информации к ним должны в обязательном порядке и своевременно применяться меры порицания и наказания в соответствии с правилами внутреннего трудового распорядка: объявление выговора, понижение в должности, лишение премии, отстранение от работы с конфиденциальной информацией, увольнение.

Важно, чтобы наказание было неотвратимым и своевременным невзирая на должностной уровень сотрудника.

Следует учитывать, что ответственность за разглашение сведений, составляющих тайну фирмы, в первую очередь несут руководители фирмы и ее структурных подразделений, направлений деятельности, филиалов, так как они полностью отвечают за разработку и реализацию мер, обеспечивающих информационную безопасность всех видов деятельности фирмы.

Факт утраты информации выявляется в основном посредством анализа публикаций, рекламы, выставочных и других материалов фирм-конкурентов. В этом случае анализируются карточки учета осведомленности сотрудников в тайне фирмы и выявляется круг сотрудников, владеющих утраченной информацией. Анализ ведется в рамках служебного расследования.

Служебное расследование организуется по фактам разглашения или утечки информации, утраты документов и изделий, другим грубым нарушениям правил защиты информации. Расследование проводится специальной комиссией, формируемой приказом первого руководителя фирмы. Расследование предназначено для выяснения причин, всех обстоятельств и их последствий, связанных с конкретным фактом установления круга виновных лиц, размера причиненного фирме ущерба. Все мероприятия обязательно документируются.

План проведения служебного расследования:

• определение возможных версий случившегося (утрата, хищение, уничтожение по неосторожности, умышленная передача сведений, неосторожное разглашение и т.д.);

• определение (планирование) конкретных мероприятий по проверке версий (осмотр помещений, полистная проверка документации, опрос сотрудников, взятие, письменного объяснения у подозреваемого лица и т.д.);

• назначение ответственных лиц за проведение каждого мероприятия;

• указание сроков проведения каждого мероприятия;

• определение порядка документирования;

• обобщение и анализ выполненных действий по всем мероприятиям;

• установление причин утраты информации, виновных лиц, объема ущерба для фирмы;

• передача материалов служебного расследования с заключительными выводами первому руководителю фирмы для принятия решения.

Служебное расследование проводится в кратчайшие сроки в ходе служебного расследования обычно анализируются следующие виды документов:

• письменные объяснения опрашиваемых лиц, составляемые в произвольной форме;

• акты проверки документации и помещений, где указываются фамилии лиц, проводивших проверку, их должности, объем и виды проведенного осмотра, результаты, указываются подписи этих лиц и дата;

• другие документы, относящиеся к расследованию (справки, заявления, планы, анонимные письма и т.д.). По результатам анализа составляется заключение о результатах проведенного служебного расследования, в котором подробно описывается проведенная работа, указываются причины и условия случившегося, определяются виновные лица, даются рекомендации по предотвращению в будущем подобных фактов. Вопрос о наказании виновных лиц ставится только после завершения служебного расследования, мера наказания определяется лично первым руководителем фирмы. При подтверждении факта передачи сотрудником информации постороннему лицу фирма должна обратиться в суд для вынесения решения о возмещении материального ущерба от кражи информации.

Следовательно, рекомендуемые направление и методы текущей работы с персоналом фирмы позволяют организовать эффективную систему заинтересованного участия сотрудников в обеспечении безопасности фирменных секретов, постоянного контроля за работой персонала с конфиденциальной информацией и своевременного выявления попыток злоумышленника завладеть интеллектуальной собственностью фирмы.

4.6. Особенности увольнения сотрудников, владеющих конфиденциальной информацией

Стабильность кадрового состава является важнейшей предпосылкой надежной информационной безопасности фирмы. Миграция специалистов — самый трудно контролируемый канал утраты ценной и конфиденциальной информации. Вместе с тем полностью избежать увольнений сотрудников не представляется возможным. Необходим тщательный анализ причин увольнения, на основе которого составляется и реализуется программа, исключающая эти причины. Например, повышение окладов, аренда жилья для сотрудников вблизи фирмы и оздоровление психологического климата, увольнение

руководителей, злоупотребляющих своим служебным положением, и др.
Технологическая цепочка увольнения сотрудника включает в себя:
• написание сотрудником заявления об увольнении с подробным раскрытием причины увольнения и желательно указанием места предполагаемой работы;
• передача заявления руководителю структурного подразделения для оформления и передачи в отдел кадров или службу персонала;
• прием службой конфиденциальной документации от увольняющегося сотрудника всех числящихся за ним документов, баз данных, носителей информации, изделий, материалов, с которыми он работал, проверка их комплектности, полноты и оформление приема в описи исполнителя или актом;
• сдача сотрудником пропуска (идентификатора) для входа в рабочую зону, всех ключей и печатей, запрещение сотруднику входить в рабочее помещение с использованием знания шифра кодового замка (при необходимости — изменение кода);
• проведение сотрудником службы безопасности или службы персонала беседы с сотрудником с целью напоминания ему об обязательстве сохранения в тайне тех сведений, которые ему были доверены по службе в фирме, предупреждение сотрудника о запрещении использования этих сведений в интересах конкурента или в личных целях, выяснение причины увольнения и места новой работы;
• подписание сотрудником обязательства о неразглашении им конфиденциальных сведений после увольнения;
• документальное оформление увольнения в соответствии с общими правилами;
• прием от сотрудника пропуска для входа в здание фирмы, выдача ему трудовой книжки и расчета по заработной плате, сопровождение его до выхода из здания сотрудником службы безопасности.
После сдачи всех документов и материалов сотруднику запрещается входить в режимную рабочую зону. При необходимости у него может быть изъят пропуск (идентификатор) сотрудника и выдан идентификатор посетителя с правом входа только в определенные административные помещения.
Беседа с увольняющимся сотрудником имеет целью предотвратить утрату информации или ее неправильное использование бывшим сотрудником в результате его природной или умышленной забывчивости. Следует напомнить увольняющемуся сотруднику, что он подписывал при поступлении на работу обязательство (подписку) о неразглашении фирменных секретов.
Ему напоминают, что и после увольнения из фирмы по крайней мере в течение года за его деятельностью будет осуществляться наблюдение. Предупреждение включается в обязательство, которое подписывает увольняющийся сотрудник.
В практике США аналогичный порядок рекомендуется применять в отношении консультантов, экспертов и временно работавших сотрудников. По крайней мере от них целесообразно в обязательном порядке потребовать письменное обязательство о неразглашении ставших известными им фактов и сведений, запрещении использования их в своей деятельности или работе конкурирующих фирм в течение определенного времени.
Эффективным средством против разглашения фирменных секретов в США считается заключение соглашения о предоставлении увольняющимся сотрудником консультационных услуг фирме в течение ряда лет. В течение этого времени, т.е. срока конфиденциальности известных ему сведений, ему выплачивается жалованье, близкое по размерам к зарплате. В результате бывший сотрудник противостоит соблазну использовать тайну фирмы в своих интересах.
Ущерб от увольнения сотрудника резко уменьшается, если тайна фирмы раздроблена и известна по частям достаточно большому числу служащих. В этом случае не приходится прибегать к указанным выше сложным и часто мало эффективным способам защиты тайны, известной уволенным сотрудникам.
В любом случае рекомендуется по истечении трех месяцев после увольнения направить бывшему сотруднику письмо-напоминание о необходимости сохранения тайны фирмы.
Если руководству фирмы стали известны случаи несанкционированного использования бывшим сотрудником конфиденциальных сведений или ноу-хау фирмы, следует начать активное судебное разбирательство выявленных фактов.
Рассмотренная технология оформления увольнения сотрудников, владеющих ценными и конфиденциальными сведениями, позволит не только повысить ответственность всего персонала за сохранность доверенных им сведений, но и предотвратить факты кражи

увольняющимися сотрудниками ценной информации, ограничить возможность использования ее в других организациях и фирмах.

5. ТЕХНОЛОГИЧЕСКИЕ ОСНОВЫ ОБРАБОТКИ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ

5.1. Защищенный документооборот

Процесс управления и документооборот жестко связаны единой технологией реализации функций управления. Целью документооборота является обеспечение управленческой деятельности, процесса принятия решений ценной, полезной, своевременной, полной и достоверной информацией. Движение документированной информации (на бумажных, магнитных или иных носителях) по линиям связи объективно сопровождает управленческую деятельность. Управлению экономическими, социальными, политическими, производственными структурами свойственна устойчивая стабильность построения и единообразие документооборота. Принципы и направления движения традиционных и электронных документов в аппарате управления едины при любых системах обработки и хранения документированной информации. Меняются методы работы с документами, но технологическая взаимосвязь документооборота с процессом управления сохраняется. Эта предпосылка создает объективную возможность для научного решения документоведческих и архивоведческих проблем безбумажного документооборота.

Как технологический процесс документооборот представляет собой схему (совокупность маршрутов) движения человекочитаемых (традиционных), машиночитаемых и электронных документов по установленным пунктам их учета, рассмотрения, исполнения и хранения для выполнения творческих, формально-логических и технических процедур и операций. При этом основной характеристикой движения документированной информации является его технологическая комплексность, т.е. соединение в единую совокупность управленческих, делопроизводственных и почтовых задач. Документооборот отражает весь «жизненный цикл» документа — период его активной жизни в управленческом процессе и период его достаточно пассивной архивной жизни. Происходит передача документированной информации не только в пространстве, но и во времени.

Конфиденциальные, как и открытые, документы находятся в постоянном движении. Перемещение конфиденциальных документов по множеству иерархических уровней управления создает серьезные предпосылки для утраты ценной информации, требует осуществления защитных мер в отношении документопотоков и документооборота в целом. Документооборот как объект защиты представляет собой упорядоченную совокупность (сеть) каналов объективного, санкционированного распространения конфиденциальной документированной информации в процессе управленческой и производственной деятельности пользователей (потребителей) этой информации.

При движении конфиденциальных документов по инстанциям увеличивается число источников (сотрудников, баз данных, рабочих материалов и т.п.), обладающих ценными сведениями, и расширяются потенциальные возможности утраты конфиденциальной информации, разглашения ее персоналом, утечки по техническим каналам, исчезновения носителя этой информации. Риск утраты конфиденциальной документированной информации существует на всех стадиях и этапах движения документов, при выполнении любых процедур и операций.

Наиболее часто встречающимися угрозами (опасностями) конфиденциальным документам в документопотоках могут быть:

• несанкционированный доступ постороннего лица к документам, делам и базам данных за счет его любопытства или обманных, провоцирующих действий, а также случайных или умышленных ошибок персонала фирмы;

• утрата документа или его отдельных частей (листов, приложений, схем, копий, экземпляров, фотографий и др.), носителя чернового варианта документа или рабочих записей за счет кражи, утери, уничтожения;

• утрата информацией конфиденциальности за счет ее разглашения персоналом или утечки по техническим каналам, считывания данных в чужих массивах, использования остаточной информации на копировальной ленте, бумаге, дисках и дискетах, ошибочных действий персонала;

• подмена документов, носителей и их отдельных частей с целью фальсификации, а также сокрытия факта утери, хищения;

• случайное или умышленное уничтожение ценных документов и баз данных, несанкционированная модификация и искажение текста, реквизитов, фальсификация

документов;
• гибель документов в условиях экстремальных ситуаций. Для электронных документов угрозы особенно реальны, так как факт кражи информации практически трудно обнаружить. В отношении конфиденциальной информации, обрабатываемой и хранящейся в компьютерах, условия возникновения угроз, по мнению ряда специалистов, классифицируются по степени риска следующим образом:
• непреднамеренные ошибки пользователей, операторов, референтов, управляющих делами, работников службы КД, системных администраторов и других лиц, обслуживающих информационные системы;
• кражи и подлоги информации;
• стихийные ситуации внешней среды;
• заражение вирусами.
В соответствии с характером указанных выше угроз формируются задачи обеспечения защиты информации в документопотоках, направленные на предотвращение или ослабление этих угроз.
Главным направлением защиты документированной информации от возможных опасностей является формирование защищенного документооборота и использование в обработке и хранении документов специализированной технологической системы, обеспечивающей безопасность информации на любом типе носителя.
Под защищенным документооборотом (документопотоком) понимается контролируемое движение конфиденциальной документированной информации по регламентированным пунктам приема, обработки, рассмотрения, исполнения, использования и хранения в жестких условиях организационного и технологического обеспечения безопасности как носителя информации, так и самой информации.
Помимо общих для документооборота принципов защищенный документооборот основывается на ряде дополнительных принципов:
• ограничения доступа персонала к документам, делам и базам данных деловой, служебной или производственной необходимостью;
• персональной ответственности должностных лиц за выдачу разрешения на доступ сотрудников к конфиденциальным сведениям и документам;
• персональной ответственности каждого сотрудника за сохранность доверенного ему носителя и конфиденциальность информации;
• жесткой регламентации порядка работы с документами, делами и базами данных для всех категорий персонала, в том числе первых руководителей.
Несколько иное содержание приобретает в защищенном документообороте принцип избирательности в доставке использовании конфиденциальной информации. В его основе лежит действующая в фирме разрешительная (разграничительная) система доступа персонала к конфиденциальной информации, документам и базам данных. Целью избирательности является не только оперативность в адресной доставке документированной информации потребителю, но и доставка ему только той информации, работа с которой разрешена ему в соответствии с его функциональными обязанностями. Избирательность распространяется не только на поступившие документы, но и на документы, которые составляются персоналом на рабочих местах или с которыми сотрудники только знакомятся.
Защищенность документопотоков достигается за счет:
• одновременного использования режимных (разрешительных, ограничительных) мер и технологических приемов, входящих в систему обработки и хранения конфиденциальных документов;
• нанесения отличительной отметки (грифа) на чистый носитель конфиденциальной информации или документ, в том числе сопроводительный, что позволяет выделить их в общем потоке документов;
•формирования самостоятельных, изолированных потоков конфиденциальных документов и часто дополнительного их разбиения на подпотоки в соответствии с уровнем конфиденциальности перемещаемых документов;
• использования автономной технологической системы обработки и хранения конфиденциальных документов, не соприкасающейся с системой обработки открытых документов;
• регламентации движения документов как внутри фирмы, так и между фирмами, т.е. с момента возникновения мысли о необходимости создания документа и до окончания

работы с документом и передачи его в архив;
• организации самостоятельного подразделения конфиденциальной документации или аналогичного подразделения, входящего (или не входящего) в состав службы безопасности или аналитической службы;
• перемещения документов между руководителями, исполнителями и иным персоналом только через службу КД.
Любому движению (перемещению, передаче) документа должны обязательно предшествовать операции по проверке комплектности, целостности и учету нового местонахождения документа. Вместе с тем дополнительные операции (защитные меры) не должны повышать трудоемкость работы с документами и увеличивать сроки их движения и исполнения.
Совокупность технологических стадий (функциональных элементов), сопровождающих потоки конфиденциальных документов, несколько отличается от аналогичной совокупности, свойственной потокам открытых документов. Так, входной документопоток включает в себя следующие стадии обработки конфиденциальных документов:
• прием, учет и первичная обработка поступивших пакетов, конвертов, незаконвертованных документов;
• учет поступивших документов и формирование справочно-информационного банка данных по документам;
• предварительное рассмотрение и распределение поступивших документов;
• рассмотрение документов руководителями и передача документов на исполнение и технологические участки службы КД;
• ознакомление с документами исполнителей, использование
или исполнение документов.
Выходной и внутренний документопотоки включают в себя следующие стадии обработки конфиденциальных документов:
• исполнение документов (этапы: определение уровня грифа конфиденциальности предполагаемого документа, учет носителя будущего документа, составление текста, учет подготовленного документа, его изготовление и издание);
• контроль исполнения документов;
• обработка изданных документов (экспедиционная обработка документов и отправка их адресатам; передача изданных внутренних документов на исполнение);
• систематизация исполненных документов в соответствии с номенклатурой дел, оформление, формирование и закрытие дел;
• подготовка и передача дел в ведомственный архив (архив фирмы).
В состав всех документопотоков включается также ряд дополнительных стадий обработки конфиденциальных документов:
• инвентарный учет документов, дел и носителей информации, не включаемых в номенклатуру дел;
• проверка наличия документов, дел и носителей информации;
• копирование и тиражирование документов;
• уничтожение документов, дел и носителей информации. Стадии, составляющие тот или иной документопоток, практически реализуются специализированной технологической системой обработки и хранения конфиденциальных документов.
Следовательно, защита документированной информации в документопотоках обеспечивается комплексом разнообразных мер режимного, технологического, аналитического и контрольного характера. Перемещение документов в процессе выполнения каждой стадии, этапа, процедуры обработки или исполнения сопровождается набором связанных учетных операций, закреплением документа за конкретным сотрудником и его персональной ответственностью за сохранность носителя конфиденциальной информации.

5.2. Технологические системы защиты и обработки конфиденциальных документов

Под технологической системой обработки и хранения конфиденциальных документов понимается упорядоченный комплекс организационных и технологических процедур и операций, обеспечивающих служб и технических средств, предназначенных для практической реализации задач, стоящих перед функциональными элементами (стадиями) документопотока. Технология обработки и хранения конфиденциальных и открытых документов базируется на единой научной и методической основе, призванной решать задачи обеспечения документированной информацией управленческие и производственные процессы. Одновременно технологическая система обработки и хранения

конфиденциальных документов решает и другую не менее важную задачу — обеспечение защиты носителей информации и самой информации от потенциальных и реальных угроз их безопасности.

В отличие от открытых документов к обработке конфиденциальных документов предъявляются следующие серьезные требования:

• централизация всех стадий, этапов, процедур и операций по обработке и хранению конфиденциальных документов;

• учет всех без исключения конфиденциальных документов;

• операционный учет технологических действий, производимых с традиционным (бумажным) или электронным носителем (в том числе чистым) и документом, учет каждого факта «жизненного цикла» документа;

• обязательный контроль вторым работником службы КД правильности выполнения учетных операций;

• учет и обеспечение сохранности не только документов, но и учетных форм;

• ознакомление или работа с документом только на основании письменной санкции (разрешения) полномочного руководителя, письменного фиксирования всех обращений персонала к документу;

• обязательная подпись руководителей, исполнителей и технического персонала при выполнении любых действий с документом в целях обеспечения персональной ответственности сотрудников фирмы за сохранность носителя и конфиденциальность информации;

• строгий контроль выполнения персоналом введенных в фирме правил работы с конфиденциальными документами, делами и базами данных, обязательными для всех категорий персонала;

• систематические (периодические и разовые) проверки наличия документов у исполнителей, в делах, базах данных, на машинных носителях и т.д., ежедневный контроль сохранности, комплектности, целостности и местонахождения каждого конфиденциального документа;

• коллегиальность процедуры уничтожения документов, дел и баз данных;

• письменное санкционирование полномочным руководителем процедур копирования и размножения бумажных и электронных конфиденциальных документов, контроль технологии выполнения этих процедур.

Технологическая система обработки и хранения конфиденциальных документов распространяется не только на управленческую (деловую) документацию, но и на конструкторские, технологические, научно-технические и другие аналогичные документы, публикации, нормативные материалы и др., хранящиеся в специальных библиотеках, информационных центрах, ведомственных архивах, документированную информацию, записанную на любом типе носителя информации.

Эволюция типов технологических систем обработки и хранения документов тесно связана с научно-техническим прогрессом, достижениями науки и техники в области документирования информации, обработки информационных ресурсов, программирования и вычислительной техники. Наблюдается устойчивая тенденция замены бумажного носителя информации техническим — магнитным и носителями других типов. Технический носитель дает возможность в определенной степени исключить человека из технологического процесса обработки и хранения документированной информации и создает основу для формирования и развития концепции «электронного (безбумажного) документооборота».

Технологические системы обработки и хранения конфиденциальных документов могут быть традиционными, автоматизированными и смешанными.

Традиционная (делопроизводственная) система основывается на ручных методах работы человека с документами и является универсальной. Она надежно, долговременно обеспечивает защиту документированной информации как в обычных, так и в экстремальных ситуациях. В связи с этим стадии защищенного документооборота в большинстве случаев технологически реализуются методами и средствами именно традиционной системы обработки и хранения конфиденциальных документов, а не автоматизированной. Система одинаково эффективно оперирует как традиционными (бумажными) документами, так и документами машиночитаемыми, факсимильными и электронными. Трудоемкость множества технических и формально-логических процедур и операций обычно снижается за счет включения в технологический процесс организационной и вычислительной техники, что в целом не меняет тип системы. Вместе

с тем система характеризуется низкой степенью оперативности доставки документов потребителям информации, невысокой эффективностью справочной, поисковой и контрольной работы по документам, потребностью в значительном количестве персонала, обслуживающего систему.

Традиционная технологическая система обработки и хранения конфиденциальных документов лежит в основе широко известного понятия «делопроизводство» или «документационное обеспечение управления» (в его узком, но часто встречающемся в научной литературе понимании как синонима делопроизводства). С другой стороны, делопроизводство часто рассматривается в качестве организационно-правового и технологического инструмента построения документационного обеспечения управления, с чем, на наш взгляд, трудно не согласиться.

Ведение конфиденциального делопроизводства централизуется в едином подразделении аппарата управления — службе КД, функционально не связанной с подразделением, обрабатывающим открытые документы. В некрупных предпринимательских структурах функция централизованной обработки и хранения конфиденциальных документов возлагается на управляющего делами, менеджера по безопасности или даже секретаря-референта (референта) первого руководителя.

Служба КД может включать с себя следующие функциональные группы (участки деятельности):

• группу учета поступивших документов;
• группу учета носителей конфиденциальной информации;
• группу учета и обработки изданных документов;
• группу учета номенклатурных дел — архив фирмы;
• группу инвентарного учета документов;
• бюро изготовления документов;
• копировально-множительную группу;
• контрольно-методическую группу.

Службу конфиденциальной документации необходимо располагать в помещении, смежном с приемной первого руководителя фирмы. В этом помещении ведется обработка и хранение всех конфиденциальных документов. Правом входа в рабочее помещение службы обладает только первый руководитель фирмы и руководитель службы безопасности.

Как отмечалось выше, конфиденциальные документы достаточно часто не входят в. сферу управленческой (деловой) документации и относятся к технической документации (конструкторской, технологической, научно-исследовательской и т.д.), которая по своей сути чаще всего содержит действительно ценные сведения, изобретения и ноу-хау фирмы. Несмотря на специфический характер этой документации, она также обрабатывается и хранится в службе КД — группе технической документации. В предпринимательских структурах, имеющих незначительный объем конфиденциальных документов или в которых основная масса документов является конфиденциальной (например, в банках, страховых компаниях), обработка конфиденциальных документов может осуществляться в подразделении или сотрудником, ведущим делопроизводство по открытым документам. Не следует забывать о том, что преимущества и эффективность традиционных (часто простейших) делопроизводственных систем в небольших фирмах далеко не исчерпаны и их надежность в отношении гарантированной защиты конфиденциальной информации достаточно велика.

Автоматизированная технология (как и традиционная, делопроизводственная) является обеспечивающей и обслуживает конкретные потребности персонала в конфиденциальной информации. Автоматизированная система, создаваемая в службе КД или службе безопасности, должна в принципе обеспечивать:

• сокращение значительного объема рутинной работы с документами и числа технических операций, выполняемых персоналом службы ручными методами;
• реализацию возможности для персонала фирмы работать с электронными документами в режиме безбумажного документооборота;
• достаточную гарантию сохранности и целостности информации, регулярного контроля и противодействия попыткам несанкционированного входа в банк данных;
• аналитическую работу по определению степени защищенности информации и поиску возможных каналов ее утраты;
• единство технологического процесса с режимными требованиями к защите информации (допуск, доступ, регламентация коллегиальности выполнения некоторых процедур,

операций и т.п.);
• персональную ответственность за сохранность конфиденциальных сведений в машинных массивах и на магнитных носителях вне ЭВМ;
• возможность постоянного учета местонахождения традиционного или электронного документа и проверки его наличия и целостности в любое время;
• предотвращение перехвата информации из ЭВМ по техническим каналам, наличие надежной охраны помещений, в которых находится вычислительная техника, охрана компьютеров и линий компьютерной связи;
• исключение технологической связи единичного компьютера или локальной сети, предназначенных для обработки конфиденциальных документов с сетями, обеспечивающими работу с открытой информацией, исключение использования их линий связи, выходящих за пределы охраняемой зоны (здания, территории).

Автоматизированная технологическая система обработки и хранения конфиденциальных документов по сравнению с аналогичными системами, оперирующими общедоступной информацией, имеет ряд принципиальных особенностей:
• архитектурно компьютеры, обрабатывающие значительные объемы конфиденциальной информации, могут объединяться в локальную сеть как в рамках службы КД, так и с охватом руководителей и основных специалистов; однако в любом варианте локальная сеть базируется на главном компьютере (сервере), находящемся у системного администратора службы КД; автоматизированные рабочие места, рабочие станции могут быть увязаны в локальную сеть только по вертикали;
• в некрупных фирмах конфиденциальная информация обрабатывается на уровне первого руководителя и его референта на единичном защищенном компьютере, не имеющем выхода в какую-либо локальную сеть;
• обязательное наличие иерархической и утвержденной первым руководителем фирмы системы разграничения доступа к информации, хранящейся как в машинных массивах, так и на магнитных носителях вне ЭВМ; охват системой разграничения доступа не только персонала фирмы, но и персонала службы КД;
• закрепление за каждым пользователем строго определенного состава массивов электронной информации и магнитных носителей; исключение возможности для пользователя «покопаться» в базе данных системы;
• автоматизированное выполнение пользователями операций справочного и поискового обслуживания, составления и иногда изготовления документов, контроля исполнения документов, работы с электронными документами, факсами и электронными налогами бумажных документов;
• сохранение информационной базы учетной функции (в правовом понимании, а также как элемента формирования страхового массива информации) и функции персональной ответственности за традиционной технологической системой с использованием учетных карточек и иных форм (описей), изготовляемых не вручную, а автоматически — на принтере ЭВМ; автоматическая допечатка в указанные формы изменений и дополнений при движении документов;
• обязательный учет конфиденциальных электронных документов, находящихся на всех магнитных носителях и в машинных массивах, постоянная проверка службой КД реального наличия этих документов на носителях и в массивах, их целостности, комплектности и отсутствия несанкционированных копий;
• необходимость исключения технической возможности копирования информации, содержащейся в компьютере (рабочей станции) пользователя, на другие магнитные носители и работы компьютера в комплекте с принтером (изъятие из ЭВМ дисководов и т.п.);
• жесткое соблюдение персоналом правил работы с конфиденциальной электронной информацией, в частности правила, которое гласит, что все операции с информацией в компьютере должны быть письменно санкционированы полномочным должностным лицом, подотчетны службе КД и протоколироваться в машинном журнале; протоколы подлежат регулярному контролю и анализу специалистами службы КД или службы безопасности;
• изъятие конфиденциальной информации из базы данных компьютера (рабочей станции) по окончании работы с ней (например, в конце рабочего дня, при длительных перерывах в работе и т.п.) и перенос информации на дискеты, подлежащие сдаче в службу КД.

Рассмотрение и исполнение электронных конфиденциальных документов и электронных аналогов бумажных документов разрешается только при наличии сертифицированной

системы защиты компьютеров и локальной сети, включающей комплекс программно-аппаратных, криптографических и технических мер защиты базы данных, компьютеров и линий связи. Помещения, в которых конфиденциальная информация обрабатывается на ЭВМ, должны иметь защиту от технических средств промышленного шпионажа, надежную круглосуточную охрану и пропускной режим. Кроме того, следует учитывать, что при автоматизированной обработке объективно резко увеличивается количество носителей (источников), содержащих конфиденциальные сведения: традиционный бумажный документ, разнообразные машинограммы карточек, описей документов, многочисленные записи информации на магнитных носителях и визуальная информация на экране дисплея. Недостатком обработки информации на ЭВМ является также необходимость постоянного дублирования информации на нескольких носителях с целью исключения опасности ее утраты или искажения по техническим причинам.

Указанные выше особенности усложняют систему, но без их соблюдения нельзя гарантировать сохранность конфиденциальной информации, эффективность защиты информационных массивов в ЭВМ от несанкционированного доступа, разрушения, копирования и подмены.

Безопасность информации в ЭВМ и локальной сети требует эффективной взаимосвязи машинной и внемашинной защиты конфиденциальных сведении. В этой связи важное актуальное значение имеет защита технических носителей конфиденциальной информации (машиночитаемых документов) на внемашинных стадиях их учета, обработки и хранения. Именно на этих стадиях особенно велика вероятность утраты машиночитаемого документа. Подобная проблема несущественна для носителей, содержащих открытую информацию. В основе обеспечения сохранности носителей электронных конфиденциальных документов, находящихся вне машины, в настоящее время эффективно используются зарекомендовавшие себя принципы и методы обеспечения безопасности документов в традиционной технологической системе.

В настоящее время наиболее широко используется смешанная технологическая система обработки и хранения конфиденциальных документов, совмещающая традиционную и автоматизированную технологии. Выборочно автоматизируются: справочная и поисковая работа по бумажным документам, процедура составления и изготовления документов и учетных форм, контроль исполнения, сервисные задачи. Остальные стадии и процедуры выполняются в русле традиционной, делопроизводственной технологии (распределение бумажных документов, их рассмотрение, исполнение, оперативное и архивное хранение документов). В силу специфики обрабатываемых сведений о документах и самих документов автоматизированные системы делопроизводственной ориентации имеют в большинстве случаев информационно-справочный характер. Недостаток смешанной технологии состоит в неполном использовании преимуществ и функциональных возможностей компьютерной технологии, отчего сохраняются рутинные делопроизводственные операции, которые мешают совершенствовать документооборот.

Следовательно, традиционные и автоматизированные технологические системы обработки и хранения конфиденциальных документов представляют собой сложные комплексы, решающие задачи как документационного обеспечения управленческой и производственной деятельности необходимой информацией, так и одновременно достаточно надежной защиты документов от несанкционированного доступа и других возникающих угроз безопасности информационных ресурсов фирмы.

5.3. Принципы учета конфиденциальных документов

Многоступенчатый учет всех процедур и операций, выполняемых с документом, существенно отличает технологию обработки и хранения конфиденциальных документов и лежит в основе процесса защиты конфиденциальных документов от любого вида угроз по организационным и техническим каналам.

По отношению к открытым документам учет (чаще используется термин «регистрация») в первую очередь преследует цель включения документа в справочно-информационную систему для выполнения функций справочной и поисковой работы по документам, контроля исполнения поручений и заданий, содержащихся в документе.

При учете конфиденциальных документов на первый план выдвигается функция сохранности документов и фиксирования их местонахождения. В связи с этим к конфиденциальным документам более применим термин «учет документов», который представляется шире и лучше отражает задачу, стоящую перед этим процессом. В данном случае регистрацию мы рассматриваем, лишь как запись исходных или рабочих сведений

о документе.
Основной целью учета конфиденциальных документов является обеспечение их физической сохранности, комплектности и целостности, контроль за доступом к ним персонала, проверка реального наличия документов и аналитическая работа по осведомленности персонала с содержанием документов. Справочная работа и контроль исполнения документов, хотя и присутствуют в качестве стадий обработки документов, часто сводятся к неосновным технологическим процессам. В отличие от регистрации открытых документов конфиденциальные документы (на любом носителе) учитываются сразу же при поступлении или перед изготовлением первого варианта беловика, т.е. до выполнения процедур рассмотрения, распределения или согласования, подписания. Индивидуальному учету подлежат все без исключения конфиденциальные документы. Учет конфиденциальных документов предусматривает не только фиксирование факта поступления или начала работы над документом, но и обязательную регистрацию всех перемещений документа и совершаемых с ним действий.
При ведении учета возможные угрозы конфиденциальным документам реализуются в результате:
• выпадения документа из учетной системы за счет ошибочных или злоумышленных действий работника службы КД;
• отсутствия фиксированного контроля за документом при переходе его от одной технологической стадии движения и процедуры обработки к другой;
• включения конфиденциальных сведений из документов в учетные формы;
• утечки информации по техническим каналам;
• использования работником службы КД традиционной или автоматизированной технологии, не предназначенной для обработки и хранения конфиденциальных документов или самодельной, непрофессиональной технологии;
• нарушения порядка выполнения учетных операций и ведения справочно-информационного банка данных по документам. Основным способом защиты информации от различных угроз является строгая регламентация специализированных технологических процедур учета и контроль за соблюдением работниками службы КД и персоналом утвержденных руководством фирмы требований и правил.
Учет конфиденциальных документов должен решать задачи фиксирования следующих фактов:
• поступления пакета с документами, отдельного бумажного или машиночитаемого документа, или документа, поступающего по электронной или факсимильной почте (линиям связи);
• регистрации исходных сведений о документе и включения его в справочно-информационный банк данных по документам;
• переноса информации с бумажного документа на машинный носитель, включения документа в электронную базу данных и помещения бумажного документа в соответствующее дело;
• перемещения документа (всех обращений персонала к документу) в процессе его рассмотрения, исполнения и возвращения в службу КД (регистрация рабочих сведений);
• местонахождения документа (у исполнителя, менеджера, референта, в деле, файле, на машинном носителе вне ЭВМ и т.д.) в любой момент времени в период исполнения документа и при его архивном хранении;
• регистрации исходных сведений о подготовленном документе;
• начала и окончания составления, изготовления и издания документа;
• дальнейшей работы над изданным документом или отправления его адресату (регистрация рабочих сведений);
• оформления специально подготовленных носителей для составления конфиденциальных документов;
• перевода документа с одного вида учета на другой и. идентификации (соответствия) учетных номеров;
• обеспечения поисковой, справочной и контрольной работы по конфиденциальным документам;
• регулярного удостоверения комплектности документа при выполнении каждой технологической процедуры с целью предупреждения утраты копий и экземпляров документа, черновиков, редакций, приложений, отдельных листов и рабочих записей;
• регистрации в машинном журнале всех действий, которые выполняются с электронными

документами в базе данных;
• регистрации регулярных контрольных операций второго работника службы КД по проверке правильности выполнения работником службы всех технологических операций и проверке наличия документов.
Учет конфиденциальных документов централизуется по категориям документов на участках службы КД. Он всегда делится на несколько изолированных видов, так называемых учетов, соответствующих стадиям в технологической схеме обработки документов в документопотоках и обеспечивающих четкое распределение учетных операций по участкам службы КД. Это позволяет дробить знание тайны фирмы между несколькими независимыми работниками этой службы и осуществлять коллегиальность в контроле за сохранностью документов на каждом участке.
В предпринимательских структурах целесообразны следующие виды учета конфиденциальных документов и дел:
• учет пакетов (конвертов), содержащих конфиденциальные документы, а также учет поступления незаконвертованных документов, документов, поступающих по телеграфной, электронной почте и факсимильной связи с грифом конфиденциальности (пакетный учет);
• пакетный учет поступления документов, не имеющих грифа конфиденциальности, но отнесенных к документам ограниченного доступа в перечне данной фирмы;
• учет входящих (поступивших, входных) документов (входящий учет);
• учет подготовленных исходящих и внутренних документов (учет подготовленных документов или исходящий учет);
• инвентарный учет документов;
• номенклатурный учет дел.
Следовательно, в предметном и технологическом аспектах учет конфиденциальных документов в значительной степени отличается от регистрации открытых документов и делится на ряд видов, что определяется необходимостью защиты документов от тех угроз, которые могут при их реализации стать причиной несанкционированного доступа злоумышленника к тайне фирмы.
При любом виде учета конфиденциальных документов выполняются следующие процедуры:
индексирование документов;
первичная регистрация (запись) исходных сведений о документе;
последующая запись рабочих сведений о документе; формирование справочно-информационного банка данных по документам;
ведение (актуализация) справочно-информационного банка данных; контроль процесса полноты и правильности регистрации документов, сохранности документов и учетных форм.
Основой индексирования (присвоения условного обозначения, имени) конфиденциального документа является валовая нумерация всего потока документов в течение календарного года. Подобная индексация гарантирует сохранность записи исходных сведений о документе — ни один номер не может исчезнуть, а карточка выпасть из систематизированного по номерам массива. К номеру документа может добавляться смысловой индекс, идентифицирующий дело, в котором будет храниться документ.
В некрупных фирмах с незначительным объемом конфиденциальных документов валовая нумерация может быть или сплошной, т.е. по всем документам независимо от их принадлежности к какому-либо виду учета, или вестись отдельно по каждому делу, содержащему конфиденциальные документы.
Состав сведений, включаемых в учетную форму (журнал или карточку) для регистрации конфиденциальных документов, подразделяется на два блока: а) фиксирующий постоянные (исходные) сведения о документе (вид документа, наименование автора, дата, индекс, краткое содержание, количество листов, наличие и количество листов приложений и др.) и б) фиксирующий переменные, текущие, рабочие сведения о движении и местонахождении документа (резолюция руководителя, обозначение фамилии исполнителя, даты передачи документа, росписи за документ, различные отметки и др.).
В практической деятельности служб КД для регистрации исходных и рабочих сведений о документе чаще всего применяется традиционная карточная форма учета документов. Однако не исчезла полностью и журнальная форма учета в силу своих серьезных и неповторимых преимуществ — абсолютной гарантии сохранности всех записей о всех конфиденциальных документах, отсутствия практической возможности подмены листов, простоты изготовления, удобства хранения.

Учетная карточка конфиденциального документа отличается от регистрационно-контрольной карточки открытого документа не только большим количеством граф, но и их взаимосвязью в отражении пути движения документа. Одним из серьезных недостатков карточной формы регистрации является отсутствие определенной гарантии сохранности учетных карточек в картотеке и возможность их легкой подмены (например, при краже документа или его фальсификации). В связи с этим возникает необходимость учета карточек и ведения с этой целью специальной учетной формы.

При карточной форме учета на каждый конфиденциальный документ заполняется 1 или 2 экземпляра регистрационной карточки. При заполнении одного экземпляра карточки она учитывается в контрольном (контрольно-учетном) журнале. Журнал предназначен для обеспечения последовательности присвоения документам учетных номеров, контроля за наличием документов и карточек, ускорения их поиска и внесения отметок о местонахождении документа. В журнале против учетного номера документа указывается фамилия исполнителя, расписавшегося в карточке за его получение. При заполнении двух экземпляров карточки все указанные сведения фиксируются во втором экземпляре, а функцию контрольного журнала выполняет валовая (нумерационная) учетная картотека. Перемещение конфиденциальных документов и учетных карточек между работниками службы КД фиксируется в передаточном журнале.

В предпринимательских фирмах, имеющих небольшой объем конфиденциальных документов, как правило, кратковременного периода ограничения доступа, учет этих документов может осуществляться в соответствии с правилами и в учетных формах открытого делопроизводства. Однако в этом случае конфиденциальные документы дополнительно вносятся в инвентарную опись с валовой нумерацией документов. Этим обеспечивается целенаправленное наблюдение за их сохранностью, движением и наличием, а также за своевременным снятием грифа конфиденциальности. Перемещаются и хранятся эти документы отдельно от документов всего потока.

В учетных формах не разрешается делать какие-либо исправления с помощью корректирующей жидкости или подчистки бритвой. Исправление аккуратно вписывается работником службы КД рядом или выше ошибочной записи и заверяется его росписью. Ошибочная запись зачеркивается одной чертой.

Значительное место в обработке конфиденциальных документов занимает инвентарный (списочный, перечневый) учет. На инвентарный учет берутся следующие конфиденциальные документы:

• документы, не включенные в номенклатуру дел и не подлежащие подшивке в дела, например сброшюрованные документы, документы большого формата, чертежно-графические, научно-технические документы, фотографии, рисунки, в том числе являющиеся приложениями к основным документам или сопроводительным письмам;

• документы, изъятые по какой-либо причине из дела, переведенные на выделенное хранение и образовавшие самостоятельное дело, папку альбом, например особо ценные документы, документы более широкого доступа, чем другие документы дела, и др.;

• технические носители информации (чистые и с записанной информацией), например дискеты, видео- и аудиокассеты, кассеты с фотопленкой и др.;

• бумажные носители информации особо ценных документов для составления черновиков, оригиналов и подлинников документов, например блокноты с отрывными листами, рабочие тетради, отдельные листы бумаги и др.;

• при необходимости — журналы учета документов и учетные картотеки, картотеки учета выдачи дел и документов, законченные производством дела.

Картотека (журнал, опись) инвентарного учета конфиденциальных документов ведется непрерывно. Номера каждого следующего года продолжают номера предыдущего года. Инвентарный номер указывается на документе в верхнем левом углу на первом и титульном листах, например: «Инв. № __, дата». Одновременно может формироваться электронная инвентарная опись конфиденциальных документов.

Автоматизированный учет конфиденциальных документов включает в себя следующие процедуры:

• подготовка документов к вводу в ЭВМ;

• ввод исходных сведений о документах в автоматизированный банк данных;

• ввод в предварительный массив автоматизированного банка данных электронных документов, документов на магнитном носителе и путем сканирования — бумажных документов;

• распечатка на бумажном носителе (карточке) исходных учетных сведений о документе, при необходимости — распечатка на бумажном носителе копий электронных документов;
• ежедневная проверка правильности регистрации документов и их наличия;
• изготовление на учтенной дискете страховой копии документа, поступившего по линии электронной почты;
• перенос электронных документов из предварительного массива в основной рабочий массив (после выполнения учетных операций);
• обозначение на бумажном документе или сопроводительном' письме к дискете отметки о вводе документа в базу данных с указанием его учетного (поискового) номера;
• подшивка бумажного документа и бумажной копии электронного документа в дело в соответствии с номенклатурой дел службы КД и помещение страховых дискет (в том числе копий поступивших дискет) в ячейку места хранения.

На основе применяемых традиционных и электронных регистрационных форм создается справочно-информационный банк данных (учетный аппарат), который предназначен для контроля за сохранностью документов, накопления и систематизации исходных данных о документах, актуализации массивов информации — внесения в учетные формы рабочих сведений в процессе исполнения или использования документов, обеспечения контроля **за** исполнением документов и проверки их наличия.

Банк данных по документам должен отвечать следующим требованиям:
• содержать полные и достоверные данные о всех конфиденциальных документах;
• иметь единообразную схему построения;
• наименования граф в учетных формах должны быть правильно сформулированы и однозначно пониматься сотрудниками;
• отличаться минимальной трудоемкостью при формировании и ведении;
• обеспечивать сопоставление учетных номеров при переводе документа с одного вида учета на другой; вестись по месту хранения документов.

Задачи справочно-информационного банка данных решаются двумя обязательными технологическими элементами: а) формированием банка и б) ведением (актуализацией) банка.

Банк может быть традиционным и автоматизированным. Традиционный справочно-информационный банк данных по конфиденциальным документам при любом виде учета обычно включает в себя:
• журналы учета документов по видам учета или:
• учетную валовую картотеку с разделами неисполненных (для вторых экземпляров карточек) и исполненных (для первых отработанных экземпляров карточек) документов, в которой карточки в разделах располагаются в последовательности учетных номеров документов;
• учетную картотеку на неисполненные документы, в которой первые экземпляры карточек располагаются по исполнителям (картотека «За исполнителями»);
• справочную картотеку на исполненные документы, в которой освободившиеся (вторые) экземпляры карточек располагаются по корреспондентам или другому удобному для использования признаку, например по рубрикам номенклатуры дел;
• кодификационную картотеку по распорядительным документам;
• контрольную картотеку, в которой дополнительные экземпляры карточек располагаются по срокам исполнения документов; • передаточный журнал для фиксирования факта перемещения документа и учетной карточки с одного участка службы КД на другой, от одного работника этой службы другому.

В некрупных фирмах три картотеки могут объединяться в одну с использованием различных классификационных схем. Например, может формироваться учетно-справочная картотека: а) «За исполнителями», б) с учетным валовым разделом для карточек на все конфиденциальные документы и в) со справочным разделом на исполненные документы, в котором карточки располагаются по рубрикам номенклатуры дел. Первый и второй экземпляры карточки помещаются одновременно в первые два раздела. Второй раздел является описью конфиденциальных документов фирмы. После исполнения документа карточка из первого раздела перемещается в третий раздел картотеки. Может применяться схема систематизации карточек сразу же в соответствии с рубриками номенклатуры дел (при нумерации документов отдельно по каждому делу).

Автоматизированный справочно-информационный банк данных по конфиденциальным документам принципиально не отличается от аналогичных систем, оперирующих открытой

информацией и документами, систем, которые широко используются в практической деятельности фирм. Конфиденциальные электронные документы и электронные аналоги бумажных документов на любом носителе, в том числе поступившие по защищенной линии электронной почты, подлежат строгому учету как и традиционные бумажные конфиденциальные документы и материалы.

В автоматизированных системах дополнительно должен быть организован учет состава и динамики актуализации всех машинных массивов документов, всех типов магнитных носителей информации и записанных на них документов. Любая операция с электронным документом, выполняемая как в службе КД, так и пользователями, подлежит фиксированию в учетной форме, машинном журнале и подтверждается росписью одного или двух сотрудников.

Автоматизированный справочно-информационный банк данных должен иметь следующие основные электронные учетные массивы:

• инвентарную валовую опись традиционных, электронных и иных конфиденциальных документов фирмы с указанием их местонахождения или валовые описи учетных карточек документов по видам учета (контрольные журналы);

• массивы электронных учетных карточек документов по видам учета;

• массив электронных карточек учета выдачи документов по видам учета (если такие карточки предусмотрены технологией);

• описи рабочего и архивного массивов электронных конфиденциальных документов по каждому компьютеру;

• массив учетных карточек (описей) магнитных носителей с перечислением документов, записанных на каждом носителе;

• описи документов (на любых носителях), находящихся у руководителей и исполнителей (по фамилиям);

• описи предварительного массива конфиденциальных документов компьютера службы КД.

Основное назначение этих массивов — обеспечение справочной, поисковой и контрольной работы по документам, учета их местонахождения и наличия возможности Немедленной проверки сохранности и комплектности этих документов на любых носителях без предварительной подготовки (составления выборки, поиска по различным признакам и т.п.).

Учетную и страховую функцию, а также функцию обеспечения персональной ответственности за сохранность документов и конфиденциальность информации могут выполнять следующие традиционные массивы, сформированные на основе бумажных экземпляров (распечаток, машинограмм) электронных массивов:

• страховая учетная валовая картотека бумажных экземпляров электронных карточек документов;

• картотека «За исполнителями» для бумажных экземпляров электронных карточек учета выдачи документов;

• картотека учетных карточек (описей) магнитных носителей информации.

Кроме того, ведется комплект постоянно обновляемых и достоверных дубликатов (страховых и резервных) всех магнитных носителей, на которых записаны сведения о конфиденциальных документах или сами документы. Заполняется также машинный журнал учета работы ЭВМ и выполняемых действий с документами.

Рабочие сведения вносят первоначально в электронные учетные формы и описи документов, а затем в службе КД допечатываются на принтере в бумажные экземпляры этих форм и описи документов, находящихся у руководителей и исполнителей.

Следует иметь в виду, что при технологическом различии автоматизированных систем в электронных документах и учетных формах пользователи могут ставить электронную подпись, ежедневный код или в бумажных экземплярах электронных документов и учетных форм — фамилию и традиционную роспись. Совмещать где-либо эти два вида подписи не допускается. Процедура ввода в автоматизированный банк данных текста электронного конфиденциального документа, документа с дискеты и текста бумажного документа выполняется в тех автоматизированных системах, которые имеют специальное сертифицированное программное обеспечение и снабжены комплексной системой защиты информации.

Заключительной процедурой при любой технологической системе учета конфиденциальных документов является контроль процесса регистрации и сохранности документов и учетных форм на каждом участке службы КД. Цель процедуры состоит в ежедневной

проверке вторым работником службы соответствия состава документов, подлежащих учету, и состава реально учтенных документов. Контроль распространяется на все виды документов на любых носителях, в том числе поступивших по линии защищенной компьютерной связи в локальной сети, электронной или факсимильной почте. Контролируется наличие самих документов или правильности внесения отметок в учетные формы о передаче документов на рассмотрение, исполнение и выполнение других действий. Факт контроля подтверждается росписью второго работника службы КД в учетных формах.

Следовательно, технологический процесс учета конфиденциальных документов включает в себя ряд процедур, которые являются обязательными для любого вида учета и любой технологической системы обработки и хранения документов. Рассмотренные процедуры включают в себя не только технологические аспекты, связанные с практической реализацией определенного типа системы обработки и хранения конфиденциальных документов, но и аспекты обеспечения защиты документов и информации от различных угроз в процессе учетной работы.

6. ТЕХНОЛОГИЯ ОБРАБОТКИ ПОСТУПИВШИХ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ

6.1. Учет поступивших пакетов и документов

В открытом делопроизводстве поступившие в фирму пакеты, конверты и другие почтовые отправления никогда не ставятся на индивидуальный учет, возможная утеря конверта с документами или некомплектность документа в конверте обычно не является предметом большого беспокойства. Иначе обстоит дело с поступающими пакетами и конвертами, содержащими конфиденциальные документы. Задача правильной организации работы с пакетами и предотвращения реальной опасности несанкционированного ознакомления с документами в пути следования пакета или их утраты в результате вскрытия, утери, кражи пакетов, уничтожения или подмены документов становится актуальной. В основе решения этой задачи лежит выполнение комплекса технологических процедур, включающего: прием пакетов, учет пакетов, распределение и вскрытие пакетов, выделение из общего документопотока ценных и конфиденциальных документов, закрытие журнала учета пакетов.

При выполнении указанного комплекса процедур осуществляются:

• контроль сохранности, целостности и комплектности документов, установление возможного факта несанкционированного вскрытия пакета на пути его следования от отправителя до адресата;

• исключение случаев попадания в фирму пакетов и документов, принадлежащих другим организационным структурам, и разглашения их секретов;

• документированное удостоверение факта получения пакета с конфиденциальными документами от службы доставки с целью предотвращения утраты документов после вскрытия пакета;

• формирование исходной учетной базы для последующей регистрации документов и фиксирования их местонахождения;

• учет документов, присланных во временное пользование (для согласования, ознакомления и т.п.);

• исключение возможности ознакомления работников службы КД с документами, составляющими особую ценность или имеющими помету «Лично»;

• предотвращение утраты документов или их частей за счет неполного изъятия их из пакетов;

• контроль соответствия количества поступивших документов количеству документов, переданных на регистрацию;

• установление связи исходящего номера поступившего документа с его регистрационным входящим номером и номером в передаточной учетной форме (журнале);

• обеспечение проверки наличия документов, зарегистрированных в пакетно-контрольном журнале (описи) учета пакетов.

Поступающие пакеты, конверты до их вскрытия и незаконвертованные документы должны быть зарегистрированы в традиционном или электронном журнале (описи) учета пакетов. Запись, сделанная в журнале, документирует факт доставки пакета или документа и является первоисточником, основанием для последующего контроля полноты состава зарегистрированных документов.

Графы журнала учета пакетов делятся на три зоны: а) исходные сведения о пакетах

(наименование и номер доставочного документа — реестра, расписки и др.; количество пакетов или незаконвертованных документов, экземпляров; подпись курьера, нарочного), б) исходные сведения о документах (порядковый номер пакета или незаконвертованного документа; номер документа, указанный на пакете; откуда поступил документ; количество листов в документе; входящий номер документа; подпись работника службы КД, подтверждающая получение пакета или документа, дата), в) рабочие сведения (инвентарный или другой регистрационный номер документа; отметка о возврате ошибочно присланных документов; отметка об отправлении или возврате документов).

В фирме должен быть установлен порядок, при котором все пакеты, конверты, а также незаконвертованные документы, поступающие по любой линии связи (в том числе получаемые от посетителей), принимались только работником службы КД, а в некрупных фирмах — секретарем-референтом первого руководителя. Это связано прежде всего с трудностью выделения конфиденциальных документов из общего потока корреспонденции. Трудность состоит в том, что, как правило, на пакетах, конвертах и часто на самих документах отправителем не ставится гриф конфиденциальности. Это объясняется не только сугубо индивидуальным подходом к присвоению информации статуса конфиденциальной, но и нежеланием отправителя обращать внимание посторонних лиц на гриф ограничения доступа.

Учитывая эту особенность, вскрытие конвертов, предварительное рассмотрение и распределение всей поступающей корреспонденции фирмы выполняется указанным выше работником, хорошо знающим структуру фирмы, функции структурных подразделений и сотрудников, состав конфиденциальной информации. Вскрываются все конверты (кроме имеющих помету «Лично»). Поступившие электронные документы первоначально вводятся в предварительный массив компьютера этого работника с целью выполнения указанных выше процедур. Введение электронных документов, а также электронных аналогов бумажных документов до регистрации сразу в рабочий массив компьютера не допускается.

Изъятые из пакетов, конвертов поступившие документы работник делит на две группы: имеющие гриф или какую-либо помету ограничения доступа и не имеющие такой пометы. Документы второй группы сравниваются с перечнем сведений, отнесенных к категории конфиденциальных. При совпадении содержания или его элементов, темы поступившего документа с одной из позиций перечня сотрудник ставит на документе гриф ограничения доступа необходимого уровня конфиденциальности, срок его действия и условия снятия, указанные в перечне. Внесенные сведения заверяются росписью руководителя службы КД. Документы, отнесенные к категории конфиденциальных (в том числе электронные, факсимильные и др.), вносятся в журнал (опись) учета пакетов с целью включения их в первичную систему обеспечения безопасности информационных ресурсов фирмы. Документы, не содержащие конфиденциальных сведений, передаются для дальнейшей обработки сотруднику службы открытой документации. Если документ поступил с грифом ограничения доступа, то этот гриф не может быть снят даже в случае, когда документ не входит в число конфиденциальных для данной фирмы. Гриф может быть изменен только в сторону повышения уровня конфиденциальности. Фирма обязана защищать не только свои секреты, но и секреты всех юридических и физических лиц, установивших с ней деловые контакты.

Следовательно, учет пакетов, конвертов и незаконвертованных документов является важным элементом обеспечения гарантированной сохранности поступивших документов и начальным этапом формирования их учетной базы.

Учет пакетов и незаконвертованных документов в технологическом аспекте тесно связан с учетом поступивших (входящих) конфиденциальных документов. Учету подлежат все зарегистрированные в журнале (описи) учета пакетов конфиденциальные документы независимо от предполагаемого периода их конфиденциальности.

Карточка учета входящего документа включает следующие зоны.

а) зона исходных сведений о документе (входящий номер и гриф конфиденциальности; дата поступления; исходящий номер документа и дата; количество листов основного документа и приложений; откуда поступил; вид документа и его краткое содержание),

б) зона сведений о месте хранения документа (индекс дела, номера листов дела, росписи, подтверждающие правильность отметок о подшивке документа; отметки о проверках наличия документа),

в) зона сведений о местонахождении (движении) документа (кому выдан; количество

листов основного документа и приложений;
роспись в получении и дата; роспись за возврат и дата; сведения о движении первого экземпляра карточки; отметка о проверке закрытия всех позиций карточки), г) зона сведений об отправке документа (куда направлен документ; количество листов основного документа и приложений; наименование и номер сопроводительного документа и его дата; росписи о проверке правильности отметок об отправке; отметка о возврате).
Традиционный или автоматизированный учет поступивших документов полностью соответствует рассмотренному выше типовому составу технологических процедур. Номер поступившего документа проставляется не только во входящем штампе на первом листе документа, но и на первом листе каждого приложения в штампе «К вх. № __ » с указанием года регистрации. Во входящем штампе документа дополнительно фиксируется количество листов основного документа и приложений с указанием грифа их конфиденциальности, например: «Количество листов: 1к + 5нк». При наличии в полученном конверте нескольких документов каждый из них учитывается за отдельным номером.
Следовательно, результатом традиционного или автоматизированного учета поступивших конфиденциальных документов должно стать подробное фиксирование исходных сведений о документе в целях последующего формирования справочно-информационного банка данных по документам, а в отдельных случаях — банка электронных документов.

6.2. Распределение, рассмотрение и направление документов на исполнение

По завершении процедур традиционного или автоматизированного учета поступившие конфиденциальные документы передаются для работы руководителям и сотрудникам фирмы. Следует помнить, что при выходе за пределы службы КД документы подвергаются широкому спектру реальных угроз за счет санкционированного включения в работу с ними значительного числа сотрудников и соответствующего возрастания количества источников, владеющих конфиденциальными сведениями. Передача документов сопровождается выполнением следующих процедур:
• распределение документов;
• рассмотрение документов руководителями;
• передача документов исполнителям или на другие участки службы КД.
Цель процедуры распределения поступивших документов — определение рационального пути (маршрута) дальнейшего движения документа в соответствии с его функциональной принадлежностью и местом в разрешительной системе доступа к конфиденциальной информации.
Реализация процедуры как традиционных, так и электронных документов основывается на анализе содержания документов, которое является главным критерием однозначного определения: кто из руководителей, кому из исполнителей (сотрудников), как, когда и с какими категориями документов разрешает знакомиться или работать. Любое обращение к конфиденциальному документу, ознакомление с ним в любой форме (в том числе случайное, несанкционированное) обязательно фиксируется в учетной карточке документа и на самом документе в виде соответствующей отметки и росписи лица, который обращался к документу. Этот факт указывается также в карточке учета осведомленности сотрудника в тайне фирмы.
В соответствии с системой доступа, функционирующей в фирме, поступившие традиционные и электронные документы распределяются на следующие группы:
• подлежащие рассмотрению первым руководителем;
• подлежащие рассмотрению конкретными заместителями первого руководителя;
• передаваемые руководителям структурных подразделений или направлений деятельности фирмы;
• передаваемые непосредственно исполнителям в соответствии со специальным перечнем.
При рассмотрении документов руководителем должны быть решены следующие задачи обеспечения защиты информации:
• принятие правильного решения по составу исполнителей, допускаемых к документу;
• исключение возможности ознакомления с документом посторонних лиц в процессе работы руководителей с документами;
• исключение возможности кражи или копирования документов посетителями, техническим и обслуживающим персоналом, секретарем и другими лицами;
• исключение возможности утечки информации по техническим каналам (визуальному,

акустическому или другим), например, при безответственном обсуждении содержания конфиденциального документа по незащищенным линиям связи;
• фиксирование факта передачи документа руководителю и возвращения документа от него;
• обеспечение физической сохранности всех частей документа (приложений, листов и т.п.).
Передача документов руководителям осуществляется работником службы КД под роспись в традиционном журнале учета документов, передаваемых руководству, или бумажном экземпляре аналогичного электронного журнала (описи). Роспись за документ ставится в учетной карточке документа в том случае, если руководитель является исполнителем данного документа. При рассмотрении документа в присутствии работника службы КД запись в журнале не делается. Передавать конфиденциальные документы руководителям через их секретарей или без росписи в учетной форме не разрешается.
Традиционные и электронные конфиденциальные документы перемещаются между руководителями или между руководителями и исполнителями только через службу КД. После рассмотрения документов руководитель возвращает их работнику службы КД. В учетную карточку документа переносятся из резолюции фамилии сотрудников фирмы, которым документ должен быть направлен. Резолюция в полном объеме в учетную форму не переносится. Если сотрудник допускается только к части документа, то в резолюции следует четко указывать конкретные пункты, разделы, страницы, приложения, с которыми этот сотрудник может быть ознакомлен.
Конфиденциальные документы, которые в соответствии с указанным выше перечнем не передаются на рассмотрение руководителю фирмы, направляются руководителям подразделений (направлений деятельности), главным менеджерам, отдельным сотрудникам. Адресование этих документов (их разметка) выполняется руководителем службы КД. Разметка оформляется в виде резолюции, но без указания задания по исполнению и срока исполнения.
Документы, возвращенные руководителем с резолюцией, и документы, прошедшие разметку в службе КД, передаются исполнителям для ознакомления, использования в работе или исполнения (работы с ними). Документы могут также быть переданы по передаточному журналу на другие участки службы КД — инвентарный, документов предварительного учета, архивный и др.
Ознакомление с конфиденциальным документом представляет собой процесс информирования сотрудника фирмы или иного заинтересованного лица, осуществляемый в соответствии с резолюцией руководителя, о принятом им решении или решении другой организационной структуры. Процесс завершается проставлением сотрудником на документе визы ознакомления и не требует, как правило, последующего составления другого документа или повторного обращения к этому документу. Ознакомление с документом производится в помещении службы КД. Документы, предназначенные для исполнения или использования в работе выдаются на рабочие места сотрудникам фирмы.
Работник службы КД, выдавая документы сотрудникам для ознакомления или работы, обязан:
• не допустить выдачу документа лицу, не имеющему права доступа к нему;
• в присутствии сотрудника проверить физическую сохранность документа, наличие всех приложений, листов и других частей документа, зафиксировать факт передачи документа в учетной форме под роспись сотрудника;
• знакомить сотрудника только с той частью документа, которая ему адресована; не разрешать сотрудникам при ознакомлении с документом делать выписки из текста на листочки, в записные книжки и т.п.;
• предотвращать любую возможность ознакомления с документом постороннего лица;
• обеспечить учет документов, находящихся у сотрудников, контроль сохранности этих документов в рабочее и нерабочее время.
Документы выдаются исполнителям для работы под роспись в традиционной учетной карточке или бумажном экземпляре электронной учетной карточки. Электронные документы передаются в копии в базу данных компьютера (рабочей станции) исполнителя с предварительным внесением исполнителем в электронную учетную карточку документа, находящуюся в компьютере службы КД, своей электронной подписи.
Все полученные исполнителем конфиденциальные документы (бумажные, на машинном носителе и электронные) в обязательном порядке вносятся им в традиционную

внутреннюю опись документов, находящихся у исполнителя. Опись предназначена для проверки наличия документов и записи отметок службы КД о возврате документов исполнителем. Опись хранится у исполнителя, ее электронный контрольный аналог может включаться в базу данных компьютера службы КД.

При возврате исполнителем документа в службу КД проверяется соответствие документа учетной форме и его комплектность, т.е. сохранность и целостность всех частей документа, листов. Количество листов обязательно просчитывается и вносится в учетную форму при любой передаче документа. Делается это с целью подтверждения факта сохранности, целостности листов и полного их приема исполнителем или работником службы КД. Кроме того, при просчитывании листов путем их перелистывания (перекладывания) выявляется возможная подмена листов или их порча (отрыв части листа, изменение формата листа и т.п.). Только после выполнения этих действий в учетной форме ставится отметка и роспись о приеме документа.

За возврат документа работник службы КД проставляет роспись в учетной карточке документа и внутренней описи документов, находящихся у исполнителя. Одновременно работник службы делает отметку о новом местонахождении документа в контрольно-учетном журнале (или электронной описи учетных карточек).

При передаче документа на другой участок службы КД для подшивки в дело, отправки, постановки на инвентарный учет и т.п. вместе с документом передается его учетная карточка, которая затем возвращается с отметкой о выполненных операциях. Росписи за полученные документы и карточки ставятся в передаточном журнале.

Следовательно, в процессе распределения, рассмотрения, передачи документов исполнителям и возврата документов выполняется комплекс технологических и ограничительных операций, позволяющих реализовать действующую в фирме разрешительную систему доступа к конфиденциальным документам и предотвратить разглашение или утечку информации, содержащейся в документе.

7. ТЕХНОЛОГИЯ ОБРАБОТКИ ПОДГОТОВЛЕННЫХ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ

7.1. Этапы подготовки конфиденциальных документов

Под исполнением конфиденциального документа понимается процесс документирования управленческих решений и действий, результатов выполнения руководителями и сотрудниками фирмы поставленных задач и отдельных заданий, поручений, а также реализации функций, закрепленных за ними в должностных инструкциях. Факторами, инициирующими процесс исполнения, являются:

- получение руководителем, сотрудником (исполнителем) поступившего документа;
- письменное или устное указание вышестоящего руководителя;
- устный запрос на информацию или принятие решения от других фирм, учреждений и отдельных лиц;
- задания и поручения, включенные в рабочие планы, графики работы, должностные инструкции и другие организационные и плановые документы;
- полезная информация, полученная из реферативных и информационных сборников, рекламных изданий. В отличие от исполнения процесс использования документа предполагает включение его в информационно-документационную систему, обеспечивающую исполнение других документов, выполнение управленческих действий и решений. Для использования в работе обычно поступают: законодательные акты, организационно-правовые, нормативные, распорядительные, справочно-информационные документы, разнообразные рекламные издания и научно-техническая информация.

В ходе исполнения конфиденциальные документы подвергаются максимально возможному спектру угроз, которые реализуются за счет:

- документирования конфиденциальной информации на случайном носителе, не входящем в сферу контроля службы КД;
- подготовки к изданию документа, не обоснованного деловой Необходимостью или не разрешенного для издания, т.е. документирования определенной информации;
- включения в документ избыточных конфиденциальных сведений, что равносильно разглашению тайны фирмы;
- случайного или умышленного занижения грифа конфиденциальности сведений, включенных в документ;
- изготовления документа в условиях, которые не гарантируют сохранность носителя, конфиденциальность информации;

• утери оригинала, черновика, варианта или редакции документа, его части, приложения к документу, умолчания этого факта и попытки подмены утраченных материалов;
• сообщения содержания проекта конфиденциального или открытого документа постороннему лицу, несанкционированного копирования документа или его части (в том числе на неучтенной дискете);
• утечки информации по техническим каналам;
• ошибочных действий работника службы КД, особенно в части нарушения разрешительной системы доступа к документам.
Передача конфиденциальной информации по деловой необходимости партнерам, посредникам, работникам государственных учреждений допускается только в случаях, установленных законодательством или соответствующим пунктом в контракте, и только по их письменному запросу с указанием конкретного состава и назначения требуемых сведений. Информация передается им всегда в письменном виде за подписью первого руководителя фирмы и с информированием об этом руководителя службы безопасности. Передача конфиденциальных сведений в устной форме не разрешается.
Исполнение конфиденциальных документов, в отличие от исполнения открытых документов, представляет собой стадию, насыщенную различными технологическими этапами и процедурами. Выделяются следующие основные этапы:
• установление уровня грифа конфиденциальности сведений, подлежащих включению в будущий документ;
• оформление и учет носителя для документирования выделенного комплекса конфиденциальной информации;
• составление вариантов и черновика текста документа;
• учет подготовленного черновика конфиденциального документа;
• изготовление проекта конфиденциального документа;
• издание конфиденциального документа. Указанные этапы характеризуются не только регламентированной технологией, но и жесткими правилами работы исполнителей с конфиденциальной информацией. Сам факт запечатления ценной информации на носителе предполагает наличие защитных мер в отношении информации и носителя от различных рисков.
Общеизвестно, что в наибольшей безопасности находится конфиденциальная информация, не зафиксированная ни на каком носителе. Угрозы ценной информации появляются немедленно при возникновении мысли о необходимости ее документирования. В связи с этим система защиты конфиденциальной информации должна начинать функционировать не после издания (подписания) конфиденциального документа, а заблаговременно, т.е. до момента нанесения на чистый лист бумаги первых письменных знаков будущего документа. Перед реализацией мысли о создании документа первоначально решаются вопросы: а) является ли данная информация конфиденциальной и, если да, то б) какой уровень грифа конфиденциальности ей должен быть присвоен.
Своевременное установление уровня грифа конфиденциальности сведений, подлежащих включению в будущий документ, является первым и основным элементом защиты документированной информации, позволяющим обеспечить относительно надежную безопасность тайны фирмы.
В основе присвоения документу грифа конфиденциальности должны лежать перечень конфиденциальных сведений фирмы, требования партнеров, условия контрактов, а также перечень конфиденциальных документов фирмы. Система грифования (маркирования) документов не гарантирует сохранности информации, однако позволяет четко организовать работу с документами и, в частности, сформировать систему доступа к документам персонала.
Гриф конфиденциальности или гриф ограничения доступа к традиционному, машиночитаемому или- электронному документу представляет собой реквизит (элемент, служебную отметку, помету, пометку) формуляра документа, свидетельствующий о конфиденциальности содержащихся в документе сведений и проставляемый на самом документе и (или) сопроводительном письме к нему.
Информация и документы, отнесенные к коммерческой тайне, имеют несколько уровней грифа ограничения доступа, соответствующих различным степеням конфиденциальности информации.
Первый, массовый, уровень — грифы «Конфиденциально», «Конфиденциальная информация».

Не следует ставить гриф «Коммерческая тайна», так как грифом обозначается не вид тайны, а характер ограничения доступа к документу.
Второй уровень достаточно редкий — грифы «Строго конфиденциально», «Строго конфиденциальная информация», «Конфиденциально. Особый контроль». Этот гриф присваивается документу лично первым руководителем фирмы, им изменяется или отменяется. Исполнение, использование и хранение документов с этим грифом также организуется первым руководителем с возможным привлечением руководителя службы **КД. Исполнителям** документы с этим грифом не передаются.
На документах, содержащих сведения, отнесенные к служебной тайне, ставится гриф «Для служебного пользования» или «Конфиденциально».
Гриф ограничения доступа, указываемый на документе, пишется полностью и не сокращается. Под обозначением грифа указывается номер экземпляра документа, срок действия грифа и иные условия его снятия. Гриф располагается в соответствии с ГОСТ Р 6.30-97 на первом и титульном листах документа, а также на обложке дела (тома) в правом верхнем углу. На электронных документах и документах, записанных на любых машинных носителях, гриф обозначается на всех листах. Ниже грифа или ниже адресата могут обозначаться ограничительные пометы типа: «Лично», «Только в руки», «Только адресату», «Лично в руки» и др. При регистрации конфиденциальных документов к его номеру добавляется сокращенное обозначение грифа конфиденциальности, например: № 37к, 89ск, 97дсп.
Документы и информация, конфиденциальные в целом (например, документация службы персонала, службы безопасности, документы, отнесенные к профессиональной тайне, и т.д.), как правило, не маркируются, потому что в полном объеме обладают строгим ограничением доступа к ним персонала.
На ценных, но неконфиденциальных документах может проставляться помета (отметка, надпись, штамп), привлекающая особое внимание к сохранности таких документов. Например: «Собственная информация фирмы», «Информация особого внимания», «Копии не снимать», «Хранить в сейфе» и др. Может ставиться штамп, что данная информация без согласия фирмы не может быть использована в каких-либо коммерческих целях и по миновании надобности должна быть возвращена собственнику. Гриф или штамп обязательно проставляются при направлении конфиденциальной для фирмы информации в государственные учреждения, которые обязаны держать ее в тайне.
Гриф конфиденциальности присваивается документу:
• исполнителем при подготовке к составлению проекта документа;
• руководителем структурного подразделения (направления деятельности) или руководителем фирмы при согласовании или подписании документа;
• работником службы КД при первичной обработке поступающих документов, если конфиденциальный для фирмы документ не имеет грифа ограничения доступа.
Изменение или снятие грифа конфиденциальности документа производится при изменении степени конфиденциальности и ценности содержащихся в нем сведений. Основаниями для этих действий являются: соответствующая корректировка перечней конфиденциальных сведений или документов фирмы; истечение установленного срока действия грифа; наличие события, при котором гриф должен быть изменен или снят (например: опубликование ноу-хау в печати, патентование изобретения и др.); установление факта неправильности присвоения грифа документу.
Руководители всех рангов и исполнители несут персональную ответственность за своевременное и правильное установление, изменение и снятие грифа конфиденциальности. Фактическое изменение или снятие грифа осуществляет должностное лицо, подписавшее (утвердившее) документ, а также первый руководитель фирмы.
Процедуры изменения и снятия грифа конфиденциальности с документов фирмы должны быть четко регламентированы. В целях своевременного информирования соответствующих должностных лиц о необходимости выполнения этих процедур сотрудник службы КД должен регулярно просматривать учетные карточки или инвентарные описи конфиденциальных документов и выявлять те документы, по которым могут быть изменены характеристики ограничения доступа. При изменении иди снятии грифа полномочное должностное лицо делает отметку на самом документе и в сопроводительном письме путем зачеркивания грифа или написания нового, указания основания для выполнения этого действия и проставления подписи и даты. В соответствии с этой отметкой делаются необходимые записи в учетной форме документа. После снятия грифа документ передается в службу

открытого делопроизводства фирмы. При необходимости об изменении или снятии грифа конфиденциальности с документа сообщается заинтересованным фирмам и предприятиям.
Другим принципиально важным вопросом, решаемым заблаговременно руководством фирмы, службой КД и исполнителями, т.е. до начала составления текста документа, является определение необходимости предварительной регистрации носителя (листов бумаги, специальных тетрадей и блокнотов с отрывными листами, листов ватмана, фотопленки, магнитных носителей и т.п.), на котором будет формироваться черновик и беловик документа.
Назначение учета носителей конфиденциальной информации состоит в том, чтобы обеспечить безопасность информации, контроль за ней не только в подлиннике документа, но и во всех черновых материалах, вариантах и редакциях документа, отдельных записях и подготовительных материалах. На чистом носителе информации ставится избранный гриф конфиденциальности будущего документа.
Носителями документированной конфиденциальной информации могут быть:
• для традиционных текстовых документов — специальный блокнот с отрывными листами и корешком, выполняющим функцию учета листов, нанесения отметок о целевом их использовании; рабочая тетрадь для больших по объему документов; отдельные пронумерованные листы бумаги, типографские формы и бланки документов;
• для чертежно-графических документов — пронумерованные листы ватмана, кальки, пленки, координатной бумаги и т.п.;
• для машиночитаемых документов — маркированные и пронумерованные магнитные ленты, диски, дискеты, карты и т.п.;
• для аудио- и видеодокументов — маркированные и пронумерованные кассеты с магнитной пленкой, лазерные диски, кассеты с кинопленкой и т.п.;
• для фотодокументов — маркированные и пронумерованные кассеты с фотопленкой, фотобумага, микрофиши, слайды, кассеты с микрофотопленкой.
Основные задачи учета носителей конфиденциальной информации или, как часто их называют в научной литературе, — документов предварительного учета:
• закрепление факта присвоения носителю категории конфиденциальности, ограниченного доступа;
• присвоение носителю учетного номера и включение его в справочно-информационный банк для обеспечения контроля за использованием и проверки наличия;
• документирование фактов перемещения носителя между сотрудниками фирмы, закрепление персональной ответственности за его сохранность;
• контроль работы исполнителя над документом и своевременного уничтожения носителя или его частей, потерявших практическое значение.
При учете носителей реализуются следующие требования обеспечения защиты информации:
• формирование основы для последующей персональной ответственности сотрудника за сохранность носителя, повышенного внимания к нему;
• предупреждение возможности нецелевого использования носителя или его неправильного хранения;
• формирование грифа конфиденциальности будущего документа;
• предупреждение возможности тайной подмены носителя, изъятия из него или включения в него отдельных частей (листов, кусков фото-, видео- или магнитной пленки), для чего фиксируются технические характеристики носителя (количество листов, длина ленты, наличие склеек и др.);
• предупреждение технической возможности тайной разборки кассет, пеналов, футляров, конвертов и иных оболочек, содержащих технические носители информации;
• включение носителя в сферу регулярного контроля сохранности и местонахождения.
В службах КД коммерческих фирм бумажные носители текстовой и технической информации ставятся на инвентарный (перечневый) учет. Специальный учет носителей текстовой информации не ведется. Кроме того, в этих структурах учет носителей целесообразен только на уровне руководства фирмы, так как именно здесь концентрируется вся действительно ценная информация. На уровне исполнителей документирование элементов конфиденциальной информации ведется на неучитываемых предварительно носителях. Однако не следует думать, что неучитываемый носитель — это любой кусок бумаги, на котором можно фиксировать конфиденциальные сведения и который затем можно смять и выбросить в мусорную корзину. Неучитываемый носитель — это блокнот или тетрадь с пронумерованными листами, наличием заверительной надписи и росписью целевого

использования каждого листа. Обязательно учитываются типовые формы и бланки документов. На чистых листах бумаги ставится штамп службы КД, листы нумеруются. У носителя может отсутствовать учетный номер, но в опись документов, находящихся у исполнителя, он обязательно вносится. Исполнитель в любой момент должен быть готов отчитаться об использовании каждого листа.

В производственных и исследовательских фирмах, обладающих оригинальными технологиями и производственными секретами типа «ноу-хау», конфиденциальные документы на всех уровнях управления целесообразно составлять только на предварительно учтенных носителях информации.

Обязательному инвентарному учету и маркировке на всех уровнях управления подлежат магнитные носители информации, для которых любые угрозы представляют значительно большую опасность, чем для бумажных, а обнаружение реализации этих угроз возможно только на основе сложных аналитических наблюдений. Маркировка предусматривает нанесение на носитель инвентарного номера, даты регистрации, наименования структурного подразделения и фамилии исполнителя. Надписи делаются механически стойким красителем. Одновременно этим же веществом окрашиваются винты и иные детали, скрепляющие корпус кассеты, дискеты или футляра с целью сигнализации об их несанкционированном вскрытии.

Этапы оформления и учета носителей конфиденциальной информации, выдачи их исполнителям и приема от исполнителей Выполняются в службе КД как в традиционном, так и автоматизированном режимах и включают в себя следующие процедуры:

• первичное оформление носителя, в процессе которого выполняются специализированные операции, позволяющие в дальнейшем контролировать подлинность носителя и сохранность всех его элементов;

• традиционный или автоматизированный учет носителя, при котором документируется факт включения носителя в категорию носителей ограниченного доступа с присвоением ему инвентарного номера;

• окончательное оформление носителя, в процессе которого учетные данные переносятся на носитель и его составные части для их идентификации;

• выдача учтенного, укомплектованного носителя информации исполнителю, закрепление за исполнителем персональной ответственности за сохранность носителя, его целостность и целевое использование;

• выдача исполнителю при необходимости дополнительных учтенных листов, форм и бланков;

• прием от исполнителя носителя информации, в процессе которого проверяются комплектность носителя, наличие оправдательных отметок за отсутствующие элементы и документирование факта передачи носителя в службу КД;

• ежедневная проверка правильности учета носителей и их наличия.

При работе с исполнителями работник службы КД педантично решает следующие задачи обеспечения защиты информации:

• предотвращение выдачи носителя лицу, не связанному с составлением конкретного документа или исключенному из состава лиц, допускаемых к данному носителю (составляемому документу);

• выявление факта утраты носителя или его частей, организация поиска носителя и проведения служебного расследования;

• предотвращение нарушения принципа персональной ответственности за сохранность носителя и фиксируемой в нем информации;

• обнаружение факта подмены носителя другим, фальсификации части носителя;

• обнаружение фактов случайной или умышленной порчи носителя» изменения формата, нумерации листов, вырывания листов, их загрязнения, склеивания и т.п.);

• предотвращение несанкционированной и неоправданной деловой необходимостью передачи носителя между руководителями и исполнителями;

• предотвращение несанкционированного ознакомления посторонних лиц с содержанием информации, зафиксированной на носителе, в процессе его выдачи исполнителю и прием от исполнителя.

Следовательно, до начала составления черновика конфиденциального документа должен быть выполнен ряд принципиально важных технологических этапов обеспечения сохранности тайны фирмы, которые дают возможность в будущем свести к минимуму риск утраты ценной информации, чье документирование пока только предполагается.

Этап составления текста конфиденциального документа методически мало отличается от аналогичной творческой, формальнологической и технической работы, проводимой при формировании содержания открытого документа. Однако исполнителю следует всегда помнить, что конфиденциальная информация документируется только при наличии серьезных объективных потребностей, а не субъективного желания сотрудника фирмы. Конфиденциальные документы составляются в строго определенных случаях, например: когда процесс или результат какой-то работы подлежит обязательному отражению в конкретных документах (обязательному документированию) или когда наличие этих документов или переписки диктуется реальной необходимостью, т.е. отсутствием условий для решения конфиденциального вопроса путем личного (но не телефонного) общения между партнерами.

Работникам службы КД необходимо знать, что контроль за работой персонала фирмы с любыми конфиденциальными документами, особенно в процессе документирования конфиденциальной информации, — это одна из главных их задач. Ответственное отношение сотрудников фирмы к своим обязанностям в значительной степени гарантирует сохранность тайны фирмы даже при отсутствии дорогостоящих и современных технических средств защиты конфиденциальной информации.

Составление текстов особо ценных конфиденциальных документов обычно централизуется на уровне руководства фирмы. Менее значимые конфиденциальные документы по отдельным функциональным вопросам составляются децентрализованно руководителями структурных подразделений (направлений деятельности) фирмы и иногда допущенными к этой работе исполнителями (опытными менеджерами, экспертами). Любые черновики, варианты, редакции конфиденциальных документов (в том числе электронных), относящиеся к ним материалы, записи, записки и т.п., составляются на заблаговременно подготовленных носителях.

При документировании конфиденциальной информации следует учитывать, что:

• объем включаемых в документ конфиденциальных сведений должен быть минимальным и определяться реальной ситуацией;

• документ всегда должен касаться только одного вопроса (темы), что важно не столько для быстрого доведения документа до исполнителя, сколько для обеспечения четкого функционирования системы доступа персонала к конфиденциальной информации, необходимой только данному сотруднику, и предотвращения несанкционированного ознакомления сотрудников фирмы и иных лиц с излишней информацией;

• необходимо заблаговременно предусмотреть, чтобы сводные плановые, организационные, распорядительные (особенно приказы по основной деятельности), отчетные и другие подобные документы, составляемые в виде сложных многоадресных схем текстовой части заданий и исполнителей, в полном объеме не рассылались по подразделениям и исполнителям; такие документы доводятся до исполнителей избирательно, в виде составленных в рамках этих документов функциональных персонифицированных приложений-заданий или отдельных документов; документы, сохраняющие исторически сложившуюся сложную, многостраничную традиционную форму текста, являются серьезным каналом утраты ценной информации;

• информация, относящаяся к тайне фирмы, должна быть максимальным образом локализована в конкретной части документа, его разделе, приложении, отдельной дискете, электронном массиве с усложненной системой доступа (например, большой по объему неконфиденциальный документ может иметь раздел, выделенный в отдельную часть и содержащий комплекс информации ограниченного доступа);

• включаемые в документ конфиденциальные фотоиллюстрации, графики, схемы и т.п. наклеиваются на учтенные листы, их количество оговаривается в сопроводительном письме или специальной записи;

• не допускается снимать копии и делать выписки из ранее изданных конфиденциальных документов без разрешения соответствующего должностного лица или организации-автора;

• конфиденциальные показатели (формулы, выводы, результаты наблюдений, опытов, описания технологических процессов и т.п.) должны фиксироваться в документе только один раз; при необходимости повторного их описания делается ссылка на документ, в котором они были ранее отражены;

• в неконфиденциальных документах не допускаются намеки на наличие конфиденциальных сведений или их описание в произвольной форме;

• сопоставление плановых и отчетных показателей деятельности фирмы, результаты перспективных маркетинговых исследований, аналитические выводы по производству и продаже продукции, параметры новой технологии, характеристики ноу-хау и т.п. допускается документировать и хранить только на уровне первого руководителя фирмы в документах, делах, базах данных с грифом «Строго конфиденциально»;
• не допускается включение в неконфиденциальные документы сведений, составляющих интеллектуальную собственность или коммерческую тайну других фирм или лиц (даже при отсутствии соответствующего пункта в договоре о сотрудничестве);
• для обеспечения высокого уровня конфиденциальности документов, пересылаемых обычной почтой, передаваемых по незащищенным каналам связи и хранящимся в компьютерах, целесообразно решить вопрос о шифровке информации.

Документирование конфиденциальной информации это более сложный процесс по сравнению с аналогичной работой по составлению открытого документа, что определяется объективной необходимостью создать условия для обеспечения сохранения в тайне сведений, включаемых в документ.

Следовательно, подготовка проекта конфиденциального документа представляет собой трудоемкий процесс из-за необходимости выполнения дополнительных вспомогательных этапов, не свойственных аналогичной работе над открытым документом. Эти этапы имеют важное значение для обеспечения защиты информации при подготовке конфиденциального документа и предусматривают установление грифа конфиденциальности будущего документа, оформление и учет его носителя.

7.2. Учет, изготовление и издание документов

Говоря о технологии подготовки к документированию и документировании конфиденциальной информации мы отметили наличие двух специфических особенностей (дополнительных этапов), необходимых для обеспечения заблаговременного сохранения в тайне содержания создаваемого документа: присвоение будущему документу определенного уровня грифа конфиденциальности и предварительный учет того носителя, на котором этот документ будет составляться. Следующая, третья, специфическая особенность состоит в том, что ни один проект конфиденциального документа не может быть изготовлен с черновика и обрести статус правомерно документированной информации без санкции (письменного разрешения) полномочного должностного лица фирмы.

Причина появления этой особенности заключается в необходимости документирования такого правового события, как зарождение персональной ответственности данного должностного лица за издание конкретного документа, т.е. распространение конфиденциальных сведений и соответствующее увеличение состава источников, владеющих данной информацией. Исполнитель документа таким правом обладать не может в силу того, что он лишь потребитель информации, а не ее собственник или владелец. Если решение об издании открытого документа принимается руководителем при подписании готового беловика документа, то вопрос об издании конфиденциального документа решается этим руководителем еще до изготовления первого проекта документа на основании анализа сложившейся ситуации и ознакомления с черновиком будущего документа.

Разрешение фиксируется двумя способами: или утвержденным первым руководителем фирмы перечнем (табелем, списком) издаваемых в подразделениях конфиденциальных документов, или индивидуальным разрешением в виде соответствующей подписанной этим руководителем записи на черновике документа. На черновике документа, вошедшего в указанный перечень, исполнитель указывает: наименование подразделения (направления деятельности) фирмы, свою фамилию и номер телефона, количество необходимых экземпляров проекта документа, номер формы бланка или типовой формы. Отметка заверяется росписью исполнителя. **Во** втором случае эта отметка утверждается разрешающей визой соответствующего руководителя фирмы.

Четвертая и, пожалуй, наиболее существенная особенность документирования конфиденциальной информации, касающаяся уже непосредственно технологических процедур изготовления самого документа, состоит в централизованном учете — присвоении единого учетного номера черновику и проекту будущего документа. Одновременно на еще не изготовленный документ в службе КД заполняется комплект учетных карточек. Полученный черновиком документа учетный номер будет сопровождать проект документа, а затем и сам документ в течение его последующего «жизненного

цикла». Обязательно учитываются проекты подготовленных конфиденциальных электронных документов, телетайпограмм, факсов и телеграмм. Ответным документам присваивается новый учетный номер. Приложения к подготовленным конфиденциальным документам являются самостоятельными документами и имеют свои учетные номера по соответствующим видам учета, в том числе номер открытого документа, если приложение не содержит защищаемых сведений.

В случае когда исполнитель имеет разрешение на самостоятельное изготовление конфиденциальных документов, перед выполнением этого этапа он обязан передать черновик в службу КД для учета. После регистрации черновик возвращается исполнителю под роспись в учетной карточке подготовленного документа. Учету подлежат черновики всех конфиденциальных документов независимо от места их составления и последующего изготовления проекта документа.

В учетной карточке подготовленного документа отражается последовательно ход работы над проектом документа в процессе его изготовления, издания, последующего исполнения или отправки, хранения или уничтожения. Карточка включает в себя следующие зоны: а) зону исходных сведений о документе (учетный номер и гриф конфиденциальности; дата печатания, вид и краткое содержание, подразделение и фамилия исполнителя, номер носителя, с которого печатался проект документа и др.), б) зону рабочих сведений о документе (росписи за уничтожение черновика и дата; дата выдачи; количество листов, экземпляров; кому выдан и др.), в) зону отметок об отправлении и возврате документа, г) зону отметок о передаче документа на другие участки службы КД или движении документа, д) зону отметок о подшивке документа в дело или взятии его на инвентарный учет, е) зону отметок об уничтожении документа. Учетная карточка регистрируется в журнале учета карточек подготовленных документов, имеющем графы: учетный номер и гриф конфиденциальности; подпись сотрудника участка подготовленных документов за получение карточки документа и дата; примечание.

Как мы видим, подготовленный черновик и проект будущего документа постоянно находятся под контролем службы КД независимо от места и способа их изготовления. Этим в определенной мере обеспечивается сохранность информации, которую руководство фирмы решило зафиксировать на том или ином типе носителя. Если открытые документы регистрируются только после их подписания или утверждения руководителем, то конфиденциальные документы — до изготовления проекта документа с черновика. Процесс превентивного, предупредительного контроля за документированием конфиденциальной информации и технологическая реализация этого процесса входят обязательной составной частью в структуру системы защиты информации от несанкционированного доступа к информации постороннего лица и утраты носителя и конфиденциальности информации. Интересно, что еще не согласованный окончательно, не подписанный и не утвержденный проект конфиденциального документа на этапе окончания работы над черновиком обязательно зафиксирован по двум видам учета: во-первых, по учету носителей документированной информации и, во-вторых, по учету подготовленных документов, в учетной карточке которого последовательно отражается ход работ над проектом документа в процессе его изготовления, издания, последующего исполнения или отправки, хранения или уничтожения.

Целью этапа изготовления конфиденциального документа является перепечатывание черновика документа и создание оформленного в соответствии с государственным стандартом оригинала (беловика) проекта документа, предназначенного по окончании этапа издания стать подлинником документа.

В процессе изготовления конфиденциального документа должны быть решены следующие задачи обеспечения защиты информации:

• предотвращение несанкционированного изготовления конфиденциального документа кем-либо из персонала фирмы, даже при наличии объективных предпосылок для такого действия; ссылки на последующее получение разрешения на издание не должны иметь силы;

• обеспечение контроля за сохранностью носителей, на которых последовательно изготовляются черновик, проект документа и его варианты; контроль за сохранностью и порядком уничтожения испорченных носителей посредством установления информационной связи различных форм учета: например, учета носителя, учета черновика и изготовленного проекта документа, инвентарного учета и других;

• обеспечение тайны информации путем изготовления документа в специально

оборудованном помещении, оснащенном комплексом технических средств защиты информации и исключающем нахождение в нем посторонних лиц;
• обеспечение оперативных и результативных проверок наличия, комплектности, целостности и подлинности документов путем нанесения на проект документа учетных и защитных отметок.
Этап изготовления конфиденциальных документов включает следующие технологические процедуры:
• прием работником службы КД от исполнителя черновика документа;
• традиционный Или автоматизированный учет черновика и проекта подготовленного документа;
• печатание и выдача черновика и проекта документа исполнителю;
• перепечатывание отдельных листов и документа в целом;
• снятие копий с документа, производство выписки и изготовление дополнительных экземпляров документа;
• ежедневная проверка наличия у работника службы КД черновиков и проектов документов, находящихся на этапе изготовления.
При полном перепечатывании документа его новый вариант регистрируется за новым учетным номером. Новый учетный номер присваивается также копиям и выпискам из документа. Дополнительно размноженные экземпляры документа учитываются в карточке и за номером основного документа с проставлением соответствующей отметки на размноженном документе и учетной карточке. Ценные текстовые и табличные конфиденциальные документы с грифом строгой конфиденциальности изготавливаются централизованно в помещении службы КД с использованием пишущих машин или персональных ЭВМ. Информационные показатели в черновиках этих документов не указываются, а вписываются от руки первым руководителем в уже изготовленный экземпляр документа.
Основная масса проектов типовых по содержанию конфиденциальных документов может с разрешения первого руководителя фирмы изготавливаться децентрализованно самими исполнителями и руководителями непосредственно на рабочих местах при наличии специального защитного оборудования в их кабинетах, рабочих комнатах и с соблюдением общего прядка учета этих документов. Проект документа, изготовленный лично исполнителем или руководителем, немедленно передается им в службу КД вместе со всеми сопутствующими материалами для внесения необходимой записи в учетную карточку. После выполнения этой операции проект документа и все материалы возвращаются исполнителю под роспись в учетной карточке.
При этом следует помнить, что исполнителям не разрешается передавать черновики документов для печатания техническим сотрудникам подразделения, не имеющим допуска к выполнению подобной работы. Изготовление конфиденциальных документов осуществляется только на выделенных для этих целей пишущих машинках, компьютерах и принтерах. Эти средства должны находиться под контролем специалистов службы безопасности.
Чертежно-графическая документация изготавливается децентрализованно исполнителями с соблюдением установленных правил и под контролем руководителя подразделения (направления деятельности) фирмы и службы КД.
Конфиденциальные документы могут копироваться и размножаться с помощью соответствующей организационной техники и с соблюдением действующих требований по защите информации и сохранности всех сопровождающих этот процесс промежуточных носителей (печатных форм). Копирование и размножение конфиденциальных документов всегда санкционируется полномочным должностным лицом с проставлением необходимых записей в учетной форме основного документа и на самом документе. Копировальная техника должна располагаться в помещении службы КД. Множительная техника обслуживается специалистами соответствующего структурного подразделения фирмы.
На принтере, как правило, изготавливается только один экземпляр конфиденциального документа. После окончательного согласования с него па копировальном аппарате снимается количество копий, указанное на обороте документа.
В ходе изготовления конфиденциальных документов не должна использоваться новая красящая лента и копировальная бумага. Под валик печатающего устройства нельзя подкладывать дополнительные уплотняющие листы бумаги. Документы не должны диктоваться или записываться на диктофон, так как это может образовать эффективный

акустический канал утечки информации. Испорченные листы и материалы, сопутствовавшие составлению и изготовлению документа, не следует выбрасывать в мусорную корзину, их необходимо помещать в специальные сборники и затем уничтожать в установленном порядке.

На последнем листе всех экземпляров отпечатанного документа (на лицевой или оборотной стороне) проставляются учетный номер, гриф конфиденциальности документа, фамилия исполнителя и номер его телефона, фамилия лица, печатавшего документ, и дата. Указывается количество изготовленных экземпляров и при необходимости — адресность каждого из них. Может указываться номер магнитного носителя, с которого печатался документ. Кроме того, учетный номер с указанием грифа конфиденциальности проставляется на нижнем поле каждого листа документа, что закрепляет каждый лист за документом определенного номера. Количество экземпляров документа определяет исполнитель, исходя из реальной потребности в них.

Особо ценные документы на бумажных носителях могут при необходимости снабжаться специальными защитными средствами, препятствующими попыткам копирования или фальсификации документов, например угасание текста при копировании документа, использование красящих лент, отпечаток которых не воспроизводится при копировании или фотографировании, проставление условно случайных знаков в установленных местах, не воспроизводимых в процессе копирования или фальсификации.

При изготовлении документов на машиночитаемых носителях могут производиться следующие действия, затрудняющие несанкционированный доступ к этим документам: шифрование всего или части текста документа, внесение программных дополнений, не позволяющих посторонним лицам прочитать или скопировать документ. После изготовления с помощью компьютера бумажного или (и) машиночитаемого конфиденциального документа информация с магнитного диска, который использовался при составлении текста документа, стирается. Дискеты подлежат многократному форматированию или физическому уничтожению. Факт уничтожения информации подтверждается росписями исполнителя и работника службы КД в учетной форме документа и аппаратном журнале компьютера.

Этап издания конфиденциальных документов технологически не отличается от процесса придания открытому документу юридической силы. Однако при издании конфиденциальных документов должны быть решены следующие задачи обеспечения защиты информации:

• предотвращение доступа к документу должностных лиц и сотрудников, не имеющих служебного отношения к данному документу;

• предупреждение утраты документа или его частей, элементов текста в процессе передачи документа при издании;

• перекрытие визуальных и акустических каналов в процессе обсуждения с должностными лицами содержания документа. Издание документа включает в себя следующие последовательно выполняемые процедуры:

• заключительное корректирование текста и подготовка документа к изданию (подбор необходимых материалов, предыдущих документов, уточнение фамилий руководителей и исполнителей, сроков исполнения, указанных в тексте, исправление допущенных неточностей и др.);

• итоговое внутреннее согласование документа (предварительное согласование проводилось при работе над черновиком и проектом документа);

• внешнее согласование документа;

• подписание документа руководителем;

• утверждение, одобрение документа (при необходимости). Процедуры этапа организует лично исполнитель документа. При направлении проекта документа должностному лицу на срок более одного дня передача осуществляется через службу КД с внесением необходимых отметок в учетную форму документа и внутреннюю опись документов, находящихся у должностного лица. Факт передачи документа на срок до одного дня фиксируется росписью должностного лица во внутренней описи документов, находящихся у исполнителя.

Проекты конфиденциальных документов должны обязательно визироваться руководителем службы КД. При визировании ему предъявляются все экземпляры документа со всеми приложениями, а также их учетные формы. Если в процессе визирования или подписания проекта документа принимается решение об изменении уровня грифа конфиденциальности, то такое изменение должно быть срочно внесено во все экземпляры документа,

черновик, редакции документа, в учетные формы и описи. Изменение грифа во всех указанных материалах заверяется росписью работника службы КД и датируется.
Следовательно, этапы изготовления и издания конфиденциальных документов характеризуются наличием комплекса специфических ограничительных и учетных процедур, предназначенных для защиты носителя и конфиденциальности информации. Особое значение в этом комплексе имеет процедура учета подготовленного черновика и проекта документа, которая дает возможность организовать постоянный контроль за движением проекта документа и работой исполнителя с ним.

7.3. Технология контроля исполнения документов и поручений

Контроль исполнения конфиденциальных документов включает в себя непосредственную проверку и регулирование хода исполнения, учет и анализ результатов исполнения контролируемых документов в установленные сроки.
Учитывая сложный и неординарный характер функции контроля исполнения документов и поручений, ее в предметном плане можно условно разделить на два неразрывно связанных компонента: контроль исполнения документов по существу затронутых в них вопросов и контроль сроков исполнения этих решений. Такое деление является условным и служит лишь целям изучения объекта исследования, его регламентации и совершенствования,
Контроль фактического исполнения документов по существу затронутых в них вопросов осуществляют: руководитель фирмы, его заместители, руководители структурных подразделений и другие должностные лица. Эту работу они ведут лично или с помощью уполномоченных ими сотрудников, например помощников, референтов, экспертов, советников, кураторов и других лиц.
Контроль сроков исполнения документов (сроковый контроль) является обеспечивающей, информационной частью фактического контроля и сосредоточивается в службе КД.
Основные задачи системы срокового контроля за исполнением документов:
• запоминать все поставленные на контроль документы, указания, поручения, задания, мероприятия, управленческие решения и помнить о них до окончания реального выполнения;
• формировать справочно-информационный банк данных по контролируемым документам и поручениям;
• корректировать массив хранимой контролируемой информации при изменении срока исполнения, состава исполнителей, содержания заданий и при движении документа в процессе работы с ним;
• информировать руководителей, специалистов (исполнителей) и сотрудников службы КД о состоянии и ходе исполнения документов, осуществлять оперативный поиск справочных сведений о документах;
• напоминать (сигнализировать) руководителям и исполнителям о наличии неисполненных документов и поручений;
• фиксировать факты исполнения или неисполнения контролируемых документов;
• анализировать уровень исполнительской дисциплины в фирме в целом, по структурным подразделения, специалистам, видам документов и другим аспектам. Контроль исполнения документов включает в себя две обязательные составные части: предупредительный контроль и контроль последующий.
Предупредительный (текущий, оперативный) контроль оказывает активное управленческое влияние на ход исполнения документа и осуществляется путем периодической проверки и регулирования процесса исполнения, сигнализирования руководителям и исполнителям о приближении срока окончания работы над документом. Ведется в течение всего периода исполнения документа. Всегда носит индивидуальный характер по отношению к документу, поручению, заданию и охватывает массив, как правило, наиболее важных документов.
Последующий (итоговый, сплошной} контроль проводится периодически (еженедельно, ежемесячно, ежеквартально). Он представляет собой аналитическое обобщение исполнительской дисциплины в структурных подразделениях фирмы и по исполнителям. При отсутствии в фирме предупредительного контроля последующий контроль решает только одну задачу — констатацию факта выполнения или невыполнения того или иного решения, когда сроки его исполнения истекли и исправить создавшееся, часто критическое, положение уже практически невозможно.
В основе рациональной организации контроля исполнения документов в фирме лежит

определение категорий документов, подлежащих контролю, установление сроков их исполнения и правильное построение технологического процесса контроля исполнения, в том числе прямой и обратной связи с исполнителями контролируемых документов.
Контролю исполнения подлежат все зарегистрированные документы, требующие принятия решения и (или) выполнения определенных управленческих действий, составления ответного или иного документа, внесения изменений в нормативные, инструктивные, плановые и другие документы.
Предметом контроля в распорядительных, плановых и других подобных документах, решениях коллегиальных органов являются не сами документы, а содержащиеся в них задания. Контролируется процесс ознакомления руководителей и специалистов с документами, предназначенными для использования в работе (приказами, инструкциями и др.) или присланными во временное пользование, для согласования или утверждения.
В деятельности фирм сложилась практика постановки на контроль не всех документов, требующих проверки исполнения, а определенной Группы (категории), т.е. индивидуальный выборочный контроль исполнения, позволяющий наиболее внимательно и технологически четко организовать наблюдение за исполнением наиболее ценных документов и производимых работ. Ставятся на контроль обычно поручения и документы вышестоящих органов управления, распорядительные документы данной фирмы и решения ее коллегиальных органов управления, важнейшие документы других учреждений, плановые, программные документы, графики важнейших работ и т.д.
Любой контролируемый документ всегда должен иметь строго определенный срок исполнения. Срок исполнения документов может быть типовым и индивидуальным.
Типовой срок указывается в перечне документов, подлежащих обязательному контролю. Как правило, типовой срок исполнения основной массы документов 10—15 дней. Для документов, не указанных в перечне, сроки исполнения не должны превышать 10 дней.
Индивидуальный срок исполнения документа определяется руководителем и фиксируется в распорядительных пунктах документа или резолюции. Этот срок не должен быть больше типового для данной категории документов. В распорядительных документах и документах коллегиальных органов индивидуальный срок исполнения указывается отдельно в каждом пункте — по заданиям и поручениям. Следует помнить, что срок исполнения — это конечная дата работы над документом. Срок исчисляется в календарных днях.
Срок исполнения всегда должен быть реальным и учитывать время, необходимое для выполнения технических операций с документами, степень загруженности исполнителя, территориальную отдаленность подразделения и другие факторы. В противном случае указанный срок будет носить формальный характер и будет заведомо невыполнимым.
Технологические процедуры контроля исполнения документов организуются таким образом, чтобы в любой момент руководители фирмы и сотрудники службы КД имели полную и достоверную информацию о ходе исполнения каждого контролируемого конфиденциального документа без обращения к самому документу или исполнителю.
В основе построения технологических процедур контроля исполнения документов лежит применяемая в фирме система учета конфиденциальных документов и ведения справочно-информационного банка данных по документам.
В технологическом процессе контроля выделяются четыре основных последовательно выполняемых этапа: постановка документов на контроль, ведение контроля, снятие документов с контроля, анализ исполнительской дисциплины.

1. Этап постановки документов на контроль

Этап включает в себя следующий типовой комплекс процедур:
• выявление документов, требующих контроля исполнения;
• запись исходных сведений о документе в традиционную или электронную карточку;
• включение карточки в рабочий (предварительный) массив картотеки контролируемых документов;
• контроль срока нахождения документов на рассмотрении руководства учреждения;
• внесение в карточку документа резолюции руководителя или отметки службы КД о направлении документа в структурное подразделение и передача документа;
• перемещение карточки документа из рабочего в основной массив картотеки службы КД.
Начало цикла контрольных операций должно совпадать с моментом учета поступивших и подготовленных документов. Часто контроль исполнения поступивших документов начинается после рассмотрения документа руководителем, что нельзя признать

правильным, так как на стадии рассмотрения могут быть значительные нарушения срока работы с документом.
При традиционной технологической системе учета на контролируемый конфиденциальный документ заполняется дополнительный экземпляр учетной карточки для обеспечения контрольной картотеки. Дополнительный экземпляр карточки может иметь цветовые отличия (цветовые полосы, различную окраску).
В целях контроля исполнения распорядительных документов, планов, решений и других документов, содержащих несколько заданий (поручений), исполняемых несколькими подразделениями и имеющих различные сроки исполнения, заполняется контрольный экземпляр карточки на каждое задание (поручение). Контрольные экземпляры карточки заполняются также при контроле исполнения устного поручения руководителя, при возвращении к документу, который ранее считался исполненным, и в других аналогичных случаях.
Систематизированный массив традиционных контрольных экземпляров учетной карточки на документы образует контрольную картотеку службы КД. Контрольная картотека (раздел) строится по срокам исполнения документов, поэтому ее часто называют сроковой. Независимо от местонахождения и объема карточек картотека формируется по единому принципу. Она состоит из 31 ячейки (по числу дней в месяце), которые образуют ее основной массив, и двух дополнительных отделений: для карточек на просроченные документы и для карточек на документы, исполнение которых намечено на следующий месяц или на более длительный срок. Карточки располагаются в картотеке по ячейкам в соответствии с установленными датами окончания исполнения документов. Внутри ячеек карточки могут размещаться по индексам структурных подразделений или по фамилиям исполнителей. Учитывая, что в карточках фиксируются задания по исполнению документов и ход исполнения, контрольная картотека является строго конфиденциальной.
При автоматизированной технологии контроля исполнения документов ввод исходной информации о контролируемом документе осуществляется или одновременно с автоматизированным учетом документов, или после рассмотрения документа руководителем и принятия им решения о необходимости контроля исполнения документа. В последнем случае ввод информации в систему ведется в режиме корректирования исходных сведений о документе. Входными документами могут быть:
• непосредственно сам контролируемый бумажный или машиночитаемый документ;
• электронный документ, поступивший по линиям связи;
• традиционная регистрационно-контрольная карточка на документ;
• перечень (ведомость) документов, поставленных на контроль;
• карточка внесения изменений, откорректированная традиционная карточка на документ и другие виды документов-корректировок.

2. Этап ведения контроля

Этап ведения контроля заключается в выполнении действий по предупредительному наблюдению за ходом исполнения конфиденциального документа и регулированию процесса исполнения. Включает следующий типовой состав процедур:
• поиск в традиционной или электронной картотеке (разделе) необходимых карточек;
• внесение в карточку отметок о передаче документа из одного структурного подразделения в другое, от одного исполнителя другому;
• устное или письменное напоминание исполнителю о приближении срока окончания работы над документом (например, за 10, 5, и 2 дня);
• внесение записи о состоянии исполнения в соответствующую зону карточки;
• составление сигнальных перечней документов и заданий, находящихся в структурном подразделении и подлежащих исполнению в текущем или последующем периоде (месяце, декаде);
• регулярное беззапросное информирование руководителей о ходе исполнения документов, причинах задержек в исполнении, мерах по обеспечению своевременного исполнения документов;
• внесение в карточку отметок об изменении срока исполнения документа или задания, состава исполнителей, работающих над документом, и т.п., перестановка карточек в традиционной картотеке;
• выдача оперативной поисковой и справочной информации о контролируемых документах по запросам руководителей;

• возвращение карточек в ячейки картотеки (раздела).

Указанные операции выполняются службой КД с использованием традиционной картотеки или базы данных автоматизированной системы. Проверка хода исполнения осуществляется в следующем порядке: задания последующих лет контролируются не реже одного раза в год, задания последующих месяцев текущего года — не реже одного раза в месяц, задания текущего месяца — каждые десять дней, за пять дней и затем ежедневно до истечения срока.

Информация о ходе исполнения документа должна поступать тому руководителю, который рассматривал документ и принимал по нему решение. В результате рассмотрения этой информации руководитель должен убедиться, что исполнение идет в соответствии с намеченным планом или предпринять действия по корректированию хода исполнения документа: уточнить задание, изменить состав исполнителей и соисполнителей.

3. Этап снятия документов с контроля

Этап снятия документов с контроля включает следующий типовой состав процедур:

• принятие руководителем решения о снятии документа с контроля и отдача соответствующего распоряжения службе КД;

• внесение отметки об исполнении документа в экземпляры учетной карточки;

• перестановка карточки из контрольной картотеки (раздела) в справочную картотеку (раздел) вместо хранившегося там экземпляра карточки;

• подшивка контролируемого документа, имеющего отметку

об исполнении, и всех относящихся к нему материалов в дело. Документ считается исполненным и снимается с контроля после реального и окончательного выполнения всех заданий, поручений и решений, содержащихся в документе и резолюции руководителя, сообщения результатов заинтересованным учреждениям, организациям, фирмам и лицам или наличия другого документированного подтверждения факта исполнения (например, внесения дополнений в другие документы).

4. Этап анализа исполнительской дисциплины

Этап анализа исполнительской дисциплины включает следующий типовой состав процедур:

• сбор необходимой информации по традиционной или электронной картотеке (разделу);

• рукописное или автоматическое составление итоговых перечней документов, количественных сводок и справок по результатам контрольной работы за определенный промежуток времени;

• распечатка (печатание) итоговых документов контроля;

• передача итоговых документов по результатам контрольной работы и материалов анализа исполнительской дисциплины на рассмотрение руководству фирмы и структурных подразделений;

• выработка и осуществление мер, стимулирующих высокий уровень исполнительской дисциплины в фирме.

Перечни заданий, поручений и документов, сводки и справки по видам документов всегда составляются в разрезе структурных подразделений и исполнителей. Например, справка о состоянии исполнения документов на определенное число в конкретном структурном подразделении может иметь следующие графы: наименование документа; его краткое содержание; дата, номер; срок исполнения; фамилия исполнителя; состояние исполнения; причины невыполнения. Целесообразно добавить графы: предполагаемый срок исполнения и роспись исполнителя. Графы, содержащие сведения о причинах невыполнения здания и предполагаемом сроке исполнения, должны заполнять лично исполнители.

При использовании автоматизированной системы контроля в установленные графиком сроки (в беззапросном режиме) или по запросам пользователей может выдавать следующие итоговые документы по результатам контроля, например:

• список всех заданий, подлежащих предупредительному контролю;

• список зданий, подлежащих промежуточному контролю;

• список заданий, не исполненных в срок (в разрезе руководителей);

• список заданий, не исполненных в срок (в разрезе структурных подразделений и исполнителей);

• список исполненных заданий;

• состояние исполнения всех неисполненных заданий.

Одновременно может осуществляться сопоставительный анализ исполнительской дисциплины по годам и месяцам.

Итоговые документы контроля должны поступать руководителям вместе с аналитическими докладами, докладными записками, письменными заключениями и рекомендациями о состоянии и мерах улучшения исполнительской дисциплины, ускорению исполнения документов, заданий и поручений.

При этом следует учитывать, что задержки в исполнении документов и поручений могут быть связаны с объективными причинами общей неупорядоченности управленческих и документационных процессов в фирме. Помимо этого руководитель, принимавший решение по документу, должен иметь в виду, что задержки в исполнении могли быть и по его вине, например: решение было нечетко сформулировано и не понято исполнителем, не было необходимых объективных условий для его выполнения, неправильно был определен срок исполнения.

При невыполнении задания в установленный срок руководитель должен изучить причины этого факта и только после этого выработать меры, направленные на исключение в будущем подобных явлений, или определить степень вины нижестоящих руководителей и исполнителей. Ошибки, допущенные самим руководителем в порядке принятия и оформления решения, должны быть. им своевременно исправлены. Повторное распоряжение в этом случае обычно не издается, обеспечивается выполнение откорректированного ранее изданного задания,

Следовательно, своевременный и фактический контроль исполнения документов и поручений в аппарате управления является основой эффективной реализации контрольной функции, составляющей в совокупности с другими функциями фундамент любой управленческой системы. Правильная организация и технология контроля исполнения документов предопределяет успешную работу фирмы, качественное решение ею производственных задач.

7.4. Порядок работы персонала с конфиденциальными документами и материалами

Уязвимость документа резко возрастает при выходе его за пределы службы КД. В этой связи правильная организация работы персонала фирмы с конфиденциальными документами и контроль за выполнением сотрудниками установленных правил представляются крайне важными.

Работникам службы КД и персоналу фирмы следует учитывать, что работающий в фирме злоумышленник или сотрудник фирмы, связанный со злоумышленником, похищают, уничтожают или фальсифицируют, как правило, не те документы, с которыми они работают, а документы и информацию, доверенные другим сотрудникам. Особую ценность в этом плане для злоумышленника представляют работники службы КД или референты руководителей как лица наиболее осведомленные в тайне фирмы.

Ответственность за сохранность конфиденциальных документов и предотвращение утраты ими конфиденциальности несут руководители подразделений (направлений деятельности) фирмы. Сотрудники фирмы, в том числе руководители любого уровня, при работе с конфиденциальными документами обязаны:

• знакомиться только с теми конфиденциальными документами, к которым они получили письменное разрешение на доступ в силу должностных обязанностей;

• немедленно предъявлять работнику службы КД все числящиеся за ним документы (на бумажных и магнитных носителях, электронные, фото-, видео-, аудиодокументы) для проверки их наличия и комплектности;

• вести совместно с работником службы учет находящихся у него конфиденциальных документов;

• ежедневно по окончании рабочего дня проверять наличие документов и сдавать их на хранение в службу КД;

• сдавать по описи работнику службы КД все материалы по окончании исполнения документа или работы над ним;

• сдавать но описи работнику службы КД все числящиеся за ним документы и материалы при увольнении, уходе в отпуск, отъезде в командировку;

• немедленно сообщать первому руководителю фирмы и в службу КД об утрате или недостаче документов, обнаружении лишних или неучтенных документов, отдельных листов. Работа с конфиденциальными документами на рабочих местах разрешается сотрудникам фирмы только при наличии условий, исключающих возможность утраты документа или хищения информации. При отсутствии этих условий сотрудники фирмы работают с конфиденциальными традиционными и электронными документами, делами и базами данных в специально предназначенном для этого помещении службы КД.

Для работы с конфиденциальными документами сотрудник должен быть обеспечен: постоянным рабочим местом, личным сейфом (металлическим шкафом), кейсом для хранения и переноса конфиденциальных документов, номерной личной металлической печатью. Рабочее место исполнителя должно быть размещено таким образом, чтобы была исключена возможность обозрения находящихся на столе документов лицами, не имеющими к ним отношения. Экран компьютера не должен быть виден коллегам по рабочему помещению, посетителям, в окно и от входной двери. Помещение, в котором конфиденциальная информация обрабатывается на ЭВМ, должно иметь защиту от технических средств промышленного шпионажа. На рабочем столе всегда должен находиться только тот конфиденциальный документ и материалы к нему, с которыми в данный момент работает сотрудник. Другие документы должны быть заперты в сейфе.

Сотрудникам не разрешается хранить конфиденциальные документы, дела, дискеты на рабочем столе, в ящиках рабочего стола, неприспособленных шкафах. Ключи от сейфа и кейса, металлическая печать постоянно хранятся у сотрудника. Дубликаты всех ключей должны находиться в службе КД в опечатанном исполнителем пенале (в том числе дубликаты ключей от сейфа и кейса, которыми пользуется первый руководитель). Прочитанные листы конфиденциального документа всегда должны лежать текстом вниз.

Если к рабочему столу подходит кто-либо из сотрудников, исполнителю следует перевернуть лист, с которым он работает, текстом вниз. При выходе из помещения на любое время исполнитель должен убрать в сейф все документы и материалы, запереть сейф, заблокировать компьютер и, если в помещении не остаются другие сотрудники, запереть входную дверь.

Руководителям и исполнителям, работникам службы КД не следует вести какие-либо вспомогательные картотеки по организации работы с конфиденциальными документами и контроля за их исполнением. Исполненные (до подшивки в дело) и неисполненные документы должны храниться только в рабочих папках, на которых указывается их целевое назначение: «Ознакомление», «Согласование», «Срочно», «Задания на такое-то число», «Подлежит возврату», «На подшивку в дело» и т.п. Папки должны иметь описи находящихся в них документов. Хранить документы в россыпи в ящиках столов, шкафах, сейфах в одной папке не допускается. Дела, закрепленные за конкретным исполнителем, имеют индивидуальное цветовое отличие, позволяющее выявлять факты несанкционированного обращения к этим делам другого сотрудника.

Всем сотрудникам фирмы, работающим с конфиденциальными документами, делами, информацией, запрещается:

• использовать конфиденциальные сведения в публикациях, открытых документах, докладах и интервью, рекламных материалах, выставочных проспектах и любых других информационных сообщениях массового распространения;

• сообщать кому-либо (в том числе коллегам по работе или родственникам) устно или письменно конфиденциальную информацию, несанкционированно передавать документы, даже если это связано со служебной деятельностью;

• вести переговоры, содержащие конфиденциальные сведения, по незащищенным линиям связи, в неприспособленных помещениях, в присутствии посторонних лиц;

• обсуждать конфиденциальные вопросы в местах общего пользования (в том числе в любых видах транспорта — служебном, личном, общественном);

• знакомиться с документами, делами и базами данных других сотрудников, работать с их компьютерами без письменного разрешения первого руководителя;

• переписывать сведения из документов в личные дневники, карточки учета работы, календари, еженедельники и т.п., переносить их в справочные и личные учетно-плановые массивы ЭВМ;

• вносить и пользоваться в помещениях фирмы личными фото- и видеоаппаратами, компьютерами, аудиотехникой, магнитофонами, плейерами, переговорными устройствами, техническими носителями информации (дискетами и др.), радиотелефонами, копировальными аппаратами;

• выносить из здания фирмы любые (в том числе открытые) служебные документы без письменного разрешения первого руководителя;

• оставлять документы на рабочем столе или работающий компьютер при выходе из помещения на любое время;

• хранить конфиденциальные документы вместе с открытыми документами и материалами, формировать в одном деле или машинном массиве конфиденциальные и открытые сведения;

• разглашать сведения о характере автоматизированной обработки конфиденциальной информации и о личных идентифицирующих кодах и паролях;
• разглашать сведения о составе находящихся у сотрудника документов и материалов, системе их защиты и месте хранения, а также известных ему элементах обеспечения безопасности фирмы и персонала.
Работникам службы КД рекомендуется регулярно проверять программное обеспечение компьютеров, на которых обрабатывается конфиденциальная информация. Цель проверки — обнаружение неутвержденных или необычных программ. Резервные и страховые копии всех документов фирмы, находящихся на магнитных носителях, должны храниться в службе КД. Актуализация копий осуществляется по мере необходимости работником службы КД с письменной санкции руководителя подразделения (направления деятельности) фирмы и в присутствии соответствующего исполнителя. Санкция и факт актуализации фиксируются в учетной карточке документа.
В конце рабочего дня исполнители обязаны перенести всю конфиденциальную информацию из компьютера на гибкие носители информации, стереть информацию с жестких дисков, проверить наличие всех конфиденциальных документов (на бумажных, магнитных и иных носителях), убедиться в их комплектности и сдать в службу КД. Оставлять конфиденциальные документы на рабочем месте не разрешается. Не допускается также хранение на рабочем месте исполнителя копий конфиденциальных документов.
Исключительным правом постоянного хранения документов на рабочих местах могут пользоваться: первый руководитель, его заместитель, сотрудники службы персонала и других служб по усмотрению первого руководителя, которые располагают объемными массивами конфиденциальных бумажных документов (картотеками, папками и др.) или большим числом машиночитаемых документов.
Конфиденциальные материалы такого рода помещаются в сейф (металлический шкаф), который запирается, опечатывается и сдается под охрану. Сейф оборудуется охранной сигнализацией. Компьютеры с обширным составом конфиденциальной информации, которую невозможно переносить на гибкие диски, или сложными базами данных опечатываются двумя печатями — исполнителя и представителя службы безопасности. Снятие печатей в начале рабочего дня также производится этими лицами.
В службу КД сдается, как правило, каждый конфиденциальный документ в отдельности. При наличии у сотрудника нескольких документов, дел, дискет, других носителей, необходимых ему для ежедневной длительной работы, их аккуратно (в папках, конвертах) укладывают вместе с описью в кейс, который запирается, опечатывается личной печатью сотрудника и сдается в службу КД. Кейсы предназначены для переноса конфиденциальных документов в пределах охраняемой зоны (внутри здания фирмы), доставки их в службу КД и обратно на рабочее место, хранения документов в нерабочее время в этой службе. Кейсы выдаются исполнителям в начале рабочего дня в обмен на удостоверение, пропуск, специальный жетон или под роспись в специальной учетной форме.
После подготовки конфиденциальных документов к сдаче в службу КД исполнитель обязан отключить ЭВМ, блокировать ее персональным ключом, проверить наличие и комплектность открытых документов, дискет, дел, других материалов, хранящихся в металлическом шкафу, и запереть шкаф. В помещении отключается электроэнергия, входная дверь запирается, опечатывается, и помещение сдается под охрану. Подобные помещения охраняются особенно тщательно, оборудуются комплексом технических средств сигнализации и оповещения. Сейфы с особо ценными документами целесообразно размещать в помещении службы КД.
Отметки о закрытии и вскрытии рабочих комнат сотрудниками фирмы, отключении технических средств сигнализации и оповещения делаются в специальном журнале службы охраны с росписью лица, ответственного за помещение, и представителя охраны. Основные и резервные ключи от рабочих комнат хранятся в сейфе в помещении охраны в специальных пеналах. Пенал закрывается и опечатывается лицом, ответственным за помещение. Уборка рабочих помещений разрешается только в присутствии указанного лица и под его наблюдением.
Следует всегда помнить, что любые ошибочные действия персонала даже при технически оснащенной системе защиты часто ведут к утрате ценной информации и слишком дорого обходятся фирме.
Следовательно, правильная организация работы персонала фирмы с конфиденциальными

документами является обязательным условием эффективного функционирования системы защиты документированной информации. Каждый сотрудник должен педантично соблюдать установленные правила, с пониманием относиться к определенным ограничениям в работе с конфиденциальными документами и не допускать провоцированных или непровоцированных кем-либо ошибочных действий.

7.5. Обработка изданных документов

Стадия обработки изданных конфиденциальных документов осуществляется централизованно службой КД в традиционном или автоматизированном режиме и предназначена для выполнения технологических комплексов, процедур и операций по отправке документов адресатам или использованию внутренних документов в целях управления фирмой и обеспечения ее основной деятельности.

Как мы уже отмечали, подготовленный конфиденциальный документ получает учетный номер на этапе изготовления проекта документа с черновика. После завершения этапа издания исполнитель отчитывается (если он не сделал этого раньше) за израсходованные носители и передает в службу КД в соответствии с внутренней описью документов, находящихся у него: подлинник и все экземпляры подписанного документа, черновик и варианты документа, испорченные листы, дискеты и бланки, чистые учтенные носители, инициативный документ, послуживший основанием для издания нового документа (с отметкой об исполнении) и другие материалы, возникшие при создании документа. Черновики, варианты и рабочие материалы (в том числе на дискетах) уничтожаются в присутствии исполнителя.

В службу КД для уничтожения сдаются не подписанные или не утвержденные проекты подготовленных документов со всеми материалами. Исполнителям запрещается самостоятельно уничтожать какие-либо конфиденциальные материалы, черновики документов. Им не разрешается также оставлять у себя материалы, подлежащие уничтожению, или их копии.

Неправильно оформленный или некомплектный документ возвращается исполнителю. Не принимается также документ, если исполнитель не смог отчитаться о местонахождении черновика, вариантов и других материалов. Об отказе в приеме документа информируется первый руководитель фирмы для принятия решения.

Стадию обработки изданных документов можно разделить на два технологических комплекса: а) комплекс процедур передачи в службу КД и обработки документов, предназначенных для отправки, и б) комплекс процедур передачи в эту службу и обработки внутренних документов.

Первый комплекс включает в себя следующие процедуры:

• получение документа от исполнителя;

• получение документа с другого участка службы КД (инвентарного, архивного и др.);

• подготовка документа к отправлению;

• отправление пакетов (конвертов). В процессе обработки отправляемых конфиденциальных документов решаются следующие задачи обеспечения защиты информации и ее носителя:

• исключение возможного тайного вскрытия конверта и несанкционированного ознакомления с документом при его пересылке (передаче) адресату, возможности подмены документа и листов;

• ограничение возможности утери, кражи или подмены конверта с конфиденциальным документом;

• подтверждение факта отправки документа и правильности оформления этого факта в учетных формах;

• исключение ошибочной отправки документа, конверта другому адресату, необоснованной рассылки документов ряду адресатов.

Разрешением на отправку конфиденциального документа является подписанное первым руководителем фирмы сопроводительное письмо к документу или разрешительная запись, сделанная лично руководителем в учетной форме, если документ отправляется без сопроводительного письма. Отправка конфиденциальных документов осуществляется централизованно службой КД фирмы. В некрупных фирмах — секретарем-референтом или управляющим делами. Исполнителям запрещается лично отправлять конфиденциальные документы.

При подготовке документа к отправлению на лицевой стороне конверта обозначаются: гриф конфиденциальности и другие необходимые адресные реквизиты, номера вложенных

документов. На оборотной стороне в местах склеивания клапанов конверта ставится печать фирмы. Конверты с конфиденциальными документами должны передаваться курьерами адресатам под роспись за получение конверта в разносной книге, реестре или расписке. Курьерам не разрешается пользоваться общественным транспортом.
При отправлении конфиденциальных документов заказными и ценными почтовыми отправлениями используется двойное пакетирование документов (вкладывание конверта в конверт). Гриф конфиденциальности и иные отметки ставятся на внутреннем конверте, который опечатывается и при необходимости прошивается. Внешний конверт оформляется в соответствии с Почтовыми правилами. Конверты (пакеты), предназначенные для отправления конфиденциальных документов, должны быть светонепроницаемыми. Особое внимание обращается на прочность проклеивания клапанов конвертов, исключающее возможность «отпаривания» мест склейки. Тексты отправляемых писем, телеграмм, телексов, факсов целесообразно шифровать. Факт оправления конфиденциальных, документов подтверждается почтовыми реестрами.
Второй комплекс — передача работником службы КД изданных внутренних документов на исполнение, для использования или ознакомления по своему содержанию соответствует составу стадий входного документопотока и включает в себя:
• передачу документа соответствующему руководителю для рассмотрения и исполнителю (исполнителям) для работы;
• ознакомление с документом соответствующих сотрудников фирмы;
• исполнение, использование и возвращение документа от исполнителя;
• передачу документа на другие участки службы КД. Технология выполнения перечисленных стадий аналогична рассмотренной выше.
Следовательно, обработка изданных конфиденциальных документов отличается четкой детализацией технологии выполнения, при которой основную роль играет соблюдение правильной последовательности выполнения технических процедур и операций, а также своевременное внесение необходимых сведений в соответствующие учетные формы.

8. ПРОВЕРКА НАЛИЧИЯ И УНИЧТОЖЕНИЕ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ, ДЕЛ И НОСИТЕЛЕЙ ИНФОРМАЦИИ

8.1. Назначение и порядок проведения проверки наличия документов, дел и носителей информации

Целью проверки наличия документов, дел и носителей конфиденциальной информации является установление их реального соответствия записям в учетных формах, сохранности, целостности и комплектности, а также своевременное выявление фактов утраты конфиденциальных материалов и определение правильности выполнения процедур и операций по их учету, хранению и использованию. Проверки стимулируют тщательное соблюдение всеми сотрудниками фирмы требований по работе с конфиденциальными материалами, обеспечение их физической сохранности и в конечном счете — информационной безопасности фирмы.
Проверка всегда ведется от учетных данных к документам, экземплярам документа и составным частям каждого документа или дела. Кроме того, в ходе проверки рассматриваются вопросы снятия с документов грифа конфиденциальности.
Проверки наличия конфиденциальных материалов могут быть регламентированными (периодическими) и нерегламентированными (непериодическими).
Регламентированные, обязательные проверки наличия документов, дел и носителей информации проводятся ежедневно, ежеквартально и по окончании календарного года. Они охватывают весь массив конфиденциальных материалов фирмы. Нерегламентированные проверки осуществляются при смене руководителей подразделений или направлений деятельности фирмы, увольнении сотрудников, после завершения экстремальной ситуации, при выявлении факта возможной утраты информации и в других случаях. Этот вид проверки обычно ограничивается конкретной частью конфиденциальных материалов.
Ежедневные проверки наличия (самопроверки или проверки вторым работником) проводятся в конце рабочего дня всеми сотрудниками фирмы, работающими с конфиденциальными материалами. Квартальные и годовые проверки наличия осуществляются специально назначаемой комиссией. По результатам квартальной и годовой проверок составляется акт.
Любой вид проверки может быть закончен лишь после выявления фактического наличия всех документов, числящихся по учетным формам. Для проверки используются только

основные учетные формы — журналы регистрации и учетные карточки. Другие учетные формы (описи, перечни, реестры, акты, карточки учета разрешений и выдачи материалов и т.д.) носят вспомогательный информационный и оправдательный характер.
Технологическая схема проверки наличия документов, дел и носителей информации включает в себя следующие процедуры:
• подготовка квартальной или годовой проверки;
• проверка в службе конфиденциальной документации;
• проверка на рабочих местах исполнителей;
• оформление и анализ результатов проверки.
В процессе проведения квартальной проверки наличия конфиденциальных материалов контролируется сохранность традиционных и электронных документов, находящихся на исполнении у сотрудников фирмы и не подшитых в дела. Одновременно проверяется соблюдение сотрудниками установленного порядка работы с конфиденциальными материалами, их хранения, правильности ведения внутренней описи документов, находящихся у исполнителя, своевременности и полноты ежедневной сдачи всех материалов в службу КД. Проверка ведется только в присутствии самого сотрудника.
В процессе проведения годовой проверки наличия конфиденциальных материалов контролируется сохранность всех традиционных и электронных документов, как находящихся на исполнении, так и исполненных, подшитых в дела независимо от времени их поступления, получения или издания. Дела проверяются полистно.
Отсутствие конфиденциального документа, дела или носителя информации у сотрудника, которому они были выданы, считается утратой этих материалов. В подобном случае комиссия составляет соответствующий акт и немедленно докладывает об утрате первому руководителю фирмы для принятия решения. Акт составляется также в случае обнаружения в базе данных компьютера сотрудника или на дискете неучтенной или несанкционированно сохраненной копии электронного документа.
Следовательно, проверка наличия документов, дел и носителей информации реализует одну из главных частей функции контроля за работой сотрудников фирмы с конфиденциальными материалами и дает возможность достоверно определить степень ответственного отношения каждого сотрудника к этой работе. Одновременно выявляются факты утраты конфиденциальных материалов, что является основанием для начала служебного расследования.

8.2. Порядок уничтожения документов, дел и носителей информации

В технологическом процессе уничтожения конфиденциальных документов, надобность в которых отпала или срок хранения которых истек, имеются некоторые особенности по сравнению с аналогичной стадией, выполняемой с открытыми документами и делами. При уничтожении конфиденциальных материалов руководством фирмы должен быть установлен порядок, исключающий возможность ознакомления с ними посторонних лиц, исключающий неполное уничтожение документов, позволяющее восстановить их текст, а также исключающий возможность уничтожения материалов, не подлежащих включению в эту категорию. В ходе уничтожения подобные материалы подвергаются опасности в случаях:
• подмены документов, выделенных для уничтожения или изъятия из документов и дел отдельных частей (листов, фотографий, образцов печатей, росписей и т.п.);
• ошибочного или умышленного выделения для уничтожения или фиктивного «уничтожения» ценных документов и дел;
• неполного уничтожения документов, дел и носителей, дающего возможность восстановить их текст;
• утраты (утери, кражи) документов и дел, выделенных для уничтожения.
Перечисленные факторы возникновения угроз могут стать контролируемыми при соблюдении:
• коллегиальности принятия решения об уничтожении документов, дел и самого процесса уничтожения;
• документирования (актирования) подготовки к уничтожению и уничтожения документов и дел;
• а также при внесении комиссией отметок об уничтожении в акт и учетные формы только после фактического уничтожения документов и дел.
Уничтожение конфиденциальных документов и дел организуется службой КД. Состав подлежащих уничтожению документов письменно согласовывается с руководителями подразделений или направлений деятельности и санкционируется экспертной комиссией

фирмы. Процесс уничтожения документов, дел, а также других конфиденциальных материалов производится с оформлением акта и без оформления акта.
Технологическая схема уничтожения конфиденциальных документов, дел и носителей информации включает в себя следующие процедуры:
• подготовка документов, дел IT носителей информации к уничтожению;
• оформление акта на уничтожение;
• уничтожение документов по акту;
• уничтожение документов и носителей информации без составления акта.
Процедура подготовки документов, дел и носителей информации к уничтожению включает:
• выделение документов, дел и носителей информации, подлежащих уничтожению по различным причинам;
• получение письменного разрешения на уничтожение **от** руководителей структурных подразделений (направлений деятельности) фирмы;
• систематизацию документов, дел и носителей информации по способам документирования факта уничтожения.
С оформлением акта уничтожаются: документы и дела, включенные в номенклатуру дел, подлинники видео- и аудиодокументов, проекты технических документов, черновики и проекты особо ценных документов, картотеки (журналы) учета конфиденциальных документов и другие подобные материалы. Акт подписывают члены экспертной комиссии и утверждает первый руководитель фирмы. С оформлением акта уничтожаются любые электронные документы, описи и учетные формы, находящиеся как в рабочем или архивном массивах компьютера, так и на магнитных носителях, хранимых вне ЭВМ.
При выполнении процедуры оформления акта на уничтожение документов осуществляются:
• включение отдельной позицией в акт каждого отобранного к уничтожению традиционного документа или дела (тома), документа или дела на магнитном или ином техническом носителе;
• оформление в акте итоговой записи, подписание итоговой записи сотрудниками, составившими акт;
• проверка наличия и комплектности документов и дел, включенных в акт;
• согласование акта с должностными лицами, подписание его членами экспертной комиссии и утверждение первым руководителем фирмы. В процедуру уничтожения документов по акту входят:
• проверка специально назначаемой комиссией наличия документов, дел (томов), магнитных и других носителей, включенных в акт, их комплектности и соответствия записям в акте;
• физическое уничтожение этой комиссией документов, дел, томов и носителей информации;
• внесение в акт и учетные формы документов и носителей информации записи об уничтожении, роспись членов комиссии.
Фактическое уничтожение документов и дел с истекшим сроком хранения производится только после утверждения описей дел постоянного и длительного срока хранения за соответствующий период. Подписание акта и внесение отметок об уничтожении в учетные формы до фактического уничтожения конфиденциальных материалов не допускается.
Бумажные документы уничтожаются путем сожжения, дробления, превращения их в бесформенную массу. Магнитные и фотографические носители уничтожаются сожжением, дроблением, расплавлением и другими способами, исключающими возможность восстановления их.
Без оформления акта уничтожаются: испорченные бумажные и технические носители, черновики и проекты документов, внутренние описи документов, находящихся у исполнителя, и другие материалы, образовавшиеся при исполнении конфиденциальных документов.
В процедуру уничтожения документов и носителей информации **без** оформления акта входят:
• разрывание листов, разрушение магнитного или иного технического носителя в присутствии исполнителя или второго сотрудника службы КД;
• накапливание остатков носителей в опечатываемом ящике (урне);
• физическое уничтожение остатков носителей несколькими сотрудниками службы КД;
• внесение отметок об уничтожении в учетные формы документов и носителей.
Следовательно, при выполнении процедур и операций уничтожения конфиденциальных

документов, дел и носителей информации особое внимание обращается на коллегиальность осуществления этих действий и жесткое соблюдение последовательности процедур и технологии уничтожения.

9. ФОРМИРОВАНИЕ И ХРАНЕНИЕ КОНФИДЕНЦИАЛЬНЫХ ДЕЛ

9.1. Особенности составления и ведения номенклатуры дел

Систематизация конфиденциальных документов в дела и ведение дел в целом соответствуют тем требованиям, которые предъявляются к аналогичной работе с документами открытого доступа.

Вместе с тем задачи, решаемые при выполнении процедур и операций формирования и ведения дел с конфиденциальными документами (конфиденциальных дел), охватывают не только сферу эффективного использования этих документов в управленческой и производственной деятельности фирмы, но и в значительной степени сферу обеспечения сохранности документов, дел, массивов информации и их носителей, а также других конфиденциальных материалов в процессе хранения и использования.

Угроз ценным и конфиденциальным материалам фирмы в период их текущего (оперативного) архивного хранения нисколько не меньше, чем во время рассмотрения, исполнения, обработки и движения. В практической деятельности фирм этот момент часто не учитывается, исполненные конфиденциальные документы выпадают из-под контроля службы КД, что создает благоприятные возможности для злоумышленника осуществить несанкционированное ознакомление с этими документами или выполнить с ними иные противоправные действия.

Помимо известных задач номенклатура конфиденциальных дел предназначена для:

• учета формируемых дел (номенклатурного учета дел) и обеспечения проверки наличия документов и дел;

• закрепления схемы разрешительной системы доступа руководителей и сотрудников фирмы к делам;

• учета дел архивного фонда;

• учета движения, использования и уничтожения архивных документов, дел и других конфиденциальных материалов до передачи в ведомственный архив или архив фирмы.

Табличная часть номенклатуры имеет следующие дополнительные графы, предназначенные для практической реализации указанных выше задач: гриф конфиденциальности дела, фамилии сотрудников, которым предоставлено право пользоваться делом, отметка о движении дела (архивный номер, номер и дата акта об уничтожении, запись об отправлении, номер и дата сопроводительного письма), отметка о проверке наличия (подписи и дата). Комплексы документов на магнитных носителях (дискетах и др.), а также архивные массивы (подмассивы) электронных документов, находящихся в компьютере, вносятся в номенклатуру дел на общих основаниях. Закрепление дел за конкретными исполнителями делает номенклатуру правовой основой для разрешения исполнителям работать с конкретными делами.

В номенклатуру не включаются конфиденциальные дела и документы, которые имеют инвентарную форму учета, например:

техническая и технологическая документация, печатные издания, аудио- и видеодокументы, особо ценные документы выделенного хранения и т.п.

Перечень заголовков дел оформляется таким образом, чтобы состав, содержание и уровень конфиденциальности документов каждого дела соответствовали функциональным обязанностям тех сотрудников фирмы, которые допущены к делу и будут с ним работать.

Конфиденциальные документы не должны попадать в государственный архив до истечения срока конфиденциальности их содержания, поэтому при их комплектовании в дела каждое дело должно содержать документы, имеющие приблизительно одинаковый период конфиденциальности. Под одним заголовком обычно заводится конфиденциальное и неконфиденциальное (открытое) дело или устанавливается предметная связь конфиденциальных и открытых дел. В этом случае конфиденциальные дела включают в себя только те документы, которые в данный момент должны иметь ограничения по доступу к ним персонала. В результате защита документов, дел и носителей информации становится более эффективной. Не следует отождествлять два разных понятия — срок хранения дела и период конфиденциальности документов, включаемых в дело, хотя конфиденциальные документы характеризуются и тем и другим понятиями. Период конфиденциальности может быть длиннее или короче срока хранения дела.

Номенклатура конфиденциальных дел, составляемая как самостоятельный документ или в виде приложения к общей номенклатуре дел фирмы, должна иметь гриф ограничения доступа, соответствующий уровню конфиденциальности содержащихся в ней дел и документов. Она учитывается как любой внутренний конфиденциальный документ по картотеке подготовленных документов.
Любые изменения, дополнения и отметки при выполнении процедуры ведения номенклатуры вносятся в нее с разрешения руководителя службы КД.
В отличие от номенклатуры дел открытых документов при работе с номенклатурой конфиденциальных дел выделяется в качестве самостоятельной процедура закрытия номенклатуры дел, которая включает в себя следующие операции:
• проверка закрытия всех заведенных дел и томов;
• проведение ежегодной проверки наличия дел и документов;
• заполнение итоговой записи о категориях и количестве заведенных дел;
• проверка полного соответствия электронного и бумажного экземпляров номенклатуры дел, допечатка отметок о закрытии номенклатуры, заверение всех отметок росписью работника участка службы КД;
• включение бумажного экземпляра номенклатуры в дело номенклатур;
• переработка электронного экземпляра номенклатуры дел для использования в следующем календарном году;
• распечатка номенклатуры дел следующего года для издания.
После окончания делопроизводственного года и проведения годовой проверки наличия дел и документов номенклатура закрывается и подшивается в дело, содержащее номенклатуры за прошлые годы. При этом номенклатура сохраняет учетную функцию архивных дел соответствующего года.
Для удобства проверки сохранности конфиденциальных дел, особенно при значительном количестве дел долговременного периода конфиденциальности, можно ввести инвентарную форму учета дел. Каждое законченное и закрытое конфиденциальное дело (том), картотека, журнал вносятся в традиционную и (или) электронную инвентарную учетную опись законченных производством дел, картотек и журналов. Учетные инвентарные номера дел вносятся в номенклатуру и указываются на обложках дел.
Следовательно, процесс составления, ведения и закрытия номенклатуры конфиденциальных дел имеет существенные отличия от аналогичного процесса систематизации открытых дел. Эти особенности касаются прежде всего установления ограничений на доступ сотрудников к делам и обеспечения проверки наличия дел как в текущем делопроизводстве, так и в архиве фирмы.

9.2. Формирование и оформление дел

Дела с конфиденциальными документами всегда формируются централизованно в службе КД. Формирование и хранение таких дел на рабочих местах сотрудников фирмы не разрешается.
В процессе формирования и хранения возникают серьезные угрозы конфиденциальным делам и документам, которые могут получить реальный характер в результате:
• получения сотрудником, работающим с делом, большего объема конфиденциальной информации, чем это необходимо (из-за неправильного формулирования заголовков дел в номенклатуре или ошибочного распределения, систематизации документов по делам);
• утери работником службы КД контроля использования дел сотрудниками фирмы (из-за плохо организованного ежедневного учета выдачи и возвращения дел);
• утраты (кражи, утери) дела или содержащегося в нем документа, частей документа, подмены документов, отдельных листов;
• ошибочной выдачи дела сотруднику, не имеющему права доступа к данному делу;
• доступа к делам посторонних лиц как следствие ошибочных действий персонала или невыполнения персоналом порядка обеспечения сохранности дел (например, невыполнения требований инструкции об эвакуации дел и документов в условиях экстремальной ситуации).
При формировании конфиденциальных документов в дела должна жестко соблюдаться разрешительная система доступа сотрудников к делам, документам и электронным сведениям, обеспечиваться информационная взаимосвязь местонахождения документа в деле с его предыдущими учетными формами и номерами, строго выполняться инструктивные требования, решающие задачу сохранности дел и документов.
Технологическая схема процесса формирования и оформления конфиденциальных дел

включает следующие процедуры: оформление дела при его заведении; оформление дела при его формировании;
оформление дела (тома) при его закрытии; выдача законченных дел сотрудникам фирмы и приема их от сотрудников.
Особенностями процедуры оформления дела при его заведении являются:
• оформление обложки дела с указанием грифа конфиденциальности дела;
• оформление списка сотрудников, допущенных к делу (на внутренней стороне обложки дела);
• оформление карточки учета разрешений и выдачи дела (помещается в конверте на внутренней стороне обложки);
• подшивка в дело чистых листов (бланков) внутренней описи документов;
• внесение в номенклатуру отметки о заведении дела.
Датой заведения дела является дата поступления первого документа на подшивку в дело. Обложка конфиденциального дела оформляется в соответствии с общими правилами. Гриф конфиденциальности указывается в верхнем правом углу обложки дела. В целях затруднения поиска дел посторонним лицом заголовок дела на обложке может не указываться, ставится только индекс дела по номенклатуре.
Внутренняя опись обязательна для всех дел, содержащих конфиденциальные документы, выполняет функцию учета документов, включенных в дело, и содержит графы: учетный номер документа, гриф конфиденциальности, дата подписания или утверждения, вид, краткое содержание, номера листов дела, соответствующих расположению документа в деле. Опись подшивается в начале дела, перед документами и имеет самостоятельную нумерацию листов. По описи проверяется сохранность документов и их комплектность.
Магнитные носители (дискеты и др.) с документами хранятся в специальных футлярах, оформление лицевой стороны которых аналогично оформлению традиционного дела. В футляр вкладываются: список исполнителей, допущенных к носителю, карточка разрешений и выдачи носителя, бумажный экземпляр электронной описи документов, записанных на носителе.
Особенностями процедуры оформления дела при его формировании являются:
• проставление в каждом документе под грифом ограничения доступа отметки о периоде его конфиденциальности или даты рассмотрения вопроса о снятии грифа (если такая отметка или дата ранее отсутствовали);
• внесение данных о подшиваемых документах во внутреннюю опись дела;
• нумерация листов документа в деле;
• при необходимости внесение изменений в реквизиты обложки дела;
• подшивка документа в дело (прошнуровывание листов документа), проверка правильности нумерации листов;
• внесение отметки о подшивке в учетную карточку документа;
• проверка правильности подшивки документа;
• возвращение учетной карточки документа на соответствующий участок службы КД, в картотеку по принадлежности. В дело включаются только исполненные конфиденциальные документы одного календарного года в комплекте с приложениями и всеми материалами, инициировавшими и сопровождавшими процесс исполнения документа. Копии формируются в отдельное дело. Сведения о документе вносятся в опись перед его подшивкой в дело.
Запрещается подшивать в одно дело конфиденциальные и открытые документы. Каждый том дела имеет самостоятельную нумерацию листов. Листы нумеруются простым карандашом в правом верхнем углу листа, не затрагивая текст документа. Не допускается открывать очередной том дела до закрытия предыдущего. Ошибки в нумерации листов оговариваются в описи и заверительной надписи. Исправления, вносимые в опись дела, заверяются исполнителем и сотрудником службы КД.
Особенностями процедуры оформления дела (тома) при его закрытии являются:
• подшивка и оформление заверительного листа — листа-заверителя (только для дел, содержащих документы долговременного периода конфиденциальности);
• оформление итоговой записи во внутренней описи дела;
• опечатывание концов шнурка на заверительном листе (только для дел, содержащих документы долговременного периода конфиденциальности);
• внесение итоговых сведений в реквизиты на обложке дела;
• проставление отметки о закрытии дела (тома) в номенклатуре дел;
• при необходимости — внесение дела в инвентарную опись законченных производством

дел, картотек и журналов;
• по окончании года — закрытие номенклатуры дел, всех картотек на исполненные документы и контрольных журналов учета карточек;
• внесение соответствующих отметок в номенклатуру дел;
• при необходимости — внесение закрытых картотек и журналов в инвентарную опись законченных производством дел, картотек и журналов.
Дата закрытия дела — дата оформления заверительного листа в деле. Дело (том) может быть закрыто только после исполнения и подшивки в него всех документов, относящихся к данному делу и году (периоду).
Законченные производством (закрытые) конфиденциальные дела в течение определенного и иногда достаточно длительного времени активно используются в текущей работе сотрудников фирмы, выдаются им для решения тех или иных вопросов.
Особенности процедуры выдачи законченных дел сотрудникам фирмы и приема их от сотрудников:
• проверка работником службы КД полномочий исполнителя — наличия на обложке дела или в карточке учета разрешений и выдачи дела его фамилии в списке сотрудников, допущенных к делу (папке, альбому, дискете);
780
• выдача дела сотруднику под роспись в карточке учета разрешений и выдачи;
• помещение карточки учета разрешений и выдачи дела в картотеку «За исполнителями»;
• при возврате дела сотрудником — проверка соответствия документов дела сведениям, зафиксированным во внутренней описи, контроль комплектности дела и документов, сохранности всех их элементов;
• роспись работника службы КД за возврат дела в карточке учета разрешений и выдачи, а также внутренней описи документов, находящихся у исполнителя;
• помещение дела и карточки в места хранения.
Выданные исполнителям для работы дела должны быть возвращены ими в службу КД в тот же день.
Все указанные процедуры могут выполняться в автоматизированном режиме, который сопровождает специфический набор внемашинных операций. Выдача и возврат исполнителями архивных электронных комплексов документов имеют более сложную технологию, что связано с необходимостью выполнения ряда дополнительных операций по проставлению электронной подписи в учетных формах.
При снятии в установленном порядке с документа грифа конфиденциальности и изъятия его из дела нумерация листов дела сохраняется, но отсутствие листов отмечается во внутренней описи дела с указанием причины изъятия документа и его нового местонахождения. Одновременно такая же отметка вносится в учетную форму документа. Учетная форма остается в картотеке исполненных конфиденциальных документов за соответствующий год и не подлежит перемещению в картотеку открытых документов. Аналогичным образом осуществляется процесс изъятия электронного документа из архивного массива компьютера службы КД или с дискеты.
После изъятия из дела последнего документа, с которого снят гриф конфиденциальности, обложка дела или футляр магнитного носителя вместе с внутренней описью продолжают храниться в службе КД на протяжении указанного в номенклатуре срока и затем уничтожаются. Отметка об уничтожении вносится в номенклатуру дел соответствующего года и (или) инвентарную опись законченных производством дел, картотек и журналов (если такая опись ведется).
Хранение дел с конфиденциальными документами на рабочих местах руководителей и специалистов дольше одного рабочего дня запрещается. Конфиденциальные текущие и архивные дела хранятся централизованно в службе КД в условиях, исключающих их хищение, уничтожение или несанкционированный доступ посторонних лиц. Хранить их вместе с делами открытого доступа не разрешается.
Дела в службе КД хранятся в сейфах (металлических шкафах), которые всегда должны быть заперты. На внутренней стороне дверцы сейфа (шкафа) должна быть наклеена опись архивных дел или номенклатура дел текущего года с указанием особенностей расположения дел на каждой из полок, а также указана последовательность эвакуации дел при экстремальных ситуациях. Дела, как правило, располагаются в последовательности номеров. Магнитные носители информации хранятся в футлярах по тому же принципу, также в металлических шкафах, в ячейках, в вертикальном

положении.
Подготовка конфиденциальных дел к передаче в ведомственный архив (архив фирмы) технологически не отличается от аналогичной работы с делами открытого доступа.
Следовательно, технологическая схема формирования и оформления конфиденциальных дел с достаточной степенью гарантии решает задачи обеспечения сохранности как традиционных дел и документов, так и архивных электронных массивов конфиденциальных документов.

10. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ НА НАИБОЛЕЕ УЯЗВИМЫХ УЧАСТКАХ ОФИСНОЙ ДЕЯТЕЛЬНОСТИ

10.1. Защита информации при проведении совещаний и переговоров

Совещания и переговоры, в процессе которых могут обсуждаться сведения, составляющие тайну фирмы или ее партнеров, именуются обычно конфиденциальными. Порядок проведения подобных совещаний и переговоров регламентируется специальными требованиями, обеспечивающими безопасность ценной, в том числе конфиденциальной, информации (далее — ценной информации), которая в процессе этих мероприятий распространяется в санкционированном (разрешенном) режиме. Основной угрозой ценной информации является разглашение большего объема сведений о новой идее, продукции или технологии, чем это необходимо.
Причины, по которым информация может разглашаться на конфиденциальных совещаниях или переговорах, общеизвестны: слабое знание сотрудниками состава ценной информации и требований по ее защите, умышленное невыполнение этих требований, провоцированные и непровоцированные ошибки сотрудников, отсутствие контроля за изданием рекламной и рекламно-выставочной продукции и др. Оглашение ценной информации в санкционированном режиме должно быть оправдано деловой необходимостью и целесообразностью для конкретных условий и характера обсуждаемых вопросов.
Основные этапы проведения конфиденциальных совещаний и переговоров: подготовка к проведению, процесс их ведения и документирования, анализ итогов и выполнения достигнутых договоренностей.
Разрешение на проведение конфиденциальных совещаний и переговоров с приглашением представителей других организаций и фирм дает исключительно первый руководитель фирмы. Решение первого руководителя о предстоящем конфиденциальном совещании доводится до сведения референта менеджера по безопасности информации, руководителя секретариата, секретаря-референта, менеджера по конфиденциальной документации, управляющего делами фирмы и начальника службы безопасности. В целях дальнейшего контроля за подготовкой и проведением такого совещания информация об этом решении фиксируется референтом в специальной учетной карточке. В этой карточке указываются: наименование совещания или переговоров, дата, время, состав участников по каждому вопросу, лицо, руководитель, ответственный за проведение, ответственный организатор, контрольные отметки, зона сведений о факте проведения, зона сведений по результатам совещания или переговоров.
Плановые и неплановые конфиденциальные совещания, проходящие без приглашения посторонних лиц, проводятся первым руководителем, его заместителями, ответственными исполнителями (руководителями, главными специалистами) по направлениям работы с обязательным предварительным информированием референта. По факту этого сообщения или проведения такого совещания референтом заводится учетная карточка описанной выше формы. Проведение конфиденциальных совещаний без информирования референта не допускается.
Доступ сотрудников фирмы на любые конфиденциальные совещания осуществляется на основе действующей в фирме разрешительной системы доступа персонала к конфиденциальной информации. Приглашение на конфиденциальные совещания лиц, не являющихся сотрудниками фирмы, санкционируется только в случае крайней необходимости их личного участия в обсуждении конкретного вопроса. Присутствие их при обсуждении других вопросов запрещается.
Ответственность за обеспечение защиты ценной информации и сохранение тайны фирмы в ходе совещания несет руководитель, организующий данное совещание. Референт оказывает помощь руководителям и совместно со службой безопасности осуществляет контроль за перекрытием возможных организационных и технических каналов утраты информации.

Подготовку конфиденциального совещания осуществляет организующий его руководитель с привлечением сотрудников фирмы, допущенных к работе с конкретной ценной информацией, составляющей тайну фирмы или ее партнеров. Из числа этих сотрудников назначается ответственный организатор, планирующий и координирующий выполнение подготовительных мероприятий и проведение самого совещания. Этот сотрудник информирует референта о ходе подготовки совещания или переговоров. Полученная информация вносится референтом в учетную карточку.

В процессе подготовки конфиденциального совещания составляются программа проведения совещания, повестка дня, информационные материалы, проекты решений и список участников совещания по каждому вопросу повестки дня. Все документы, составляемые в процессе подготовки конфиденциального совещания, должны иметь гриф «Конфиденциально», изготовляться и издаваться в соответствии с требованиями инструкции по обработке и хранению конфиденциальных документов. Документы (в том числе проекты договоров, контрактов и др.), предназначенные для раздачи участникам совещания, не должны содержать конфиденциальные сведения. Эта информация сообщается участникам совещания устно при обсуждении конкретного вопроса. Цифровые значения наиболее ценной информации (технические и технологические параметры, суммы, проценты, сроки, объемы и т.п.) в проектах решений и других документах не указываются или фиксируются в качестве общепринятого значения, характерного для сделок подобного рода и являющегося стартовой величиной при обсуждении. В проектах не должно быть развернутых обоснований предоставляемых льгот, скидок или лишения льгот тех или иных партнеров, клиентов. Документы, раздаваемые участникам совещания, не должны иметь гриф конфиденциальности.

Список участников конфиденциального совещания составляется отдельно по каждому обсуждаемому вопросу. К участию в обсуждении вопроса привлекаются только те сотрудники фирмы, которые имеют непосредственное отношение к этому вопросу. Это правило касается и руководителей. В списке участников указываются фамилии, имена и отчества лиц, занимаемые должности, представляемые ими учреждения, организации, фирмы и наименования документов, подтверждающих их полномочия вести переговоры и принимать решения. Название представляемой фирмы может при необходимости заменяться ее условным обозначением.

Документом, подтверждающим полномочия лица (если это не первый руководитель) при ведении переговоров и принятии решений по конкретному вопросу, может служить письмо, предписание, доверенность представляемой лицом фирмы, рекомендательное письмо авторитетного юридического или физического лица, письменный ответ фирмы на запрос о полномочиях представителя, в отдельных случаях телефонное или факсимильное подтверждение полномочий первым руководителем представляемой фирмы. Эти документы передаются участниками совещания ответственному организатору непосредственно перед началом совещания для последующего включения их референтом в дело, содержащее все материалы по данному совещанию или переговорам.

Документы, составляемые при подготовке конфиденциального совещания, на котором предполагается присутствие представителей других фирм и организаций, согласовываются с референтом и руководителем службы безопасности. Отмеченные ими недостатки в обеспечении защиты ценной информации должны быть исправлены ответственным организатором совещания. После этого документы утверждаются руководителем, организующим совещание.

Одновременно с визированием подготовленных документов референт, руководитель службы безопасности и ответственный организатор определяют место проведения совещания, порядок доступа участников совещания в это помещение, порядок документирования хода обсуждения вопросов и принимаемых решений, а также порядок рассылки (передачи) участникам совещания оформленных решений и подписанных документов.

Любое конфиденциальное совещание организуется в специальном (выделенном) помещении, имеющем лицензию на проведение подобного мероприятия и, следовательно, оборудованном средствами технической защиты информации. Доступ в такие помещения сотрудников фирмы и представителей других фирм и организаций разрешается руководителем службы безопасности.

Перед началом конфиденциального совещания сотрудник службы безопасности обязан убедиться в отсутствии в помещении несанкционированно установленных аудио- и видеозаписывающих или передающих устройств и в качественной работе средств

технической защиты на всех возможных каналах утечки информации. Помещение должно быть оборудовано кондиционером, так как открытие окон, дверей в ходе совещания не допускается. Окна закрываются светопроницаемыми шторами, входная дверь оборудуется сигналом, оповещающим о ее неплотном закрытии. В целях звукоизоляции целесообразно иметь двойную дверь (тамбур) или зашторивать двери звукопоглощающей тканью.

Проведение совещания в неприспособленных и необорудованных соответствующим образом помещениях фирмы (кроме кабинета первого руководителя) не разрешается.

В помещении для проведения конфиденциальных совещаний не должны находиться приборы, оборудование и технические средства, которые непосредственно не используются для обеспечения хода совещания (например, телефоны городской сети, ПЭВМ, телевизионные и радиоприемники и др.). При необходимости они размещаются в соседней, изолированной комнате. Аудио- и видеозапись конфиденциальных совещаний, фотографирование ведутся только по письменному указанию первого руководителя, фирмы и осуществляются одним из сотрудников фирмы, готовивших совещание. Чистый магнитный или фотографический носитель информации для этих целей выдается референтом под роспись в учетной форме и возвращается ему с зафиксированной информацией по окончании каждого дня работы совещания.

Доступ участников конфиденциального совещания в помещение, в котором оно будет проводиться, осуществляет ответственный организатор совещания под контролем сотрудника службы безопасности в соответствии с утвержденным списком и предъявляемыми участниками персональными документами. Перед началом обсуждения каждого вопроса состав присутствующих корректируется. Нахождение (ожидание) в помещении лиц, в том числе сотрудников данной фирмы, не имеющих отношения к обсуждаемому вопросу, не разрешается.

Целесообразно, чтобы при открытии совещания организовавший его руководитель напомнил участникам о необходимости сохранения производственной и коммерческой тайны, уточнил, какие конкретные сведения являются конфиденциальными на данном совещании.

Ход конфиденциального совещания документируется одним из готовивших его сотрудников или секретарем-стенографисткой. На закрытых совещаниях с повышенным уровнем конфиденциальности эту работу выполняет непосредственно ответственный организатор совещания. Составляемый протокол (стенограмма) должен иметь гриф конфиденциальности необходимого уровня и оформляться в стенографической тетради, зарегистрированной референтом.

Целесообразность записи участниками хода совещания определяет руководитель, организовавший совещание, исходя из содержания информации, которая оглашается. Руководитель имеет право не разрешить участникам совещания вести какие-либо записи или санкционировать ведение этих записей на листах бумаги, зарегистрированных референтом, с последующей сдачей их этому лицу и доставкой курьерами фирмы по месту работы участников совещания.

При необходимости вызова на проходящее совещание дополнительных лиц (экспертов, консультантов, представителей других фирм и организаций) факт их участия в совещании фиксируется в протоколе с указанием мотивов вызова. Присутствие этих лиц на совещании ограничивается временем рассмотрения той ситуации, по которой они были вызваны.

Участникам конфиденциального совещания, независимо от зажимаемой должности и статуса на совещании, не разрешается:

• вносить в помещение, в котором проводится совещание, фото-, кино- и видеоаппаратуру, компьютеры, магнитофоны, плейеры, диктофоны, радиоприемники, радиотелефоны и другую аппаратуру, пользоваться ею;

• делать выписки из документов, используемых при решении вопросов на совещании и имеющих гриф ограничения доступа;

• обсуждать вопросы, вынесенные на совещание, в местах общего пользования;

• информировать о совещании (вопросах повестки дня, составе участников, времени и месте проведения, ходе обсуждения вопросов, содержании решений и т.п.) любых лиц, не связанных с проведением данного совещания, в том числе сотрудников фирмы.

Участники совещания, замеченные в несанкционированной аудио- или видеозаписи, использовании средств связи, фотографировании, лишаются права дальнейшего присутствия на совещании. По факту составляется акт, копия которого направляется

фирме, представителем которой является данное лицо, или передается первому руководителю фирмы — организатора совещания, если это лицо является сотрудником последней. Одновременно носитель несанкционированно записанной информации передается референту для учета и хранения (или уничтожения). Устройство записи возвращается владельцу. Участники совещания не могут оглашать больший объем ценных сведений, чем это было установлено при подготовке совещания, или сообщать сведения, не относящиеся к обсуждаемому вопросу. Состав оглашаемых сведений регламентируется руководителем, организовавшим совещание.

По окончании конфиденциального совещания сотрудник службы безопасности осматривает помещение, запирает, опечатывает и сдает под охрану.

Документы, принятые на совещании, оформляются, подписываются, при необходимости размножаются и рассылаются (передаются) участникам совещания в соответствии с требованиями по работе с конфиденциальными документами фирмы. Все экземпляры этих документов должны иметь гриф ограничения доступа. Рассылать документы, содержащие строго конфиденциальную информацию, не разрешается.

При проведении переговоров по заключению, продлению или прекращению какого-либо договора (контракта) должны соблюдаться некоторые дополнительные требования, соблюдение которых контролирует референт.

В процессе подготовки переговоров первоначально необходимо выяснить намерения организации или фирмы, с которой предполагаются переговоры. Если это мало известная фирма, то целесообразно получить о ней подробную информацию, чтобы избежать ошибочного выбора партнера или клиента. Подготовительная работа к проведению переговоров предполагает выработку плана переговоров и определение на этой основе дозированного состава ценной информации, которую допускается использовать в общении с участниками переговоров, порядка ее оглашения и условий возникновения в этом рабочей необходимости. Сообщаемые на этом этапе сведения не должны содержать производственной или коммерческой тайны. Сотрудникам фирмы, участвующим в переговорах, не разрешается использовать в дискуссии конфиденциальную информацию и раскрывать желаемые результаты переговоров, итоги аналогичных переговоров с другими партнерами. В процессе неофициальной части переговоров обсуждение вопросов, связанных с содержанием и ходом дискуссии, не допускается.

При ведении переговоров не следует сразу же передавать партнеру всю запрашиваемую им информацию в полном объеме. Прежде всего следует выяснить, с какой целью ему необходимы эти сведения и как знание этих сведений отразится на ходе дальнейшего сотрудничества с ним. На этом этапе переговоров, при выяснении сути взаимных намерений, целесообразно строить дискуссию таким образом, чтобы ответы на вопросы были максимально лаконичными («да — нет», «можем — не можем»). Однако после юридического оформления взаимоотношений и подписания партнерами, клиентами обязательства о неразглашении ценных сведений они могут быть более подробно ознакомлены с предметом договора. В договоре по итогам переговоров должно найти отражение взаимное обязательство сторон о защите ценных и особенно конфиденциальных сведений, недопустимости передачи их без предварительного согласия сторон третьему лицу, необходимости ознакомления с предметом договора ограниченного числа сотрудников, которые предварительно должны подписать обязательства о сохранении в тайне полученных сведений.

В коммерческой практике местом проведения переговоров часто становятся постоянно действующие и периодические торговые или торгово-промышленные выставки и ярмарки. Референт должен знать порядок защиты ценной информации фирмы в ходе этих переговоров, инструктировать их участников и контролировать соблюдение ими установленных правил.

Любая выставка является, с одной стороны, отличным источником полезной для бизнеса информации, объектом добросовестного маркетингового исследования рынка товаров, а с другой — опасным каналом несанкционированного получения конфиденциальных сведений, касающихся новых идей, технологий и продукции. Обобщенно источники ценных сведений в процессе выставочной деятельности включают в себя: экспозицию, персонал фирмы, участвующий в выставке, и рекламно-выставочные материалы. Утрата ценной информации происходит в результате общения специалистов родственных профессий, но разных фирм и наличия в выставочной экспозиции самого нового продукта. Проводимые параллельно с выставочными мероприятиями пресс-конференции, семинары, презентации фирм и товаров

создают дополнительную угрозу сохранности ценной информации.
Работа персонала фирмы с посетителями выставки должна быть строго регламентирована, прежде всего в части состава оглашаемых сведений о продукции, технических и технологических новшествах, заключенных в этой продукции. Обязательно учитывается, что состав этих сведений дифференцируется в зависимости от категории посетителей — массового посетителя-дилетанта («любителя») и посетителя — специалиста в данной области («эксперта»). Целесообразно использовать метод «черного ящика», при котором посетителю сообщается все, что касается назначения продукции и ее потребительских качеств, но остаются в тайне технология и способы, которыми достигнуты эти качества, функциональные возможности продукции. Поэтому персоналу, обслуживающему экспозицию фирмы, должны быть недоступны сведения о продукции, отнесенные к производственной или коммерческой тайне. В свою очередь, специалисты фирмы, осведомленные о ее секретах, не должны участвовать в работе выставочного стенда. Объясняется это тем, что специалист в процессе дискуссии с посетителем может увлечься и сообщить больший объем сведений, чем это предусмотрено. Не допускается знакомить посетителей, клиентов и партнеров с изобретателями, конструкторами, технологами, работающими над новыми идеями и новой продукцией.
Рекламно-выставочные материалы (проспекты, пресс-релизы, прайс-листы, брошюры и т.п.) следует рассматривать как контролируемый канал распространения ценных сведений. При этом следует помнить, что этот канал тщательно и глубоко анализируется конкурентом с целью выявления тех сведений, которые составляют тайну фирмы, издавшей рекламные материалы.
Защита информации в рекламно-выставочной деятельности предусматривает заблаговременный анализ, экспертизу предназначенной для широкого оглашения любой информации о деятельности фирмы и ее продукции в целях обнаружения в содержании или элементах отображения этой информации (таблицах, формулах, рисунках, фотографиях, схемах) конфиденциальных сведений или намека на наличие таких сведений. Подобная информация должна, как правило, анализироваться от противного — с точки зрения того интереса, который будет проявлен к ней конкурентами, и объема полезных сведений, извлекаемых конкурентом из ее содержания. Материалы, не прошедшие экспертизу, публикации не подлежат. Экспертиза включает также последующий контроль всех опубликованных о фирме материалов, сообщений средств массовой информации, рекламных изданий и рекламно-выставочных проспектов. Помимо этого анализируются подобные материалы других фирм для определения возможной утраты ценных сведений. Рекламно-выставочные издания не должны сигнализировать недобросовестному конкуренту о том, что и где искать.
Чтобы предотвратить разглашение ценных сведений в рекламно-выставочных материалах, следует заблаговременно:
• проанализировать множество предполагаемых к изданию и изданных материалов с точки зрения возможности извлечения из них ценных конфиденциальных сведений;
• осуществить разбиение (дробление) информации на части и распределение их между разными рекламно-выставочными материалами, предназначенными для массового посетителя и посетителей-специалистов, издать серию дополнений к основному проспекту для специалистов разного профиля;
• осуществить разбиение информации по видам и средствам рекламы — традиционным бумажным изданиям, электронной рекламе, Web-странице, рекламе в средствах массовой информации и др.
Вместе с тем должен соблюдаться разумный баланс: рекламно-выставочные материалы не должны быть мало информативными для посетителей, все наиболее важные параметры новой продукции должны найти в них отражение.
Следовательно, подготовка и проведение совещаний и переговоров по конфиденциальным вопросам, оформление их результатов связаны с выполнением ряда обязательных процедур, необходимых для правильной организации работы организаторов и участников этих мероприятий. При несоблюдении изложенных требований возникает серьезная опасность разглашения или утечки ценных сведений и секретов фирмы, ее партнеров и клиентов, Контроль за выполнением этих требований возлагается на референта, который обеспечивает информационную безопасность деятельности фирмы, сохранение ее деловых и производственных секретов.

10.2. Защита информации при работе с посетителями

Организация приема посетителей имеет не только общеизвестный набор функций, но и другую менее изученную, но актуальную сторону, затрагивающую сферу обеспечения информационной безопасности деятельности фирмы при работе с посетителями. Профессионализм персонала фирмы предполагает сочетание умения организовать эффективную и полезную для фирмы работу с посетителями и одновременно выполнить ее таким образом, чтобы была сохранена конфиденциальность и целостность ценной информации, достигнута безопасность деятельности фирмы.

Под посетителем понимается, во-первых, лицо, которому необходимо решить определенный круг деловых или личных вопросов с руководителями и менеджерами фирмы, и, во-вторых, лицо, совместно с которым полномочные лица вырабатывают определенные решения по направлениям деятельности фирмы. Посетители не только по определению, но и по существу представляют собой сложный и неоднозначный круг людей, что требует прежде всего грамотного решения вопросов защиты ценной, в том числе конфиденциальной, информации от угроз, которые могут создать ей посетители. Поэтому организацию приема посетителей и контроль за работой с ними целесообразно централизовать на уровне референта или секретаря-референта первого руководителя фирмы. Работа именно этого сотрудника фирмы в наибольшей степени связана с посетителями и требует грамотного подхода к ее выполнению.

Процесс защиты информации при приеме посетителей предполагает проведение четкой их классификации, на базе которой формируется система ограничительных, технологических, контрольных и аналитических мер, призванных не допустить несанкционированный доступ к ним посетителей. Эти меры позволяют также в определенной степени гарантировать физическую безопасность сотрудников, работающих с посетителями.

Прием посетителей и установление с ними деловых взаимоотношений достаточно сложный процесс для руководителей фирмы и ее структурных подразделений (направлений деятельности), специалистов-менеджеров. На уровне руководителей фирмы посетителей можно разделить на две категории: сотрудники фирмы и посетители, не являющиеся ее сотрудниками.

К посетителям — сотрудникам фирмы относятся:

• сотрудники, имеющие право свободного входа в кабинет руководителя в любое время рабочего дня (заместители руководителя, референты, секретари);

• сотрудники, работающие с руководителем в режиме вызова или решающие с ним деловые вопросы в часы приема по служебным делам (нижестоящие руководители, эксперты, специалисты-менеджеры);

• сотрудники, инициирующие свой прием руководителем в часы приема поличным вопросам.

Угрозы информационной безопасности, исходящие от посетителей-сотрудников, могут наступить в случае, если эти сотрудники являются злоумышленниками (тайными представителями конкурирующих фирм, агентами служб промышленного или экономического шпионажа, криминальных структур) или их сообщниками. Состав угроз может быть самым разнообразным: от кражи документов со стола руководителя до выведывания нужной информации с помощью хорошо подготовленного перечня, на первый взгляд, безобидных вопросов. Может случиться также, что сотрудник, получивший при общении с руководителем больший объем ценной информации, чем это необходимо ему для работы, разглашает ее постороннему лицу по причине элементарной безответственности.

Посетители, не являющиеся сотрудниками фирмы, в соответствии с характером их взаимоотношений с фирмой могут подразделяться на:

• лиц, не включенных в штат сотрудников, но входящих в качестве членов в коллективный орган управления деятельностью фирмы (акционеры<члены различных советов и др.);

• представителей государственных учреждений и организаций, с которыми фирма сотрудничает в соответствии с законом (работники различных инспекций, муниципальных органов управления, правоохранительных органов и др.);

• сотрудничающих с фирмой физических лиц и представителей предприятий и организаций, банков, рекламных агентств, торговых представительств, средств массовой информации (клиенты, партнеры, коммерсанты, инвесторы, спонсоры, журналисты и др.);

• представителей иных государственных и негосударственных структур, с которыми

фирма не имеет деловых отношений;
• частных лиц.
Перечисленные представители и лица должны находиться под особо внимательным контролем референта, так как если они относятся к категории злоумышленников, спектр исходящей от них опасности крайне велик и определяется теми целями, которые перед ними поставлены. Утрата информации может идти по организационным или техническим каналам или в сочетании того и другого. Например: шантаж руководителя и запись беседы на диктофон, установка подслушивающего устройства, фотографирование документов на столе руководителя и др. Не исключено силовое воздействие на руководителя в целях получения нужных сведений.
На уровне руководителей подразделений и специалистов-менеджеров фирмы выделяются аналогичные группы посетителей, но в каждой категории и группе посетители делятся на: 1) направленных руководителем и 2) пришедших на прием без санкции руководителя.
При приеме руководителем фирмы любой из указанных категорий и групп посетителей референту следует соблюдать следующие основные правила организации приема.
Руководитель не должен принимать посетителей во время, выделенное для творческой работы с документами и базами электронных данных, особенно конфиденциальными. При вызове кого-либо из менеджеров в связи с работой над документом на столе руководителя должен находиться только тот документ, с которым он работает, другие документы следует хранить в запертом сейфе или металлическом шкафу. Целесообразно, чтобы в это время в кабинет руководителя никто не заходил без вызова, в том числе и лица, имеющие право свободного входа в кабинет.
В целях ограничения возможностей для злоумышленника получить необходимые ему сведения за счет неупорядоченной организации труда руководителя, суеты в работе с документами и посетителями для приема посетителей любых категорий следует выделить специальные часы, в течение которых руководитель не должен работать с документами, не относящимися к визиту того или иного лица, или вести деловые переговоры по телефону. Различные категории посетителей целесообразно принимать в разные часы.
Прежде всего выделяется время для ежедневного приема нижестоящих руководителей и менеджеров фирмы по служебным вопросам. Во-вторых, выделяется время для ежедневного приема посетителей, не являющихся сотрудниками фирмы, но представляющих ту или иную организационную структуру. В-третьих, отдельные часы приема выделяются в разные дни для частных (посторонних) лиц, которым необходимо решить вопрос, относящийся к компетенции руководителя. В часы приема указанных категорий посетителей любые сотрудники фирмы могут посещать руководителя только по вызову и только по вопросу, связанному с визитом конкретного посетителя. В-четвертых, периодически выделяются часы приема сотрудников фирмы по личным вопросам.
Посетители, в том числе сотрудники фирмы, не должны входить в кабинет руководителя в пальто, шубе или иметь при себе объемные кейсы, чемоданы, сумки — их следует оставлять в приемной.
Не допускается оставлять посетителя одного при выходе руководителя из кабинета. Во время отсутствия руководителя никто из посетителей или персонала фирмы не должен входить в его кабинет.
Наиболее тщательно должна быть организована работа референта с посетителями, которые не являются сотрудниками фирмы. Следует учитывать, что посещение руководителя, как правило;
является начальной стадией их визита в фирму. Другие стадии, в соответствии с решением руководителя, будут связаны с посещением нижестоящих руководителей и специалистов-менеджеров. С точки зрения необходимости решения задач обеспечения информационной безопасности фирмы таких посетителей можно классифицировать следующим образом:
• по степени разрешенного им доступа в помещения фирмы:
во все помещения, только в определенные помещения, только к определенному сотруднику, только в операционный зал общего доступа;
• по степени разрешенного им ознакомления с информацией фирмы: только с рекламными изданиями, только с материалами, касающимися заинтересованной структуры или лица, только с материалами по определенному вопросу только с открытыми служебными материалами фирмы, только с конкретными конфиденциальными сведениями. Любые разрешительные действия в отношении посетителей совершаются первым руководителем

фирмы и контролируются при реализации службой безопасности.
Работа референта с посторонним посетителем состоит из следующих этапов:
• подготовительный этап;
• идентификация и регистрация посетителя;
• организация приема посетителя руководителем;
• организация дальнейших действий посетителя. Подготовительный этап предназначен для согласования возможности и условий приема посетителя руководством или сотрудником фирмы. Визит, как правило, инициируется самим посетителем и должен быть заранее обсужден им по телефону, электронной почте или факсу с руководителем или референтом, а также с менеджером, если посетитель предполагает решить с ним возникший вопрос. В процессе согласования визита выясняется цель предполагаемого посещения фирмы, состав необходимых для ознакомления документов, дата и время посещения. Визит к руководителю предполагает, что посетителю необходимо решить вопрос, входящий в компетенцию этого должностного лица, или при необходимости получить санкцию руководителя на выполнение определенной работы в подразделении фирмы и ознакомление с документами, базами данных. В других случаях посетителя следует направить к специалисту-менеджеру, в компетенцию которого входит рассмотрение интересующего посетителя вопроса.
По результатам согласования уточняется должностное лицо фирмы, которое вправе решить поставленный посетителем вопрос, корректируются дата и время визита. После согласования фамилия, имя, отчество посетителя, наименование представляемой организационной структуры и указанные выше сведения вносятся в график приема посетителей фирмы.
Составление, уточнение и дополнение графика приема посетителей является обязанностью референта. График согласовывается референтом с руководителями и специалистами-менеджерами в начале предыдущего рабочего дня. О намеченном визите и часах Приема напоминается будущему посетителю.
Ежедневное число посетителей должно соответствовать реальному времени, отведенному руководителем или менеджером на этот вид работы. В часы приема каждой из категорий и групп посетителей важно четко определить период нахождения каждого посетителя в приемной и кабинете руководителя или на рабочем месте менеджера, для чего устанавливаются очередность приема и предполагаемая продолжительность переговоров. Сложные и длительные по времени вопросы обсуждаются в первую очередь. Особенно четко должен регламентироваться прием лиц, не являющихся сотрудниками фирмы. Следует планировать прием таким образом, чтобы посетители длительное время не находились в приемной, так как подобные ожидания всегда сопровождаются подсознательным или умышленным прослушиванием переговоров в Приемной, получением значительного объема ценной информации. Возможно фиксирование злоумышленником переговоров с помощью диктофона или миниатюрной видеокамеры. Не допускается организовывать очередность приема путем образования так называемой «живой очереди».
График целесообразно формировать централизованно в виде единой схемы, охватывающей посетителей руководства фирмы и структурных подразделений. Руководители подразделений и менеджеры обязаны ежедневно сообщать референту о согласованных с ними визитах посетителей для включения фамилий в график приема. Это позволяет обеспечить высокую достоверность включаемых в график сведений и контролировать обоснованность визитов посетителей на уровне подразделений фирмы. В помещениях фирмы не должны находиться посторонние лица, относящие себя к категории посетителей, хотя их визит не был согласован и зафиксирован в графике приема.
На основании графика референт ежедневно в начале рабочего дня сообщает сведения о посетителях и характере разрешенного из доступа к делам фирмы в службу безопасности для оформления Пропусков. Пропуск может оформляться только по инициативе референта. Одновременно он напоминает сотрудникам структурных подразделений фамилии посетителей, визит которых намечен на текущий день, и время приема. При изменении даты визита необходимое исправление вносится в график приема посетителей, а посетитель в обязательном порядке заблаговременно информируется об этом. С ним согласовывается новая дата визита и время.
Идентификация, т.е. установление соответствия личности посетителя сведениям в графике приема и документе, удостоверяющем его личность, выполняется на двух уровнях: а) сотрудником службы безопасности при входе в здание фирмы и выдаче

посетителю пропуска; б) референтом при входе посетителя в приемную руководителя фирмы. На первом уровне идентифицируется личность посетителя и соответствие фамилии, имени, отчества записи в переданном референтом в службу безопасности перечне посетителей на конкретный день и час. При входе в помещение фирмы (кроме операционного зала общего доступа) посетитель обязан предъявить сотруднику службы безопасности паспорт или служебное удостоверение, подтверждающие его личность (но не визитную карточку). Особое внимание обращается на выявление подлинности предоставленного персонального документа и установление соответствия фотокарточки в этом документе внешним данным посетителя. После идентификации посетителю выдается подготовленный заранее соответствующий визуальный идентификатор (пропуск), регламентирующий его права в помещениях фирмы. Перемещение посетителя в здании осуществляется только в сопровождении работника фирмы — секретаря, менеджера, с которым посетитель обговорил свой визит, сотрудника службы безопасности.

Все посетители фирмы, в том числе посетители структурных подразделений, сначала направляются к референту с целью их идентификации и регистрации. Войдя в приемную руководства, фирмы, посетитель должен предъявить референту удостоверяющий его личность документ и предписание. Идентификация посетителя на этом уровне предполагает проверку соответствия его Личности, места работы и должности сведениям, указанным в графике приема. При возникновении каких-либо сомнений в личности посетителя референт может уточнить сведения о нем в организации, которую представляет данное лицо (по телефону, факсу, электронной почте). Если сомнения не устранены, референт должен получить разрешение на доступ данного посетителя в кабинет руководителя или структурное подразделение от начальника службы безопасности фирмы.

После завершения этапа идентификации референт на основе предоставленных документов вносит сведения о посетителе в традиционный или электронный журнал учета (регистрации) посетителей. Указываются: дата и время приема, фамилия, имя, отчество посетителя, место работы и должность, наименование вопроса, исходные данные предписания, фамилия сотрудника фирмы, ответственного за визит, принятое решение. Группа посетителей, прибывшая для переговоров, регистрируется пофамильно. Записи делаются в журнале лично референтом. Не допускается, чтобы посетитель знакомился со сведениями в графике приема и журнале регистрации посетителей, так как информация, включаемая в эти учетные формы, является конфиденциальной, раскрывающей деловые связи фирмы. После регистрации посетители структурных подразделений направляются по назначению в сопровождении встретивших их секретарей или менеджеров, а посетители руководителей фирмы остаются в приемной, и референт приступает к организации их приема руководителем. Ожидающий приема посетитель должен находиться на значительном расстоянии от рабочих мест референта, секретаря-референта, секретаря, чтобы он не мог видеть документы, находящиеся на их столах, экран дисплея, прослушивать их переговоры по средствам связи. Холл для ожидающих приема посетителей может отделяться от рабочего места референта стеклянной тонированной перегородкой. При приеме посетителей референту не разрешается покидать помещение приемной даже на непродолжительное время. Переговоры с руководителем ведутся им по соответствующему коммуникативному устройству.

В период ожидания посетителем приема референту целесообразно внимательно наблюдать за его поведением, фиксировать возможные странности в движениях, излишнюю возбужденность и т.п. Под особым контролем референта должна находиться группа посетителей, ожидающих приема для переговоров по одному вопросу, например заключение контракта, получение согласия на выполнение определенной работы и др. При возникновении каких-либо опасений референт должен вызвать сотрудника службы безопасности, который будет присутствовать в кабинете при беседе руководителя с посетителем или посетителями. Сотруднику этой службы не следует быть в традиционной униформе подразделения охраны, внешне он не должен отличаться от других работников фирмы. При приеме частных (иногда случайных) лиц руководитель может вести беседу не в рабочем кабинете, а в специально предназначенном для этого помещении, в присутствии сотрудника службы безопасности. Переговоры руководителя с посетителем могут документироваться секретарем-стенографисткой или записываться на магнитный носитель с помощью диктофона, видеокамеры.

Посетитель — представитель другой организационной структуры предъявляет

руководителю предписание, в котором указываются его полномочия, цель и задачи визита в данную фирму, состав сведений и документов, которые ему необходимы для ознакомления или анализа. Представление оформляется на бланке организации, подписывается первым руководителем, подпись руководителя заверяется печатью. На предписании руководитель фирмы пишет резолюцию, в которой дает разрешение посетителю на выполнение стоящих перед ним задач, устанавливает порядок и сроки его работы, регламентирует конкретный состав информации, к которой может быть допущен посетитель, назначает сотрудника фирмы, функциональные обязанности которого соответствуют цели визита посетителя, ответственным за работу с этим лицом. Руководитель имеет право не давать разрешения или ограничить характер работы посетителя в фирме. Устные пожелания посетителя, не имеющего предписания, и пожелания, не устраивающие руководителя, выполняться не должны.

Прием посетителя или группы посетителей может иметь формул-переговоров, например о поставках продукции, финансовой помощи, совместных исследованиях и другим вопросам. В переговорах могут участвовать сотрудники фирмы, состав которых был} заранее определен и внесен в график приема. Ход переговоров обычно фиксируется секретарем-стенографисткой. Прием посетителей (групп посетителей, делегаций) может также иметь формуй экскурсий по фирме (предприятию) с целью ознакомления с возможностями фирмы и применяемыми прогрессивными технологиями. В этом случае заблаговременно определяется маршрут движения группы, состав объектов для ознакомления, готовится и издается иллюстративный материал (проспекты, видеофильмы, Web-страницы на дискетах и др.). Программа пребывания группы посетителей на территории фирмы (предприятия) должна сочетать максимальное гостеприимство и высокую степень ограничения в передаче посетителям дозированной информации о производственных и деловых процессах. Лаборатории, исследовательские центры демонстрироваться посетителям не должны.

По окончании приема руководителем референт организует дальнейшие действия посетителя: или посетитель в сопровождении сотрудника службы безопасности направляется к выходу из здания, или секретарь-референт вызывает в приемную секретаря руководителя подразделения фирмы или специалиста-менеджера, к которым посетитель направлен для решения важных для него задач, в том числе содержащихся в предписании. Референт вносит необходимое дополнение в пропуск-идентификатор посетителя, заверяя сделанную запись штампом приемной. Соответствующая запись делается в журнале регистрации посетителей. При необходимости референт предупреждает посетителя о недопустимости разглашения полученных во время визита сведений. Целесообразно, чтобы посетитель подписал письменное обязательство о сохранении в тайне секретов фирмы. Одновременно референт напоминает руководителю подразделения или менеджеру о порядке предоставления посетителю минимально необходимого состава документов и сведений. Предписание передается референтом лицу, сопровождающему посетителя, для использования в работе и включения в дело; посетителю оно не возвращается. При отрицательном решении руководителя предписание передается им референту для включения в соответствующее дело.

Сведения о посетителях, работа которых в здании фирмы будет продолжаться несколько дней или во внерабочее время, вносятся референтом в специальный журнал учета работы посетителей. Одновременно эти сведения сообщаются в службу безопасности для выдачи посетителю необходимого пропуска-идентификатора и контроля за его пребыванием в здании фирмы. В журнале службы безопасности ежедневно делаются отметки о времени прихода и ухода посетителя.

По истечении часов приема посетителей любой категории кабинет руководителя осматривается сотрудником службы безопасности в присутствии референта с целью обнаружения забытых посетителями вещей, документов, выявления возможно установленных посетителями подслушивающих и записывающих устройств, взрывных, химических и самовозгорающихся материалов и т.п.

В подразделениях фирмы соблюдается в целом тот же порядок приема и работы с посетителями. Посетителю, направленному в подразделение вышестоящим руководителем, с учетом занятости руководителя подразделения или менеджера может быть назначен другой день приема. Однако более правильно организовать работу посетителя таким образом, чтобы в течение одного визита в фирму он смог решить все необходимые задачи.

Посетитель может быть допущен только к тем документам, сведениям, которые указаны в предписании и работа с которыми ему разрешена в резолюции руководителя. Ознакомление с документами осуществляется в присутствии сотрудника подразделения, назначенного в резолюции ответственным за выполнение посетителем порученного ему задания. Записи и выписки из документов, которые делает посетитель, могут выполняться на учтенном референтом носителе и затем пересылаться с курьером по месту работы посетителя. Факт ознакомления посетителя с любым конфиденциальным или открытым документом фирмы фиксируется в учетной форме этого документа. На самом документе посетитель ставит визу ознакомления, расшифровку росписи, наименование организации и дату. Не разрешается знакомить посетителя с документами и другими информационными ресурсами фирмы, даже если они связаны с целью его визита, без письменной санкции первого руководителя фирмы. В устных беседах с посетителем запрещается сообщать ему открытые или конфиденциальные сведения, которые не оговорены в резолюции руководителя, делать намек на наличие таких сведений.

Все перемещения посетителя в здании фирмы осуществляются в строгом соответствии с выданным ему идентификатором, желательно — в сопровождении менеджера или секретаря. Наблюдение за передвижением и работой посетителя может быть организовано с помощью видеокамер. Бесконтрольное пребывание посетителя в здании фирмы не допускается. Посетители, нарушившие правила работы с информационными ресурсами фирмы, замеченные в попытке проникновения в другие помещения фирмы или несанкционированного получения ценных сведений у персонала, лишаются права дальнейшего пребывания в здании фирмы. По окончании работы в структурном подразделении посетитель покидает здание в сопровождении сотрудника службы безопасности. При выходе посетитель сдает идентификатор (пропуск).

Посетитель-злоумышленник, получивший доступ в здание фирмы, может использовать его в криминальных целях, для создания определенной, выгодной ему экстремальной ситуации. В числе основных видов подобных ситуаций, которые может провоцировать посетитель, следует назвать следующие: поджог или задымление помещений с целью ограбления, овладения документами, делами, личными вещами сотрудников, захват сотрудников в заложники, угроза физического насилия с целью выведать у сотрудника нужные сведения, получить документы, материальные ценности и др. Самостоятельная ликвидация указанных экстремальных ситуаций силами работников службы безопасности не разрешается, так как требует специальных знаний, умений и осуществляется правоохранительными и противопожарными органами.

Чтобы предотвратить возникновение по вине посетителей той или иной экстремальной ситуации персонал фирмы должен неукоснительно соблюдать указанные выше требования безопасности при приеме посетителей и работе с ними. Всегда целесообразнее предупредить экстремальную ситуацию, чем ликвидировать ее последствия. Важно, чтобы персонал фирмы был заблаговременно обучен выполнению необходимых действий в случае возникновения конкретной экстремальной ситуации. У каждого сотрудника должна сложиться система устойчивых стереотипов (мотиваций) поведения в неординарных условиях.

Разработка системы противодействия злоумышленнику и обучение сотрудников возлагается на службу безопасности. Система предусматривает классификацию экстремальных ситуаций для конкретной фирмы, систематическое проведение учебных занятий для должностных групп персонала, работающих с посетителями, обучение нормам поведения в том или ином случае, разработку схемы оповещения персонала об опасности и вступлении в действие плана эвакуации документов, дел, ценного оборудования, разработку схемы оповещения правоохранительных и противопожарных органов и служб, схемы эвакуации персонала в безопасную зону и др.

Обучение персонала должно включать изучение нормативных и плановых документов, решение ситуационных задач и проведение регулярных деловых игр. Большое значение имеет не только наличие необходимых нормативных и плановых документов, схем, программ обучения и инструктирования сотрудников, но и инженерно-техническое обеспечение действий персонала. Здесь следует отметить необходимость функционирования в здании фирмы современных средств оповещения: о возгораниях, задымлении, нападении на сотрудника и т.п. Например, при приеме посетителей руководитель и референт должны располагать исправной сигнализацией для вызова сотрудника службы безопасности или оповещения этой службы о нападении. Устройство

включения сигнализации должно находиться в доступном и скрытом от злоумышленника месте рабочего стола или на полу.
Следовательно, разработка и использование в практической деятельности любой фирмы эффективной системы обеспечения информационной безопасности в процессе приема и работы с посетителями является одной из важных частей системы защиты ценной информации, охраны материальных ценностей фирмы, жизни и здоровья ее персонала.

10.3. Защита информации в работе кадровой службы

Работа службы персонала, управления или отдела кадров, менеджера по персоналу, иногда, в некрупных фирмах, — секретаря-референта (далее — отдела кадров) связана с накоплением, формированием, обработкой, хранением и использованием значительных объемов сведений о всех категориях сотрудников. Эти сведения относятся к так называемым персональным данным, которые по своей сути отражают личную или семейную тайну граждан, их частную жизнь и входят в круг информации, подлежащей защите от несанкционированного доступа.
Личная тайна гражданина охраняется Конституцией Российской Федерации. Разглашение этой тайны, т.е. бесконтрольное распространение персональных данных во времени и пространстве, может нанести значительный ущерб физическому лицу. Понятие личной тайны близко примыкает к семейной тайне. Семейная тайна или тайна нескольких физических лиц, членов семьи не тождественна личной тайне по составу защищаемых сведений. Например, к семейной тайне относятся: тайна усыновления, тайна отцовства, тайна наследственного заболевания и др.
Под персональными данными (информацией о гражданах) понимается любая документированная информация, относящаяся к конкретному человеку. Персональные данные идентифицируют его личность. Субъектами персональных данных являются граждане Российской Федерации, иностранные граждане и лица без гражданства, находящиеся на территории России, к личности которых относятся соответствующие персональные данные. Держатели персональных данных — органы государственной власти и местного самоуправления, предприятия, учреждения, организации, юридические и физические лица, осуществляющие владение и пользование этими данными. Пользователями персональных данных могут быть органы государственной власти и местного самоуправления, предприятия, учреждения, организации, юридические и физические лица, обращающиеся к держателю данных за получением необходимых им персональных данных и пользования ими без права передачи.
Персональные данные всегда относятся к категории конфиденциальной информации. Не допускается сбор, передача, уничтожение, хранение, использование и распространение информации о частной жизни, а равно информации, нарушающей личную тайну, семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений физического лица без его согласия, кроме как на основании судебного решения. Режим конфиденциальности персональных данных снимается в случаях обезличивания этих данных или по истечении 75 лет срока их хранения, если иное не определено законом.
Работа с персональными данными должна осуществляться только в целях, по перечням и в сроки, которые необходимы для выполнения задач соответствующего держателя или пользователя персональных данных, и устанавливается действующим законодательством, лицензией или договором. Персональные данные не могут быть использованы в целях причинения имущественного и (или) морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан на основе использования информации об их социальном происхождении, расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.
Субъект персональных данных самостоятельно решает вопрос передачи кому-либо сведений о себе за исключением случаев, предусмотренных законодательством. В свою очередь, субъект имеет право на доступ к персональным данным, относящимся к его личности, и получение сведений о наличии этих данных и самих данных. При наличии оснований, подтвержденных соответствующими документами, субъект персональных данных вправе требовать от держателя этих данных внесения в них изменений и дополнений. С другой стороны, субъект обязан сообщить держателю об изменении тех или иных персональных данных.
Конфиденциальность и сохранность персональных данных, их защита обеспечиваются

отнесением их к сфере негосударственной тайны — служебной или профессиональной тайне. Профессиональная тайна включает в себя врачебную, адвокатскую, банковскую, нотариальную тайну, тайну органов ЗАГС, предприятий связи, тайну исповеди и др.
Персональные данные накапливаются и используются, например: в налоговых инспекциях, правоохранительных органах, страховых агентствах, туристических и гостиничных фирмах, в некоторых подразделениях муниципальных органов самоуправления и т.д. Но наиболее концентрированное и обширное отражение персональные данные находят в разнообразной по составу и значительной по объемам кадровой документации (документации по личному составу), образующей соответствующую информационно-документационную систему, которая обеспечивает информацией функции управления персоналом и сопровождает реализацию правовых взаимоотношений граждан с государственными и негосударственными учреждениями, организациями, предприятиями и фирмами. Эта система имеет не только текущее, оперативное назначение в осуществлении кадровых функций, но и является одновременно ценным социологическим, биографическим и археографическим источником для исследования и обобщения сложных социальных процессов, протекающих в современной России.
В целях выявления состава конфиденциальных сведений и определения основных направлений защиты персональных данных в отделе кадров выделим две большие группы документации: а) документация по организации работы отдела и б) документация, образующаяся в процессе основной деятельности отдела и содержащая персональные данные в единичном или сводном виде.
Первая группа документации содержит организационно-правовую документацию отдела кадров и включает: положение об отделе, должностные инструкции работников отдела, приказы, распоряжения, указания руководства фирмы, регламентирующие структуру отдела и распределение сфер ответственности между его работниками, рабочие инструкции по выполнению основных функций отдела, ведению документации и формированию персональных данных в комплексы (документы, базы данных и т.п.). Сюда относятся также дела с документацией по планированию, учету, анализу и отчетности в части основной деятельности отдела. Учитывая значительное своеобразие в формировании статуса отдела и организации основных процессов, сопровождающих его деятельность в различных фирмах, конфиденциальный характер этой группы документации определяется тем, что злоумышленник может извлечь из анализа этой документации в конкретной фирме следующие полезные для себя сведения:
• распределение функций между отделом кадров и планово-финансовым отделом, бухгалтерией, юридическим отделом, военно-учетным столом и другими подразделениями, т.е. сведения от том, где искать требуемую информацию;
• распределение функций внутри отдела кадров между структурными единицами отдела (группами, секторами) и между работниками, т.е. сведения о том, у кого искать требуемую информацию;
• регламентацию рабочего процесса по оформлению документации, пропусков, удостоверений, т.е. сведения о том, как можно воспользоваться этим в несанкционированном режиме для фальсификации документов, баз данных;
• регламентацию места хранения документов, дел, баз данных, т.е. сведения о том, где и как можно украсть или подменить, тот или иной документ, получить требуемую информацию;
• регламентацию отчетной и справочной работы, т.е. сведения о том, когда и как можно перехватить требуемую информацию по организационным или техническим каналам.
Любые посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе кадров. Следует также учитывать, что работник отдела кадров не должен быть осведомлен о порядке работы других сотрудников этого отдела.
Вторая группа — документация, образующаяся в процессе основной деятельности отдела кадров и содержащая персональные данные, включает:
• комплексы документов, сопровождающие процесс оформления трудовых правоотношений гражданина (при решении вопросов о приеме на работу, переводе, увольнении и т.п.);
• комплексы материалов по анкетированию, тестированию, проведению собеседований с кандидатами на должность;
• подлинники и копии приказов по личному составу;
• личные дела и трудовые книжки сотрудников;

• дела, содержащие основания к приказам по личному составу;
• дела, содержащие материалы аттестации сотрудников, служебных расследований и т.п.;
• справочно-информационный банк данных по персоналу — учетно-справочный аппарат (картотеки, журналы, базы данных и др.);
• подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству предприятия, руководителям структурных подразделений и служб;
• копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения.
• Главным моментом в защите персональных и иных конфиденциальных данных является четкая регламентация функций работников отдела кадров и в соответствии с этим — регламентация принадлежности работникам документов, дел, карточек, журналов персонального учета и баз данных.
Для реализации этого положения руководитель фирмы должен издать приказ или распоряжение о закреплении за работниками отдела определенных массивов документов, необходимых им для информационного обеспечения функций, указанных в должностных инструкциях этих работников, утвердить схему доступа работников отдела кадров и руководящего состава фирмы, структурных подразделений к документам отдела, ввести личную ответственность перечисленных должностных лиц и работников за сохранность и конфиденциальность персональных данных.
По каждой функции, выполняемой работником отдела кадров, должен быть регламентирован состав документов, дел и баз данных, к которыми этот работник имеет право работать. Не допускается, чтобы работник мог знакомиться с любыми документами и материалами отдела. Целесообразно, в целях разграничения доступа и разбиения знания персональных данных между работниками, закрепить за разными работниками: а) документирование оформления трудовых правоотношений (приема, перевода, увольнения и др.), б) ведение личных дел и трудовых книжек, в) составление и хранение приказов по личному составу и контрактов, г) ведение справочно-информационного банка данных. Распределение сфер деятельности может варьироваться в зависимости от объема работы и штатной численности работников отдела, но разграничение обязанностей и массивов документации должно быть обязательно. Это позволит построить работу отдела в соответствии с указанными выше основополагающими принципами и обеспечить сохранность и конфиденциальность персональных данных. В случае необходимости перераспределения обязанностей среди работников отдела (например, при болезни одного из них, увольнении) должно быть издано соответствующее распоряжение начальника отдела кадров, в котором регламентируются характер изменений, их срок и дополнения в систему доступа к документам, делам и базам данных. Важно, что в этом распоряжении фиксируется изменение степени осведомленности работников в знании ими персональных данных и сферы личной ответственности за сохранность и конфиденциальность документации.
Работа с отдельными группами документации по кадрам имеет специфические особенности.
Операции по оформлению, формированию, ведению и хранению личных дел выполняются одним работником отдела кадров, который несет личную ответственность за сохранность документов в делах и доступ к делам других работников. Документы для формирования и ведения личных дел сдаются ему под роспись в передаточном журнале работником, отвечающим за процесс документирования трудовых правоотношений граждан с фирмой. Материалы, связанные с анкетированием, тестированием, проведением собеседований с кандидатами на должность, помещаются не в личное дело принятого сотрудника, а в специальное дело, имеющее гриф «Строго конфиденциально». Необходимость этого объясняется тем, что подобные материалы раскрывают личностные и моральные качества сотрудника и могут при разглашении содержащихся в них сведений стать полезными злоумышленнику в процессе поиска им канала несанкционированного доступа к ценной информации предприятия, для шантажа сотрудника и склонения его к сотрудничеству. Материалы с результатами тестирования работающих сотрудников, материалы их аттестаций формируются в другое дело, также имеющее гриф строгой конфиденциальности.
На личных делах гриф ограничения доступа не ставится, так как весь комплекс личных дел является конфиденциальным. Личное дело должно обязательно иметь опись

документов, включенных в дело. Листы дела нумеруются в процессе формирования дела. При помещении в личное дело нового документа данные о нем первоначально вносятся в опись дела, затем листы документа нумеруются и только после этого документ подшивается. На оборотной стороне обложки личного дела может указываться список руководителей, которым дело может быть выдано для ознакомления. Здесь же подклеивается конверт для карточки учета (контрольной карточки) выдачи дела.

Изменения и дополнения в персональные данные вносятся в дополнение к личному листку по учету кадров и (или) личную учетную карточку формы Т-2 на основании приказов по личному составу и документов, предоставляемых сотрудниками (свидетельства о браке, диплома и т.д.). Устное заявление сотрудника не является основанием для внесения указанных изменений (кроме второстепенных сведений — изменения номера домашнего телефона, места работы близких родственников и т.п.). Все новые записи в дополнении к личному листку по учету кадров и учетных формах заверяются росписью работника отдела кадров. При переносе сведений из приказа по личному составу работник расписывается против перенесенного пункта.

В случае изъятия из личного дела документа в описи дела производится запись с указанием основания для подобного действия и нового местонахождения документа. С документа, подлежащего изъятию, снимается копия, которая подшивается на место изъятого документа. Отметка в описи и копия заверяются росписью работника отдела кадров. Замена документов в личном деле любым лицом запрещается. Новые, исправленные документы помещаются вместе с ранее подшитыми.

Приказом первого руководителя фирмы должен быть установлен порядок выдачи или ознакомления руководящего состава с личными делами сотрудников. Личные дела могут выдаваться на рабочие места только первого руководителя, его заместителя по кадрам или персоналу и начальника отдела (управления) кадров Дела выдаются под роспись в контрольной карточке. При возврате дела тщательно проверяется сохранность документов, отсутствие повреждений, включения в дело других документов или подмены документов. Просмотр дела производится в присутствии руководителя. Передача личных дел руководителям через их секретарей или референтов не допускается. Другие руководители фирмы могут знакомиться с личными делами подчиненных им сотрудников. Ознакомление с делами осуществляется в помещении отдела кадров под наблюдением работника, ответственного за сохранность и ведение личных дел. Факт ознакомления фиксируется в контрольной карточке личного дела. Сотрудник фирмы имеет право знакомиться только со своими личным делом и трудовой книжкой, учетными карточками, отражающими его персональные данные. Факт ознакомления с личным делом также фиксируется в контрольной карточке.

В сферу ответственности работника, осуществляющего ведение личных дел, входит работа с трудовыми книжками сотрудников фирмы. Трудовые книжки всегда хранятся отдельно от личных дел. Особое внимание обращается на учет в бухгалтерии и отделе кадров чистых бланков книжек и бланков листов-вкладышей. Начальник отдела должен строго контролировать, чтобы подчиненные ему работники не оформляли трудовые книжки на неучтенных бланках (купленных и, как правило, поддельных). Под особым контролем должны находиться операции по проставлению в трудовых книжках печатей и штампов. Целесообразно, чтобы эти операции производил только начальник отдела кадров, так как в противном случае может возникнуть опасность несанкционированного использования печатей и штампов.

Не менее строгого контроля требует работа со справочно-информационным банком данных по персоналу фирмы (картотеками, журналами и книгами персонального учета сотрудников). Этот банк содержит основную, концентрированную массу ценных сведений о сотрудниках. Множество применяемых традиционных учетных форм осложняет обеспечение их конфиденциальности. Однако переход на автоматизированный тип этого банка создает другие сложности, связанные с необходимостью ведения комплексов страховых и резервных машиночитаемых и бумажных копий, включенных в банк учетных форм. Конфиденциальными при любом типе банка являются накопительные ведомости, записи в промежуточных рабочих формах, которые ведутся работником отдела кадров для последующего одноразового внесения в учетные формы. Доступ работников отдела к справочно-информационному банку данных должен быть ограничен и определяться их служебными обязанностями. Разовое ознакомление с учетной карточкой какого-либо сотрудника разрешает начальник отдела кадров.

Отчетная и справочная работа отдела формирует каналы объективного санкционированного распространения персональных данных и может служить основой формирования канала несанкционированного получения и незаконного использования ценных сведений. В этой связи требуется повышенное внимание к обеспечению сохранности и конфиденциальности отчетных и справочных массивов информации. Первым руководителем фирмы должен быть регламентирован порядок получения нижестоящими руководителями необходимых им для работы справочных данных. Устанавливается: кто, когда, какие сведения и с какой целью может запрашивать в отделе кадров. И, что особенно важно, определяется порядок дальнейшего хранения сведений, работа с которыми закончена: где эти сведения будут находиться, кто несет ответственность за их сохранность и конфиденциальность.

Передаваемые из отдела кадров руководителям отчетные и справочные сведения обязательно документируются в виде сводок, списков, справок и т.п. Устное сообщение сведений, как правило, использоваться не должно, за исключением случаев, когда запрашивается единичная информация, например: дата рождения сотрудника, название вуза и т.п. На документах, выходящих за пределы отдела кадров, может ставиться гриф «Конфиденциально» или «Для служебного пользования». В отделе кадров обязательно остаются копии всех отчетных и справочных документов. Целесообразно, чтобы после использования подлинники этих документов возвращались в отдел кадров для включения в дело вместо хранящейся там копии.

В структурных подразделениях предприятия могут быть следующие документы, содержащие персональные данные: журнал табельного учета с указанием должностей, фамилий и инициалов сотрудников (находится у работника, ведущего табельный учет — табельщика), штатное расписание (штатный формуляр) подразделения, в котором могут дополнительно указываться, кто из сотрудников занимает ту или иную должность, каковы вакантные должности (находится у руководителя подразделения), дело С выписками из приказов по личному составу, касающихся персонала подразделения (находится у табельщика). Руководитель подразделения может иметь список сотрудников с указанием основных биографических данных каждого из них (год рождения, образование, местожительство, номер домашнего телефона и др.). Все перечисленные документы следует хранить в соответствующих делах, включенных в номенклатуру дел и имеющих гриф ограничения доступа. Не реже одного раза в год работники отдела кадров проверяют наличие этих дел в подразделениях и правильность их ведения.

В отделе кадров дела, картотеки, учетные журналы и книги учета хранятся в рабочее и нерабочее время в металлических запирающихся шкафах. Работникам не разрешается при любом по продолжительности выходе из помещения оставлять какие-либо документы на рабочем столе или оставлять шкафы незапертыми. У каждого работника должен быть свой шкаф для хранения закрепленных за ним дел и картотек. Трудовые книжки всегда хранятся в сейфе.

На рабочем столе работника должен всегда находиться только тот массив документов и учетных карточек, с которым он в настоящий момент работает. Исполняемые документы следует помещать в папки, на которых указывается вид производимых с ними действий (для подшивки в личные дела, для отправки и т.п.) или фамилии граждан, к работе с которыми относятся данные документы. Каждая папка должна иметь опись находящихся в ней документов. Документы, с которыми закончена работа, немедленно подшиваются в соответствующее дело. Карточки в процессе работы с ними хранятся в промежуточной рабочей картотеке, а после окончания работы помещаются в основные картотеки.

В конце рабочего дня все документы, дела, листы бумаги и блокноты с рабочими записями, инструктивные и справочные материалы должны быть убраны в металлические шкафы, сейфы, которые запираются и опечатываются печатью данного работника, Ключи от шкафов сдаются начальнику отдела кадров под роспись в соответствующем журнале. На рабочем столе не должно оставаться ни одного документа. Следует также проверить урну для бумаг и убедиться в отсутствии там листов бумаги, которые могут представлять интерес для постороннего лица. Печати, штампы, бланки документов, ключи от рабочих шкафов хранятся только в сейфе начальника отела кадров. Черновики и редакции документов, испорченные бланки, листы со служебными записями в конце рабочего дня уничтожаются в специальной бумагорезальной машине двумя работниками отдела.

Помимо операций с документами работники отдела кадров значительную часть времени

тратят на прием посетителей. Этот вид работы также должен быть строго регламентирован, так как посетители могут представлять определенную угрозу информационным ресурсам отдела кадров и безопасности работников отдела.
Важно, чтобы прием посетителей осуществлялся только в те часы, которые ежедневно выделяются для этой цели. В другое время в помещении отдела кадров не могут находиться посторонние лица, в том числе сотрудники фирмы.
В часы приема посетителей работники отдела не должны выполнять функции, не связанные с приемом, вести служебные и личные переговоры по телефону. На столе работника, ведущего прием, не должно быть никаких документов, кроме тех, которые касаются данного посетителя. В помещении отдела кадров в часы приема посторонних лиц может находиться работник службы безопасности фирмы. Целесообразно также наличие сигнализации, оповещающей сотрудников этой службы о необходимости немедленно вмешаться в сложившуюся ситуацию. На столе работника отдела не должно быть тяжелых предметов.
Прием посетителей чаще всего связан с ведением справочной работы: ответов на вопросы посетителей и выдачей им справок. Ответы на вопросы даются только лично тому лицу, которого они касаются. Не допускается передача персональной информации по телефону. Ответы на письменные запросы других учреждений, фирм и, организаций даются в письменной форме, на бланке фирмы или отдела кадров и в том объеме, который позволяет не разглашать излишний объем персональных сведений.
При выдаче справки с места работы необходимо удостовериться в личности сотрудника, которому эта справка выдается. Не разрешается выдавать ее родственникам или сослуживцам лица, которому требуется справка. Справка выдается на основании учетной карточки Т-2, а не пропуска, так как сотрудник при увольнении мог не сдать пропуск или удостоверение. Справку подписывает начальник отдела кадров. На подпись справку передает работник отдела, а не посетитель. Одновременно начальник отдела ставит на справке печать. За получение справки сотрудник предприятия расписывается в журнале учета выдачи справок.
Чистые бланки справок подлежат обязательному учету. Они хранятся у начальника отдела кадров и выдаются в дневной норме работнику, выдающему справки. По окончании приемных часов этот работник отчитывается перед начальником отдела об израсходованных бланках справок и сдает ему оставшиеся чистыми и испорченные бланки. Заранее ставить на чистых бланках справок подпись начальника отдела и печать не допускается.
В целях удобного доступа посетителей в отдел кадров помещения отдела должны располагаться на первом этаже здания, поблизости от входа. В часы приема лиц, не являющихся сотрудниками предприятия, вход в отдел должен быть свободным для всех желающих. Проход посторонних лиц в помещение отдела контролируется сотрудником службы безопасности: посетитель идентифицируется по паспорту или служебному удостоверению, при необходимости посетителя провожают. Не допускается бесконтрольное нахождение посторонних лиц в здании фирмы.
Отдел кадров должен иметь три смежных помещения: комнату для работников отдела, кабинет начальника отдела и помещение, в котором размещаются шкафы и сейфы для документов, дел и картотек. Вход в отел кадров может быть только один. Для ожидающих приема посетителей целесообразно выделить дополнительное помещение за пределами основных помещений отдела. Помещение для размещения шкафов может не иметь окон и оборудуется эффективными техническими средствами пожаротушения. Все помещения оборудуются охранной сигнализацией.
Сдачу на охрану и снятие с охраны помещений отдела кадров осуществляет начальник отдела или его заместитель. Уборка помещений допускается только в присутствии этих лиц. Мусор, выносимый из помещений, должен сжигаться.
Подбор персонала для работы в отделе кадров ведется с учетом требований, которые разработаны для должностей, связанных с владением и обработкой конфиденциальных сведений и документов.
Следовательно, работа отдела кадров любой фирмы связана с обработкой значительных объемов персональных сведений (данных), отражающих профессиональные, деловые и личные качества сотрудников и являющихся конфиденциальными. Конфиденциальность определяется тем, что эти сведения составляют личную или семейную тайну граждан и подлежат защите в соответствии с законом. Функционирование отдела кадров должно

быть подчинено решению задач обеспечения безопасности персональных сведений, их защиты от множества видов угроз, которые может создать злоумышленник, чтобы завладеть этими сведениями и использовать их в противоправных целях.

10.4. Нормативно-методические документы по обеспечению безопасности информации

Нормативно-методическое обеспечение системы защиты конфиденциальной информации предназначено для регламентации процессов обеспечения безопасности информации фирмы, в том числе при работе персонала с конфиденциальными сведениями, документами, делами и базами данных. Оно включает в себя ряд обязательных организационных, инструктивных и информационных документов, устанавливающих принципы, требования и способы предотвращения пассивных и активных угроз ценной информации, которые могут возникнуть по вине персонала, конкурентов, злоумышленников и других лиц.

Нормативно-методическое обеспечение базируется на тех обязательных положениях, которые должны содержаться в учредительных и иных основополагающих документах фирмы и определять правовой статус информационной безопасности фирмы. Указанные положения позволяют на законных основаниях вести речь о сохранении коммерческой тайны, выделять ценную информацию, составляющую собственность и тайну фирмы, и выполнять действия по ее защите. Предмет и направления защиты должны найти отражение, например, в уставе фирмы, типовых формах контрактов различного рода и назначения, положениях о структурных подразделениях фирмы, должностных инструкциях сотрудников и других документах.

Важнейшими организационными документами, фиксирующими задачи, функции и ответственность служб, осуществляющих защиту ценной документированной информации фирмы, являются: положение о службе безопасности, положение о службе конфиденциальной документации, должностные инструкции сотрудников этих служб, должностная инструкция менеджера (референта) по безопасности небольшой предпринимательской фирмы и другие документы.

Технологические инструктивные документы отличаются большим разнообразием и по своему назначению, составу и содержанию отражают избранную фирмой систему защиты документированной информации. Можно выделить основные, на наш взгляд, регламентирующие документы, имеющие значение для любой фирмы и необходимые при использовании любой системы защиты информации или отдельных элементов такой системы:

1. Перечень сведений предпринимательской фирмы, составляющих ее тайну или являющихся особо ценными. Содержание перечня обычно делится на несколько частей: общую методическую часть по способам составления перечня и правилам работы с ним, списки конфиденциальных сведений по структурным подразделениям или управленческим функциям фирмы, список видов конфиденциальных документов и баз данных с указанием места их хранения, срока конфиденциальности и т.п.
2. Инструкция по обеспечению безопасности конфиденциальной информации фирмы, которая регламентирует:

• обязанности сотрудников фирмы при работе с конфиденциальной информацией;
• порядок доступа сотрудников к конфиденциальным документам и базам данных, оформление доступа;
• обеспечение сохранности документов на бумажных и магнитных носителях при работе с ними руководителей, исполнителей (специалистов) и технического персонала;
• порядок сохранения тайны фирмы при проведении совещаний, заседаний и переговоров;
• требования к помещениям для работы с конфиденциальной информацией;
• порядок охраны территории, здания, помещений, транспортных средств и персонала фирмы;
• пропускной режим помещений фирмы, учет и порядок выдачи удостоверений, пропусков и визуальных идентификаторов;
• порядок приема, учета и контроля деятельности посетителей;
• требования к защите информации в рекламной и выставочной работе, публикациях, при интервьюировании и собеседованиях;
• организационное обеспечение защиты информации в ПЭВМ и линиях связи, при использовании в обработке документов средств организационной техники;
• ответственность сотрудников фирмы за разглашение конфиденциальной информации и утрату ценных документов.

3. Инструкция по обработке, хранению и движению конфиденциальных документов фирмы. Она регламентирует организацию работы сотрудников службы КД, менеджера (референта) по безопасности, управляющего делами фирмы, секретаря-референта первого руководителя.

Основные разделы Инструкции:

• структура защищенного документооборота фирмы;
• установление, изменение и снятие грифа конфиденциальности документов;
• порядок составления, учета, изготовления и издания конфиденциальных документов;
• копирование и размножение документов;
• прием и распределение поступивших документов;
• учет (регистрация) поступивших документов;
• отправка и рассылка документов;
• порядок передачи документов в процессе их рассмотрения и исполнения;
• контроль исполнения документов;
• порядок систематизации документов и формирования дел;
• порядок передачи документов и дел в архив фирмы, уничтожения документов и дел с истекшим сроком хранения;
• оперативное (текущее) и архивное хранение дел;
• проверка наличия документов, дел, баз данных и носителей конфиденциальной информации;
• правила хранения и использования бланков документов, печатей и штампов.

В приложении к инструкции даются учетные и иные технологические формы, необходимые для организации обработки, хранения и движения документов.

Информационные (методические, советующие, обучающие) документы (правила, требования, указания, методики, памятки и т.п.), детализирующие процессы защиты информации, носят, вместе с тем, обязательный характер и устанавливают порядок работы с конфиденциальной информацией и документами отдельных категорий сотрудников фирмы или всех сотрудников в конкретных типовых ситуациях. При необходимости они могут составляться по каждому отдельному сотруднику.

Прежде всего следует выделить Правила работы руководителей и исполнителей (специалистов) предпринимательской фирмы с конфиденциальными документами и базами данных. Правила регламентируют:

• порядок распределения документов между руководителями и исполнителями в соответствии с действующей системой доступа персонала к конфиденциальной информации;
• рассмотрение документов руководителем и адресования их исполнителям;
• порядок передачи и получения документов исполнителями;
• ознакомление исполнителей с содержанием документов и решением по ним руководителя;
• составление и изготовление документов исполнителями;
• работу руководителя с подготовленными документами;
• порядок хранения документов, дел, носителей информации, чистых бланков документов и штампов на рабочем месте руководителя и исполнителя;
• проверку наличия конфиденциальных документов и баз данных на рабочем месте руководителя и исполнителя;
• порядок ведения телефонных переговоров, факсимильной переписки;
• особенности работы с ПЭВМ при обработке конфиденциальной информации, правила работы с копировальной техникой;
• порядок работы с конфиденциальными документами за пределами фирмы, в командировках, транспорте, порядок хранения документов;
• обеспечение сохранности документов и баз данных во внерабочее время.

Правила работы менеджера по безопасности (управляющего Делами, референта, секретаря-референта) фирмы с конфиденциальными документами и базами данных регламентируют:

• порядок приема и отправки конфиденциальных документов;
• порядок учета (регистрации) поступивших документов;
• организацию доступа исполнителей к конфиденциальным документам;
• распределение документов по руководителям и исполнителям, ознакомление с документами исполнителей и передача документов на исполнение;

• формирование и ведение справочно-информационного банка данных по конфиденциальным документам;
• контроль исполнения документов;
• учет и изготовление документов на пишущих устройствах;
• оформление и ведение номенклатуры дел фирмы;
• формирование и хранение (текущее и архивное) дел фирмы;
• порядок организации приема руководителем посетителей, методы обеспечения безопасности руководителя;
• защиту информации при ведении телефонных переговоров и передаче информации по факсимильной связи;
• защиту информации при работе с ПЭВМ;
• построение систем охраны кабинета руководителя, приемной, сейфов, шкафов с документацией, вычислительной и организационной техники в рабочее и нерабочее время;
• ответственность за нарушение правил работы с конфиденциальной документацией и базами данных. Правила работы менеджера по персоналу предпринимательской фирмы регламентируют:
• обязанности менеджера в области защиты информации и работы с сотрудниками, обладающими секретами фирмы;
• организацию и документирование приема сотрудников на работу;
• обязательства сотрудников по сохранению тайны фирмы;
• контроль соблюдения персоналом правил работы с конфиденциальными документами и информацией;
• организацию и документирование переводов сотрудников на другие должности и изменения условий контрактов;
• порядок формирования и ведения личных дел сотрудников;
• порядок оформления и ведения трудовых книжек сотрудников;
• порядок ведения справочно-информационного банка данных по персоналу фирмы;
• правила и методы защиты персональных данных;
• организацию и документирование увольнений сотрудников;
• порядок оформления доступа сотрудников к конфиденциальным сведениям, документам и базам данных;
• принципы и направления формирования нормального психологического климата в коллективе, воспитания фирменной гордости персонала;
• психологический анализ сотрудников, тестирование, анкетирование, инструктирование и обучение персонала;
• правила хранения документов и работы с ними;
• организацию охраны помещения службы персонала в рабочее и нерабочее время;
• ответственность менеджера по персоналу за разглашение персональных данных о сотрудниках фирмы и другой конфиденциальной информации.
Информационные документы регламентируют также требования по единообразному выполнению персоналом определенных видов типовых действий. Так, правила обеспечения безопасности секретов фирмы и конфиденциальной информации в экстремальных ситуациях включают в себя классифицированный перечень экстремальных ситуаций и соответствующих мероприятий по защите секретов фирмы, информации и документов и регламентируют:
• порядок (при необходимости — план) эвакуации и охраны документов, дел и баз данных;
• порядок (при необходимости — план) эвакуации и оказания помощи персоналу;
• порядок охраны имущества фирмы, оборудования и технических средств защиты информации;
• порядок охраны персонала при индивидуальных экстремальных ситуациях (угрозах, шантаже, нападении и т.п.);
• порядок взаимодействия с правоохранительными органами
при возникновении экстремальных ситуаций. Рассмотренные нормативно-методические документы отражают действующую в фирме систему защиты информации и потому являются строго конфиденциальными. После их утверждения первым руководителем фирмы они доводятся в выборочном порядке до сведения всех сотрудников фирмы под роспись. Одновременно могут быть внесены необходимые изменения и дополнения в должностные

инструкции сотрудников. При внесении обязательных периодических изменений в систему обеспечения безопасности фирмы соответствующим образом своевременно корректируется нормативно-методическая документация. Контроль за соблюдением сотрудниками фирмы изложенных в документах требований возлагается на службы: безопасности, конфиденциальной документации, персонала, а в некрупных фирмах — на менеджера по безопасности.

Следовательно, система защиты ценной, конфиденциальной информации предпринимательской фирмы реализуется в комплексе нормативно-методических документов, которые детализируют и доводят ее в виде конкретных рабочих требований до каждого работника фирмы. Знание работниками своих обязанностей по защите секретов фирмы является обязательным условием эффективности функционирования системы защиты и определенной гарантией сохранности собственной информации фирмы.

11. СТРУКТУРИРОВАННЫЙ МАТЕРИАЛ ДЛЯ УГЛУБЛЕННОЙ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ПО ПРОБЛЕМАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОФИСНОЙ ДЕЯТЕЛЬНОСТИ

Словарь-справочник терминов

А

Аналитическая работа — комплексное исследование различной целевой направленности, предназначенное для выявления, структуризации и изучения опасных объективных и субъективных, потенциальных и реальных ситуаций, которые могут создать риск для экономической безопасности фирмы, ее деятельности или персонала, привести к материальным, финансовым или иным убыткам, падению престижа фирмы или ее продукции. Аналитическая работа ведется службой безопасности или информационно-аналитической службой фирмы, носит превентивный, информационный характер и использует в качестве инструмента учетный аппарат, предназначенный для фиксирования (протоколирования) необходимых для анализа сведений. Результаты аналитической работы показывают степень безопасности интеллектуальной собственности, условий функционирования фирмы и являются основой для построения и совершенствования системы защиты традиционных и электронных конфиденциальных информационных ресурсов фирмы, формирования рубежей охраны территории, здания, помещений, оборудования, продукции и персонала фирмы.

Аналитическая работа по выявлению каналов несанкционированного доступа к конфиденциальной информации — прогнозирование и выявление на основе комплексного исследования сложившихся или предполагаемых ситуаций состава и особенностей образования каналов несанкционированного доступа к конфиденциальной информации конкретной фирмы в единстве с изучением характера возможных угроз ее информационной безопасности. Исследование проводится в целях выработки методов защиты, пассивного и активного противодействия злоумышленнику, который тайно находит или формирует и использует каналы несанкционированного доступа (НСД) к информации, получения (добывания) ценных для него сведений. В основе исследования фирмой возможных каналов НСД лежит классификация, учет и: изучение источников конфиденциальной информации фирмы, каналов естественного, объективного распространения этой информации, источников угрозы конфиденциальной информации и контроль эффективности системы защиты информации. Другие методы носят случайный характер ожидания ошибки в тайных действиях злоумышленника. На основе результатов аналитической работы определяются, учитываются и контролируются организационные и технические каналы НСД, вырабатываются меры предотвращения образования этих каналов, разрабатывается и систематически модифицируется система защиты информации фирмы, определяется ее структура и стоимость в соответствии с реальными опасностями, угрожающими ценной информации, ведется оценка надежности этой системы.

Аналитическая работа с источником конфиденциальной информации — комплексное исследование максимального числа источников, владеющих или содержащих конфиденциальные сведения. Предусматривает: выявление и классификацию источников конфиденциальной информации, изучение реального классифицированного состава циркулирующей конфиденциальной информации фирмы с указанием источников, обеспечиваемых функций и видов работы; изучение данных учета осведомленности сотрудников в тайне фирмы в разрезе каждого руководителя и сотрудника (в том числе технического), т.е. изучение степени и динамики реального владения персонала

конфиденциальной информацией; изучение состава конфиденциальной информации в разрезе документов, т.е. изучение правильности расчленения тайны (конфиденциальной информации) между документами и определение избыточности ценной информации в документах; изучение выявленных угроз каждому отдельному источнику конфиденциальной информации; определение степени эффективности методов защиты информации, предпринятых по каждому источнику, и методов защиты, которые могут быть дополнительно использованы при активных действиях злоумышленника. При этом учитывается, что персонал является главным источником и виновником утраты конфиденциальной информации. Обязательному учету подлежат все санкционированные и несанкционированные обращения сотрудников к конфиденциальной информации, документам и базам данных.

Аналитическая работа с источником угрозы конфиденциальной информации — комплексное исследование максимального числа объектов и субъектов, представляющих опасность для информационной безопасности фирмы. Предусматривает выявление и классификацию источников угрозы конфиденциальной информации, разработку мероприятий по локализации и ликвидации объективных угроз, изучение каждого отдельного субъективного внутреннего и внешнего источника угрозы конфиденциальной информации, учет направленности интересов каждого источника, степени его опасности (анализ риска) при реализации угрозы. В области внешних источников угрозы аналитическая работа связана с маркетинговыми исследованиями, которые регулярно ведет любая фирма. Анализ внутренних источников угрозы имеет целью выявление и изучение недобросовестных интересов и злоумышленных устремлений отдельных сотрудников фирмы и партнеров. В процессе анализа источников выявляются факты получения злоумышленником секретов фирмы, факты сотрудничества персонала фирмы с конкурентами или наличия в составе сотрудников фирмы злоумышленника.

Аналитическая работа с каналом объективного распространения конфиденциальной информации — комплексное исследование максимального числа коммуникативных каналов, по которым перемещаются конфиденциальные сведения в санкционированном режиме. Предусматривает: выявление и изучение реального классифицированного состава каналов объективного распространения конфиденциальной информации фирмы; изучение составных элементов каждого канала с целью нахождения опасных участков, способствующих возникновению канала несанкционированного доступа к информации, изучение состава ценной информации, циркулирующей в каждом канале; изучение состава ценной информации, циркулирующей между источниками; изучение распространения информации при коммуникативных связях; изучение методов защиты, предпринятых по каждому каналу, дополнительных мер противодействия злоумышленнику при активных угрозах и к экстремальных ситуациях. Информация должна поступать к конкуренту только по контролируемому каналу.

Аутентификация — проверка подлинности документов, информации, передаваемых по запросу пользователей или иных лиц.

Б

Безопасность — защищенность жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, состояние, при котором чему-либо или кому-либо не угрожает опасность.

Безопасность информационная — составная часть экономической безопасности предпринимательской деятельности. Включает в себя: а) комплексную программу (концепцию) обеспечения безопасности информационных ресурсов, отражающую актуальные задачи в этой области, и б) целесообразную в настоящий момент технологическую систему защиты информации, обеспечивающую необходимый уровень безопасности информационных ресурсов фирмы. Предполагает: наличие программы безопасности информационных ресурсов и аналитических исследований, систематической работы по определению и эволюции состава ценной, конфиденциальной информации, разработку организационных, распорядительных, нормативных и инструктивных документов, регламентирующих порядок реализации программы и систему защиты информации фирмы в части защиты информации в традиционном и электронном документообороте, защиты информации в компьютерах, сетях, линиях связи, защиты документированной информации от ошибочных и злоумышленных действий персонала, организации разрешительной системы доступа персонала к информации, защиты информации при ведении деловых переговоров, в рекламной и выставочной работе, защиты технических каналов распространения

информации.

Безопасность информационных ресурсов (информации) — защищенность информации во времени и пространстве от любых объективных и субъективных угроз (опасностей), возникающих в обычных условиях функционирования фирмы и условиях экстремальных ситуаций. Безопасность ценной документированной информации (документов) определяется уровнем ее защищенности от стихийных бедствий, других неуправляемых событий, пассивных и активных попыток злоумышленника создать потенциальную или реальную угрозу несанкционированного доступа к документам, делам, базам данных, а также опасностей неправомерного использования кем-либо ценных сведений, нарушения их сохранности, целостности и конфиденциальности. Безопасность предполагает также защищенность конфиденциальной информации в информационных системах от случайных и преднамеренных воздействий естественного и искусственного свойства, направленных на изменение степени доступности ценных сведений в машинной и внемашинной сферах. Без учета требований по внемашинной защите конфиденциальной информации на магнитных, бумажных и иных носителях (что несущественно для автоматизированной обработки открытой информации) уязвимость информации резко возрастает и гарантировать в этих условиях безопасность информационных ресурсов, коммерческой (предпринимательской) тайны становится невозможно.

Безопасность маркетинговая — составная часть экономической безопасности предпринимательской деятельности. Предполагает: наличие аналитических исследований деловых интересов добросовестных конкурентов и партнеров, конъюнктуры рынка продукции, анализ направленности интересов недобросовестных конкурентов, злоумышленников, организацию разведки в бизнесе, аналитическую работу по выявлению ситуаций, опасных для деятельности фирмы.

Безопасность правовая — составная часть экономической безопасности предпринимательской деятельности. Предполагает наличие: правовой грамотности учредителей и персонала, документов, решений и организации деловых отношений, процессуальной защиты интересов предпринимателя, лицензирование деятельности, правовое обеспечение защиты коммерческой (предпринимательской) тайны, технических и технологических новшеств (ноу-хау).

Безопасность физическая — составная часть экономической безопасности предпринимательской деятельности. Предполагает: наличие обученного персонала охраны, эффективной инженерной системы охраны территории, здания, помещений, транспорта, оборудования, продукции, персонала фирмы, наличие технических средств охраны, сигнализирования и оповещения о нарушении системы охраны, наличие установленного взаимодействия службы охраны с правоохранительными органами, регламентацию действий персонала в экстремальных ситуациях, организацию службы телохранителей, охраны инкассации, наличие эффективных средств пожаротушения.

Безопасность экономическая — всесторонняя защищенность предпринимательской деятельности, деловых интересов каждого творческого коллектива, предприятия, фирмы и предпринимателя в большом и малом бизнесе во времени и пространстве. Является обязательным условием успеха в бизнесе, получения прибыли и сохранения в целостности предпринимательской организационной структуры. Экономическая безопасность предпринимательской деятельности включает в себя составные части: правовую, маркетинговую, информационную и физическую безопасность.

Бланк документа — набор реквизитов, идентифицирующих автора официального письменного документа.

В

Видеограмма — изображение электронного документа на экране дисплея. В полном смысле слова документом не является, представляет собой заверенную или незаверенную копию документа (как и факсограмма).

Владелец информационных ресурсов — субъект, осуществляющий владение и пользование указанным объектом и реализующий полномочия распоряжения в пределах, установленных законом и собственником информационных ресурсов.

Выделение документов к уничтожению — выявление в процессе экспертизы научной и практической ценности документов с истекшими сроками хранения, утративших практическое, научное или общественное значение, и отбор их к уничтожению.

Выделенное помещение — рабочая комната или иное изолированное и охраняемое помещение, предназначенное для работы (исполнения, обработки, хранения) с

традиционными (бумажными) и электронными документами, компьютерными базами конфиденциальных данных, изготовления и хранения изделий ограниченного доступа, проведения конфиденциальных совещаний, переговоров и заседаний. Подобные помещения, именуемые режимными, характеризуются; четкой разрешительной регламентацией и контролем доступа персонала в помещение, наличием постоянной охраны помещения и пропускного режима входа и выхода, контролем вносимых и выносимых предметов, в том числе личных вещей персонала, строгими правилами работы персонала с конфиденциальными документами, перекрытием всех потенциальных технических каналов утечки информации, автономной системой связи и энергоснабжения и другими особенностями.

Г

Гриф конфиденциальности — см. Гриф ограничения доступа к документу.

Гриф ограничения доступа к документу — реквизит (элемент, служебная отметка, помета, пометка) формуляра документа, свидетельствующий о конфиденциальности сведений, содержащихся в документе, проставляемый на самом документе и (или) сопроводительном письме к нему, называется часто грифом конфиденциальности. Гриф ограничения доступа обозначается в соответствии с ГОСТ Р 6.30-97 и имеет несколько уровней, отражающих степень конфиденциальности защищаемых сведений, относимых к коммерческой (предпринимательской) тайне. Массовый уровень — грифы «Конфиденциально», «Конфиденциальная информация». Второй уровень, достаточно редкий — грифы «Строго конфиденциально», «Строго конфиденциальная информация», «Конфиденциально. Особый контроль». Не следует ставить гриф «Коммерческая тайна», так как грифом обозначается не вид тайны, а характер ограничения доступа к документу. Под грифом указывается номер экземпляра документа, срок действия фифа или иные условия его снятия, изменения. Может ставиться помета «Лично». На документах, содержащих сведения, отнесенные к служебной тайне, ставится гриф «Для служебного пользования» с указанием номера экземпляра документа. На электронных документах указанные грифы обозначаются на всех листах. На документах, содержание которых отнесено к профессиональной тайне, а также на документации службы персонала гриф конфиденциальности, как правило, не ставится, так как весь массив указанных документов является конфиденциальным. На ценных, но не конфиденциальных документах целесообразно проставлять отметку (надпись, штамп), предполагающую особое внимание к сохранности таких документов (например: «Собственная информация фирмы», «Информация особого внимания», «Хранить в сейфе» и др.). Гриф конфиденциальности присваивается документу: исполнителем при подготовке к составлению проекта документа; руководителем структурного подразделения (или направления деятельности фирмы) или руководителем фирмы при согласовании или подписании документа; работником службы конфиденциальной документации при первичной обработке поступивших документов, если конфиденциальный для фирмы документ не имеет грифа ограничения доступа. Изменение или снятие грифа конфиденциальности документа производится при изменении степени конфиденциальности (ценности) содержащихся в нем сведений.

Д

Действия персонала в экстремальных ситуациях — система устойчивых и заблаговременно выработанных стереотипов (мотиваций) поведения персонала фирмы при возникновении опасности возникновения конкретного типа экстремальной ситуации. Разработка системы возлагается на службу безопасности фирмы. Система предусматривает классификацию экстремальных ситуаций для конкретной фирмы, систематическое обучение должностных групп персонала правилам поведения в том или ином случае, разработку схемы оповещения персонала об опасности (стихийном бедствии, возгорании, задымлении, возможности взрыва, нападении на фирму и т.п.) и вступлении в действие плана эвакуации документов, дел, ценного оборудования, уничтожения ценных и конфиденциальных баз данных, разработку схемы оповещения правоохранительных и противопожарных органов и служб, схемы эвакуации персонала в безопасную зону. Обучение персонала должно основываться на изучении нормативных и плановых документов, решении ситуационных задач и проведении регулярных деловых игр. Большое значение имеет не только наличие и постоянное обновление нормативных и плановых документов и схем, но и материальное обеспечение действий персонала — наличие запирающейся тары для упаковки и переноса ценных документов, дел, магнитных носителей, технически исправных тележек, автотранспорта и т.п. Следует

предусмотреть формирование групп сотрудников для оказания помощи сотрудникам фирмы и службам экстремальной помощи, а также организацию охраны здания, помещений, оборудования и эвакуированных документов и дел, персонала. Кроме того, система должна обязательно включать обучение сотрудников правилам поведения при возникновении индивидуальной опасности.

Дело — совокупность документов или документ, относящиеся к одному вопросу или участку деятельности, помещенные в отдельную обложку.

Делопроизводство, документационное обеспечение управления — отрасль деятельности, обеспечивающая документирование и организацию работы с официальными документами.

Делопроизводство конфиденциальное — традиционная технологическая система обработки и хранения конфиденциальных документов, основанная на использовании ручных методов работы с документами. Трудоемкость множества технических и формально-логических процедур и операций обычно снижается за счет включения в технологический процесс организационной и вычислительной техники. Система является универсальной. Она надежно, долговременно обеспечивает защиту документированной информации как в обычных, так и в экстремальных ситуациях. В связи с этим технологические стадии защищенного документопотока в большинстве случаев реализуются методами и средствами именно традиционной системы обработки и хранения документов. Система одинаково эффективно оперирует как традиционными (бумажными), так и документами машиночитаемыми, факсимильными и электронными. Помимо документационного обеспечения управленческой и производственной деятельности конфиденциальное делопроизводство решает другую, не менее важную задачу — обеспечение сохранности носителя и конфиденциальности информации. Эта задача выполняется за счет: автономности функционирования указанной технологической системы, ее изолированности от аналогичных систем, связанных с обработкой других, в том числе открытых документов; операционного учета всех технологических действий, производимых с документом или чистым носителем информации; учета и обеспечения сохранности не только документов, но и учетных форм; персональной ответственности сотрудников за сохранность документа и тайну информации; наличия разрешительной системы доступа к документам; постоянного контроля за наличием, комплектностью и правильностью использования документов. Ведение конфиденциального делопроизводства централизуется в самостоятельном подразделении фирмы — службе конфиденциальной документации или в некрупных фирмах возлагается на управляющего делами, менеджера по безопасности или секретаря-референта (референта) первого руководителя.

Документ, документированная информация — зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

Документ аудиовизуальный - документ, содержащий изобразительную и звуковую информацию.

Документ беловой — рукописный или машинописный документ, текст которого переписан с чернового документа или написан без помарок и исправлений. При автоматизированном изготовлении документов беловиком является машинограмма (твердая копия) или машиночитаемый документ, но не видеограмма.

Документ внутренний — подготовленный документ, не выходящий за пределы подготовившей его организации.

Документ входящий (входной) — документ, поступивший в организацию.

Документ выделенного хранения — ценный документ, изъятый по какой-то причине из дела, оформленный в самостоятельное дело и переведенный на инвентарный вид учета (см. Учет конфиденциальных документов), например документ более ограниченного доступа, чем другие документы дела.

Документ дублетный — один из экземпляров копии документа.

Документ изобразительный — документ, содержащий информацию, выраженную посредством изображения какого-либо объекта.

Документ исходящий (выходной) — подготовленный документ, отправляемый из организации.

Документ конфиденциальный — документ ограниченного доступа, на любом носителе, содержащий информацию, отражающую приоритетные достижения в сфере экономической, производственной, предпринимательской, управленческой и другой деятельности, а также информацию, состав которой является принадлежностью служебной деятельности. Утрата конфиденциального документа может нанести ущерб интересам или деловому

успеху собственника или владельца информации. Под конфиденциальным (закрытым) документом понимается необходимым образом оформленный носитель документированной информации, содержащий сведения, которые относятся к негосударственной тайне, составляют интеллектуальную собственность юридического или физического лица и подлежат защите. Называть конфиденциальные документы секретными или ставить на них гриф секретности не допускается. Особенностью конфиденциального документа является то, что он представляет собой одновременно: массовый постель ценной, защищаемой информации; основной источник накопления и распространения этой информации, в том числе ее разглашения, утечки; обязательный объект защиты.

Документ машиночитаемый — официальный документ, созданный для обеспечения работы вычислительной техники. Например, документы на машиночитаемых носителях, машиночитаемые зоны на бумажных документах и др.

Документ официальный — документ, созданный юридическим или физическим лицом, оформленный и удостоверенный в установленном порядке.

Документ персональный — документ, содержащий персональные данные о гражданине, отражающие в том числе его личную или семейную тайную. Комплекс персональных документов служит инициативным условием возможности установления, изменения или прекращения трудовых правоотношений гражданина с учреждением или фирмой. Однако факт их выдачи или наличия сам по себе эти отношения не устанавливает. Комплекс включает в себя:

• документы, выдаваемые гражданам соответствующими государственными органами, организациями и юридически подтверждающие те сведения, которые граждане сообщают о себе, об образовании, семейном положении и т.д. (паспорт, трудовая книжка, военный билет, диплом, свидетельство, листок нетрудоспособности и др.);

• документы, выдаваемые рабочим и служащим организацией или фирмой по месту работы для подтверждения различных правовых фактов и целевого предоставления: ходатайство, письмо-рекомендация, характеристика, справка, удостоверение, пропуск, командировочное удостоверение и др.;

• документы, составляемые и направляемые гражданами администрации или профсоюзной организации фирмы в целях установления, изменения или прекращения трудовых или иных правоотношений: личные заявления, резюме, объяснительные записки, жалобы и др.;

• служебные документы, характеризующие профессиональные и деловые качества работника и не предназначенные для передачи этому работнику: представление к назначению на должность, аттестационный лист, протокол проведения собеседования, результаты тестирования, биографическая справка и другие документы.

Документ подлинный — документ, сведения об авторе, времени и месте создания которого, содержащиеся в самом докуете или выявленные иным путем, подтверждают достоверность его происхождения. Обычно это оригинал документа, оформленный в установленном порядке и подписанный, т.е. имеющий юридическую силу.

Документ секретный — документ на любом носителе, отнесенный к информационным ресурсам ограниченного доступа и содержащий сведения, составляющие государственную тайну, которые включены в утвержденный специальный перечень таких сведений.

Документ черновой — рукописный, машинописный или электронный документ, отражающий работу автора или редактора над его текстом. Множество черновиков порождает обилие вариантов и редакций документа.

Документальный фонд — совокупность документов, образующихся в деятельности юридического или физического лица.

Документирование — запись информации на различных носителях по установленным правилам. Способы документирования: текстовое, изобразительное, в том числе техническое, фото-, кино (видео)-, фоно (аудио)- документирование, текстовое и техническое документирование с использованием печатающих устройств ЭВМ, документирование на языках общения человека с техническими средствами. Средства документирования: а) простейшие — ручки, карандаши; б) механические, электромеханические и электронные (пишущие машины, магнитофоны, диктофоны, фото-, кино-, видео- и аудиотехника, регистрирующие приборы и т.д.; в) средства автоматизированного документирования на базе компьютерной техники.

Документирование конфиденциальной информации — этап стадии исполнения конфиденциального документа. Представляет собой процесс составления документа — запечатления (фиксирования) на выбранном типе носителя его текста, содержащего

конфиденциальные сведения. Конфиденциальный документ составляется при наличии серьезных объективных потребностей, а не в силу субъективного желания сотрудника фирмы. Необходимость документирования конфиденциальной информации санкционируется полномочным должностным лицом, которое берет на себя ответственность за распространение защищаемой информации (см. также Составление текста конфиденциального документа).

Документооборот — движение документов в организации с момента их создания или получения до завершения исполнения или отправки. По отношению к организационной структуре выделяется внутренний и внешний документооборот как составной элемент «жизненного цикла» документа.

Документооборот (документопоток) защищенный — контролируемое движение конфиденциальной документированной информации по регламентированным пунктам приема, обработки, рассмотрения, исполнения, использования и хранения в жестких условиях организационного и технологического обеспечения безопасности как носителя информации, так и самой информации. Принципы и направления движения конфиденциальных традиционных и электронных документов в аппарате фирмы едины при любой технологической системе обработки и хранения документов. Меняются методы работы с документами, но технологическая взаимосвязь документооборота с процессом управления сохраняется. Документооборот, как объект защиты, представляет собой упорядоченную совокупность (сеть) каналов объективного, санкционированного распространения конфиденциальной документированной информации (документов) в процессе управленческой и производственной деятельности пользователей (потребителей) этой информации. В результате увеличивается число источников, обладающих ценными сведениями и расширяются потенциальные возможности для утраты конфиденциальной информации. Защищенность документопотоков достигается за счет: формирования самостоятельных, изолированных потоков конфиденциальных документов и часто — дополнительного их разбиения на подпотоки в соответствии со степенью конфиденциальности перемещаемых документов; использования автономной технологической системы обработки и хранения конфиденциальных документов; регламентации избирательности в доставке информации разрешительной (разграничительной) системой доступа персонала к конфиденциальной информации, документам и базам данных; расчленения (дробления) информации между исполнителями в соответствии с их функциональными обязанностями (см. также Структура потоков (документопотоков) конфиденциальных документов).

Документопоток — движение документов в определенном направлении для облегчения решения управленческих задач. Могут быть: входящий (входной), исходящий (выходной) и внутренний документопотоки. Является обязательной частью любой информационной системы. Документопоток делится на технологические стадии обработки документов в процессе их движения.

Допуск к конфиденциальной информации — часть разрешительной (разграничительной) системы доступа персонала к конфиденциальной информации, представляет собой процедуру оформления права сотрудника фирмы или иного лица на доступ к информации ограниченного распространения и одновременно правовой акт согласия (разрешения) собственниками владельца информации на передачу ее для работы конкретному лицу. Наличие допуска предоставляет сотруднику формальное право работать со строго определенным кругом конфиденциальных документов, дел и баз данных. Оформление допуска всегда носит добровольный характер и отражается в приказе первого руководителя фирмы или соответствующим пунктом в контракте.

Доступ к информации несанкционированный — случайное или преднамеренное овладение конфиденциальными сведениями и возможное опасное воздействие на них лиц, не имеющих права доступа к конкретной защищаемой информации. Доступ, не санкционированный полномочным должностным лицом, считается незаконным. Случайный несанкционированный доступ к. конфиденциальной информации возникает в силу обстоятельств или в результате безответственности персонала, работающего с документами, информационными ресурсами ограниченного доступа. Лицо, случайно получившее знание конфиденциальных сведений, обычно не заинтересовано в их запоминании и использовании. Преднамеренный несанкционированный доступ к конфиденциальной информации осуществляет злоумышленник, который целенаправленно организует канал несанкционированного доступа к интересующей его информации. Злоумышленник, получивший информацию, имеет

возможность совершить с ней противоправные действия, использовать в своих целях, нарушить целостность информации или ее сохранность, уничтожить носитель. Владелец информационных ресурсов обязан оповещать собственника этих ресурсов о всех фактах нарушения режима конфиденциальности информации.

Доступ к информации санкционированный — часть разрешительной (разграничительной) системы доступа персонала к конфиденциальной информации, представляет собой практическую реализацию права сотрудника на работу с подобной информацией, необходимой ему для выполнения возложенных на него функций. Доступ санкционируется полномочным должностным лицом (первым руководителем, его заместителем, руководителем подразделения, службы или направления деятельности) в отношении конкретной информации и конкретного сотрудника фирмы. Разрешение на доступ к конфиденциальным сведения (документам, делам, базам данных и т.п.) всегда является строго персонифицированным (индивидуальным) и дается полномочным руководителем только в письменном виде: резолюцией на документе, приказом, утверждающим схему именного доступа к конкретным группам информации, утвержденным руководителем списком-разрешением на обложке дела. Иерархическая последовательность доступа к информации реализуется по принципу «чем выше ценность конфиденциальных сведений, тем меньшее число сотрудников может их знать». Должностное лицо, разрешившее доступ сотрудника к конфиденциальным сведениям, несет персональную ответственность за правильность принятого решения. Аналогичным образом персональную ответственность за сохранность носителя и конфиденциальность информации несет сотрудник, получивший доступ к конкретной информации.

Доступ к компьютеру — санкционирование полномочным должностным лицом работы сотрудника с определенным составом вычислительной техники. ^Предусматривает: регламентацию состава сотрудников, имеющих право входа 'в помещение, в котором находится соответствующая вычислительная техника, средства связи; регламентацию временного режима нахождения этих лиц в указанных помещениях; персональное и временное протоколирование разрешения и периода работы этих лиц в иное время (вечернее, выходные дни); организацию охраны этих помещений в рабочее и нерабочее время, определение порядка снятия помещений с охраны и отключения охранных технических средств, определение порядка постановки помещений на охрану; организацию контролируемого, пропускного режима входа в указанные помещения; регламентацию действий охраны и персонала в экстремальных ситуациях; контроль вносимых и выносимых из помещения персоналом машинных и бумажных носителей информации, оборудования и личных вещей. По окончании рабочего дня конфиденциальная информация переносится на дискеты, которые сдаются в службу конфиденциальной документации. Информация на жестких дисках компьютеров стирается. Однако помещение подлежит охране, так как в неохраняемые компьютеры легко установить средства технической разведки (см. Средства несанкционированного доступа к информации) или специальными методами восстановить информацию на жестких дисках.

Доступ к базам данным и файлам — санкционирование полномочным должностным лицом работы сотрудника с определенным составом конфиденциальных сведений и файлов. Предусматривает: определение и регламентацию состава сотрудников, допускаемых к работе с определенными конфиденциальными базами данных и файлами; контроль доступа персонала администратором базы данных; фиксирование в машинной памяти имен пользователей и операторов, имеющих право доступа к базам данных и файлам; учет состава базы данных и файлов, регулярную проверку наличия, целостности и комплектности электронных документов; регистрацию (протоколирование) входа в базу данных или файл, автоматическую регистрацию имени пользователя и времени работы, сохранение первоначальной информации; регистрацию (протоколирование) попыток несанкционированного входа в базу данных или файл, регистрацию ошибочных действий пользователя, автоматическую передачу сигнала тревоги охране и автоматическое отключение компьютера; установление и бессистемное по сроку изменение имен пользователей, массивов и файлов (паролей, кодов, классификационных идентификаторов, ключевых слов); отключение ЭВМ при нарушениях в системе регулирования доступа или сбое системы защиты информации; блокирование отключенной, незагруженной ЭВМ при недлительных перерывах в работе пользователя.

Доступ к машинным носителям, находящимся вне ЭВМ — санкционирование полномочным должностным лицом работы сотрудника с определенным составом носителей информации.

Предусматривает: организацию оформления, учета и выдачи сотрудникам чистых технических носителей информации; организацию ежедневной фиксируемой выдачи сотрудникам и приема от сотрудников носителей с записанной информацией (основных и резервных); регламентацию состава сотрудников, имеющих право работать с конфиденциальной информацией на компьютере и получать в службе конфиденциальной документации учтенные носители информации; организацию системы закрепления за сотрудниками технических носителей информации и контроля за сохранностью и целостностью информации, учета динамики изменения состава записанной информации; организацию порядка уничтожения информации на носителе (форматирования носителя и порядка его физического уничтожения); организацию хранения носителей в службе конфиденциальной документации в рабочее и нерабочее время, порядок эвакуации носителей в экстремальных ситуациях; определение и регламентацию состава сотрудников, не сдающих по объективным причинам машинные носители информации на хранение в службу конфиденциальной документации в конце рабочего дня, организацию особой охраны помещений и компьютеров этих сотрудников. Работа сотрудников службы конфиденциальной документации с техническими носителями информации должна быть организована по аналогии с бумажными конфиденциальными документами.

Дубликат документа - повторный экземпляр подлинника документа, имеющий юридическую силу.

Единица хранения архивных документов — учетная и классификационная единица, представляющая собой физически обособленный документ или совокупность документов, имеющих самостоятельное значение.

З

Защита информации — практическая реализация комплексной программы (концепции) информационной безопасности фирмы, жестко регламентированный и динамический технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности ценных информационных ресурсов и в конечном счете обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности фирмы. В данном случае безопасность расценивается в качестве реального результата, достигнутого за счет функционирования выбранной системы защиты информации. Предполагается, что защита конфиденциальной информации (или защита секретов) осуществляется от различного вида угроз безопасности информации, прежде всего — несанкционированного доступа к нем злоумышленника. Защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю или иному лицу. Защиты требует не только конфиденциальный документ. Часто обычный открытый правовой акт важно сохранить в целостности и безопасности от похитителя или стихийного бедствия.

Защита информации в публикаторской и выставочной деятельности — направление обеспечения безопасности информации, предусматривающее заблаговременный анализ и экспертизу предназначенной для широкого оглашения любой информации о деятельности фирмы и ее продукции в целях обнаружения в содержании или элементах отображения этой информации (таблицах, формулах, рисунках, фотографиях, схемах) конфиденциальных сведений или намека на наличие таких сведений. Подобная информация должна, как правило, анализироваться от противного — с точки зрения того интереса, который будет проявлен к ней конкурентами, и объема полезных сведений, извлекаемых конкурентом из ее содержания. При рекламировании потребительских достоинств и возможностей новой продукции не должна раскрываться сущность технологических новшеств, технологических секретов, за счет которых достигнуты эти достоинства. Материалы, не прошедшие экспертизу, опубликованию не подлежат. Экспертиза включает также последующий контроль всех опубликованных о фирме материалов, сообщений средств массовой информации, рекламных изданий и выставочных проспектов. Помимо этого анализируются подобные материалы других фирм для определения возможной утраты данной фирмой ценных сведений.

Защита информации в службе персонала — направление обеспечения безопасности информации фирмы в части сохранения конфиденциальности персональных данных, которые формируются в процессе документирования трудовых правоотношений сотрудников с фирмой. В состав документации, содержащей персональные данные, входят: приказы поличному составу, комплексы документов кандидатов на должность, комплексы

материалов по анкетированию, тестированию кандидатов на должность, проведению собеседований (строго конфиденциальны), личные дела сотрудников, их трудовые книжки; дела, содержащие основания к приказам по личному составу, учетно-справочный аппарат (картотеки, журналы учета, базы данных), отчетные, аналитические и справочные материалы. Кроме того, конфиденциальной является организационная, распорядительная и инструктивная документация службы персонала, документы по планированию, контролю и анализу эффективности работы службы. Эта документация раскрывает технологию работы службы, распределение обязанностей среди сотрудников и другие ценные для злоумышленника сведения. Система защиты информации в службе персонала должна предусматривать: четкое распределение функций между сотрудниками, закрепление за каждым сотрудником необходимых ему для выполнения функциональных обязанностей массивов документов и информации, установление персональной ответственности этих сотрудников за сохранность носителей и конфиденциальность информации, проведение регулярных проверок наличия документов и материалов, регламентацию порядка ведения работы с посетителями и справочной работы и т.п. Не менее важно правильно организовать рабочие места сотрудников службы, перекрыть технические каналы утечки информации, организовать охрану помещения с использованием современных технических средств.

Защита информации при ведении переговоров и совещаний — направление обеспечения безопасности информации, которое распространяется в процессе этих мероприятий. К требованиям защиты относятся: заблаговременная регламентация состава участников по каждому обсуждаемому вопросу, проведение переговоров, совещаний в специально подготовленном, выделенном помещении, контроль доступа участии ков переговоров и совещаний отдельно по каждому вопросу, регламентация порядка документирования хода переговоров и совещаний, их результатов и порядка рассылки принятых документов. Первый руководитель фирмы должен установить максимально возможный состав конфиденциальных сведений, который может быть сообщен сотрудниками фирмы участникам переговоров или совещаний. Информация оглашается при условии предупреждения участников указанных мероприятий о ее конфиденциальности, а иногда — после подписания ими обязательств о сохранении ее в тайне. Участники переговоров от фирмы должны заранее выработать тактику ведения переговоров и соответствующую динамику (очередность) оглашения конфиденциальной информации, а также определить условия возникновения в этом рабочей необходимости. Целесообразно строить переговоры таким образом, чтобы сообщаемые конфиденциальные сведения всегда были минимальными по составу и объему.

Защита информации при приеме посетителей — направление обеспечения безопасности информации, предусматривающее классификацию посетителей фирмы по степени их деловых отношений с фирмой (клиенты, партнеры, представители других организационных структур, частные лица), по степени разрешенного им доступа в помещения фирмы (во все помещения, только в определенные помещения, только к определенному сотруднику, только в операционный зал), по степени разрешенного им ознакомления с информацией фирмы (только с рекламными изданиями, только с материалами, касающимися заинтересованной структуры или лица, только с материалами по определенному вопросу, только с открытыми материалами фирмы, только с конкретными конфиденциальными сведениями). Любые разрешительные действия в отношении посетителей совершаются первым руководителем фирмы, обеспечиваются и контролируются службой безопасности. При входе в служебные помещения фирмы (кроме операционного зала общего доступа) посетитель обязан предъявить документ, удостоверяющий его личность (но не визитную карточку). Ему выдается соответствующий визуальный идентификатор (пропуск), регламентирующий его права в помещениях фирмы. При выходе идентификатор должен быть сдан. Перемещение посетителя в здании фирмы осуществляется только в сопровождении полномочного сотрудника фирмы — секретаря руководителя, сотрудника, с которым посетитель обговорил заблаговременно свой визит, сотрудника службы безопасности. Факт ознакомления посетителя с любым документом фирмы фиксируется сотрудниками служб конфиденциальной или открытой документации фирмы в учетной форме этого документа; на самом документе посетитель ставит роспись ознакомления, расшифровку росписи, наименование представляемой организации и дату. При приеме частных (иногда случайных) лиц руководители и сотрудники ведут беседу не в рабочих комнатах, а в специально предназначенном для этого помещении, в присутствии секретаря или

сотрудника службы безопасности.

Злоумышленник — лицо (группа лиц), предполагающее совершить или умышленно совершающее противоправные действия с целью овладения информацией, составляющей тот или иной вид тайны. К злоумышленникам относят недобросовестных конкурентов и партнеров, лиц, действующих в их интересах, профессиональных агентов, занимающихся промышленным или экомическим шпионажем, агентов, информаторов, представителей криминальных структур, отдельных преступных элементов, психически больных лиц, работника данной фирмы, сотрудничающего со злоумышленником, иных лиц, пытающихся нанести ущерб фирме, ее руководству или персоналу. Понятие злоумышленник» тесно связано, с понятием «постороннее лицо».

Идентификатор— персональное обозначение (код, шифр, имя, пропуск, персональная карточка определенного цвета с фотографией, магнитная или иная карта и т.п.), позволяющее однозначно выделить идентифицируемый объект среди других в полном множестве объектов. Используется в системах доступа.

Идентификация пользователя — отождествление лиц по их характеристикам или путем опознавания по приметам или документам в целях определение полномочий, связанных с доступом к конфиденциальной информации. Присвоение имени пользователю информационной системы, потребителю информации.

Изготовление конфиденциального документа — этап стадии исполнения конфиденциального документа. Осуществляется централизованно в службе конфиденциальной документации с санкции полномочного должностного лица, а не по инициативе исполнителя. Перед изготовлением беловика документа производится учет — присвоение единого учетного номера черновику и проекту будущего документа. Одновременно на еще не изготовленный документ заполняется комплект учетных форм. Полученный черновиком учетный номер (номер по учету подготовленных документов) будет сопровождать документ в течение его последующего «жизненного цикла». В учетной карточке отражается последовательно ход работы над проектом документа в процессе его изготовления, издания, последующего исполнения или отправки (см. Конвертование конфиденциальных документов), хранения или уничтожения. Обязательно учитываются проекты конфиденциальных электронных документов, факсов, телеграмм. Этим обеспечивается контроль службы конфиденциальной документации за сохранностью черновика, проекта, самого документа и всех материалов к нему. Изготовление документа включает в себя следующие процедуры: прием работником службы конфиденциальной документации от исполнителя черновика документа; традиционный или автоматизированный учет черновика и проекта будущего документа; печатание и выдача черновика и проекта документа исполнителю; перепечатывание отдельных листов и документа в целом; снятие копий с документа, производство выписки и изготовление дополнительных экземпляров документа; ежедневная проверка наличия у работника службы конфиденциальной документации черновиков и документов, находящихся на этапе изготовления. На последнем листе всех экземпляров отпечатанного документа на лицевой или оборотной стороне проставляются номер документа, фамилия исполнителя и номер его телефона, количество экземпляров и адресность каждого из них. Может указываться номер магнитного носителя, с которого печатался документ.

Издание конфиденциального документа — этап стадии исполнения конфиденциального документа. Представляет собой процесс придания подготовленному документу юридической силы, преобразование беловика документа в подлинник. Включает следующие процедуры: заключительное корректирование текста и подготовка документа к изданию (подбор необходимых материалов, предыдущих документов, уточнение фамилий, сроков исполнения и т.п.); итоговое внутреннее согласование документа (предварительное согласование проводилось при работе над черновиком и проектом документа); внешнее согласование документа; подписание документа руководителем; утверждение, одобрение, разрешение использования документа (при необходимости).

Инженерно-технический элемент системы защиты информации — комплекс организационно-технических, технических и технологических мероприятий защиты информации, предназначенных для пассивного и активного противодействия средствам технической разведки и формирования рубежей охраны территории, здания, помещений и оборудования с помощью совокупности технических средств. Элемент включает: сооружения инженерной (физической) защиты от проникновения посторонних лиц на территорию, в здание и помещения фирмы; средства защиты технических каналов распространения и возможной

утечки информации, средства защиты помещений от визуальных способов технической разведки; технические средства обеспечения охраны фирмы; средства противопожарной охраны; средства обнаружения приборов и устройств технической разведки; средства противодействия этим приборам и устройствам, технические средства контроля, предотвращающие вынос персоналом из помещений специально маркированных предметов, документов, дискет.

Интеллектуальная собственность — исключительное право юридического или физического лица на результаты интеллектуальной деятельности, творческого труда (информационный продукт), имеющего конкретную ценность для собственника или владельца этих результатов. Обычно выделяются два вида информации, интеллектуально ценной для предпринимателя, его собственной, частной информации: а) техническая или технологическая (ценная идея, технологическое новшество, ноу-хау, новое знание, параметры, формулы, рецептуры, результаты испытаний опытных образцов и т.п.) и б) деловая (творческое решение управленческой или иной проблемы, результаты исследования рынка, экономические показатели, прогнозы, стратегия действий на рынке, реорганизация структуры фирмы и т.п.).

Информационные ресурсы — отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах). Документирование информации (создание официального документа) является обязательным условием включения информации в информационные ресурсы. По принадлежности к тому или иному виду собственности информационные ресурсы могут быть государственными или негосударственными и как элемент состава имущества находятся в собственности граждан, органов государственной и исполнительной власти, органов местного самоуправления, государственных учреждений, организаций и предприятий, общественных объединений, предпринимательских структур. Информационные ресурсы могут быть товаром, за исключением случаев, предусмотренных законодательством Российской Федерации. В соответствии с интересами обеспечения национальной и экономической безопасности и степенью ценности для государства, а также правовыми, экономическими и другими интересами предпринимательских (негосударственных) структур информационные ресурсы могут быть: а) открытыми, т.е. общедоступными, используемыми в работе без специального разрешения, публикуемыми в средствах массовой информации, оглашаемыми на конференциях, в выступлениях, интервью и т.п., и б) ограниченного доступа и использования.

Информационные ресурсы ограниченного доступа — документы и массивы документов, содержащие сведения, отнесенные к тому или иному way тайны и подлежащие защите, охране, наблюдению и контролю. Документированная информация с ограниченным доступом по условиям ее правового статуса подразделяется на информацию, отнесенную к. государственной тайне— секретную и отнесенную к негосударственной тайне — конфиденциальную.

Информационный продукт — документированная информация, подготовленная в соответствии с потребностями пользователей и предназначенная или применяемая для удовлетворения потребностей пользователей, потребителей.

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

Информация защищаемая — синоним понятий информация секретная и информация конфиденциальная. Информация может быть отнесена к категории защищаемой, если ее содержание неизвестно конкуренту или противнику, а также, если указанная неизвестность дает определенные преимущества в политической, экономической или предпринимательской деятельности. При отнесении информации к защищаемой должны соблюдаться принципы законности, обоснованности, своевременности и др.

Информация конфиденциальная — документированная информация, относимая к одному из видов негосударственной тайны или персональным данным, доступ к которой ограничивается в соответствии с законодательством Российской Федерации. Решение о таком ограничении принимает собственник или владелец указанной информации, т.е. он устанавливает правовой режим информации, являющейся его интеллектуальной собственностью (кроме персональных данных). Ограничение предполагает наличие особых правил документирования конфиденциальной информации, работы с ней персонала, специальной технологической системы обработки и хранения этой информации.

Информация может быть отнесена к конфиденциальной при соблюдении следующих условий: информация не должна отражать негативные стороны деятельности фирмы; информация не должна быть общедоступной или общеизвестной; возникновение или получение информации предпринимателем должно быть законным и связанным с расходованием материального, финансового или интеллектуального потенциала фирмы; предпринимателем должны быть выполнены реальные действия по защите этой информации и обучению персонала фирмы работе с ней. Конфиденциальными не могут быть сведения по установленным формам отчетности о финансово-хозяйственной деятельности и иные сведения, необходимые для проверки правильности исчисления и уплаты налогов и других обязательных платежей; сведения о численности и составе работающих, их заработной плате, а также другие сведения, установленные законодательством и постановлениями Правительства Российской Федерации.

Информация секретная — сведения, которые в соответствии с Законом Российской Федерации «О государственной тайне» и утвержденными государственным, отраслевыми и ведомственными перечнями содержат государственные секреты.

Информация ценная — информация, которая составляет интеллектуальную собственность предпринимателя или группы предпринимателей и дает им возможность производить качественную продукцию, товары и услуги, пользующиеся повышенным спросом на рынке, заключать выгодные сделки, находить новых клиентов, покупателей как самой продукции, так и технологии ее производства. Подобная информация охраняется нормами авторского и смежного права, патентного права, товарным знаком, знаком обслуживания или защищается включением ее в категорию конфиденциальной. Ценная информация образуется в производственной и деловой сферах деятельности предпринимателя — в прогнозировании и планировании этой деятельности, управлении фирмой, финансовой, производственной и торговой деятельности, формировании ценовой политики и состава компаньонов, партнеров и поставщиков, потребителей продукции, изучении состава и направлений деятельности конкурентов фирмы, проведении научной и исследовательской деятельности, использовании новых технологий, подборе и управлении персоналом, организации экономической безопасности фирмы. Определение состава ценных деловых и технологических сведений основывается на принципе экономической целесообразности и оценивается стоимостными показателями, размерами упущенной выгоды и убытков фирмы при утрате информации, а также размером прибыли от использования этой информации с учетом затрат на ее защиту. Часто информация становится ценной ввиду ее правового значения для фирмы (учредительные документы, контракты и др.).

Исполнение конфиденциального документа — процесс составления и оформления официального документа. В отличие от открытых документов стадия исполнения конфиденциальных документов включает ряд дополнительных технологических этапов и процедур, обеспечивающих сохранность носителя и конфиденциальность документируемой информации. Стадия включает в себя следующие технологические этапы: установление уровня грифа конфиденциальности сведений, подлежащих включению в будущий документ; оформление и учет носителя для документирования данной конфиденциальной информации; документирование информации; изготовление конфиденциального документа; издание документа. Указанные этапы характеризуются не только регламентированной технологией, но и жесткими правилами работы персонала с конфиденциальным документом.

Использование конфиденциального документа — включение документа в информационно-документационную систему, обеспечивающую исполнение других документов, выполнение управленческих действий и принятие решений. Для использования в работе обычно поступают: законодательные акты, организационно-правовые, нормативные, распорядительные, справочно-информационные документы, разнообразные рекламные издания и научно-техническая информация.

Источник конфиденциальной информации — объективно пассивный накопитель (концентратор) конфиденциальной информации. В научной литературе часто используется альтернативный для сферы защиты информации термин — «носитель конфиденциальной информации» по аналогии с термином «секретоноситель». К основным видам источников относятся: традиционные и электронные документы, базы данных, персонал фирмы и окружающие ее люди, физические поля, сопровождающие работу вычислительной и другой офисной техники, публикации о фирме и ее разработках, рекламные издания, выставочные материалы. Каждый из источи и ков делится на множество подвидов.

Классификация источников конфиденциальной информации, сопровождающих работу конкретной фирмы, является одной из главных составных частей аналитической работы по выявлению каналов несанкционированного доступа к конфиденциальной информации и обеспечению безопасности информации в каждом источнике.

Источник угрозы конфиденциальной информации — объективные и субъективные явления, события, факторы, действия и обстоятельства, содержащие опасность для ценной информации. К объективным источникам можно отнести: экстремальные ситуации, несовершенство технических средств и др. Субъективные источники связаны с человеческим фактором и включают: злоумышленников различного рода, посторонних лиц, посетителей, неквалифицированный или безответственный персонал, психически неполноценных людей, сотрудников, обиженных руководством фирмы, и др. Источники угрозы могут быть внешними и внутренними. Внешние источники находятся вне фирмы и представлены чрезвычайными событиями, а также организационными структурами и физическими лицами, проявляющими определенный интерес к фирме. Внутренние источники угрозы связаны с фатальными событиями в здании фирмы, а также с персоналом. Однако наличие источника угрозы само по себе не является угрозой. Угроза реализуется в действиях.

К

Канал несанкционированного доступа к информации — совокупность незащищенных или слабо защищенных фирмой направлений возможной утраты конфиденциальной информации, которые злоумышленник использует для получения необходимых сведений, преднамеренного незаконного доступа к защищаемой информации. В основе выявления возможного канала несанкционированного доступа лежит взаимодействие злоумышленника с источником информации или преобразование канала объективного распространения информации в канал ее утраты. Этот процесс требует проведения поисковой и аналитической работы и организуется тайно. Каждая фирма обладает своим набором каналов несанкционированного доступа к информации, что зависит от множества моментов — профиля деятельности, объема защищаемой информации, совершенства применяемой системы защиты информации и противодействия злоумышленникам, эффективности аналитической работы, профессионального уровня персонала, местоположения здания фирмы и др. Канал несанкционированного доступа может быть организационным и техническим и обеспечиваться легальными и нелегальными методами.

Канал несанкционированного доступа организационный — направление несанкционированного доступа злоумышленника к конфиденциальной информации, включающее в себя: установление разнообразных, в том числе законных, взаимоотношений злоумышленника с фирмой (поступление на работу в фирму, участие в работе фирмы в качестве партнера, посредника, клиента, использование разнообразных обманных способов, разрешенная или не разрешенная работа с документом, делом, базой данных и т.п.); сотрудничество с работником фирмы или лицом, имеющих доступ к документации фирмы; тайное или по фиктивными документам проникновение в здание фирмы, помещения, незаконное получение документов, информации; использование коммуникативных связей фирмы (участие в конфиденциальных совещаниях и переговорах, переписке с фирмой и др.). Организационный канал в большинстве случаев основывается на таком распространенном явлении, как случайное или умышленное разглашение конфиденциальной информации персоналом фирмы. Организационные каналы отбираются или формируются злоумышленником индивидуально в соответствии с его профессиональным умением, конкретной ситуацией и прогнозировать их сложно.

Канал несанкционированного доступа технический — физически и путь утечки информации от источника или канала объективного распространения информации к злоумышленнику. Основывается на применении злоумышленником специальных технических средств разведки, позволяющих получить защищаемую информацию без непосредственного контакта с источником, владеющим этой информацией. Канал возникает: при анализе злоумышленником физических полей и излучений, появляющихся в процессе работы вычислительной и другой офисной техники, при перехвате информации, имеющей звуковую, визуальную или иную форму отображения. Основными видами технических каналов являются: акустический, электромагнитный, визуально-оптический и др. Каналы носят стандартный характер и перекрываются также стандартным набором средств противодействия. Это каналы прогнозируемые. Часто используются злоумышленником одновременно с трудно прогнозируемыми организационными каналами.

Канал объективного распространения конфиденциальной информации — путь перемещения конфиденциальных сведений из одного источника в другой в качестве санкционированного (разрешенного, законного) действия или в силу объективных закономерностей. Указанный канал отличается активностью и включает в себя: деловые, управленческие, торговые, научные и другие коммуникативные регламентированные связи, информационные сети, естественные технические каналы излучения, создания фона, поля. Например: обсуждение конфиденциального вопроса на закрытом совещании, передача документа на исполнение, запись на бумаге изобретения, переговоры с потенциальным партнером, работа на ЭВМ и др.

Картотека учетная — традиционный справочно-информационный банк данных по конфиденциальным документам при любых видах учета. Разновидность учетных картотек: валовая нумерационная картотека, в которой карточки располагаются в последовательности учетных номеров документов; картотека на неисполненные документы, в которой карточки располагаются по исполнителям (картотека «За исполнителями»); справочная картотека на исполненные документы, в которой карточки располагаются по корреспондентам, рубрикам номенклатуры дел или другому удобному для использования признаку; кодификационная картотека по распорядительным документам; контрольная сроковая картотека.

Карточка архивного фонда — учетный документ, содержащий название, сведения о количестве, составе документов архивного фонда и месте его хранения, предназначенный для централизованного государственного учета архивных документов.

Коллегиальность контроля — один из важнейших методов обеспечения сохранности носителя и конфиденциальности информации. Предусматривает регулярную проверку вторым сотрудником службы конфиденциальной документации полноты охвата учетом всех поступивших и подготовленных документов, чистых носителей информации, правильности заполнения учетных форм и указания местонахождения документа, правомерности передачи документов. Коллегиально ведется проверка наличия документов, уничтожение документов и проверка соблюдения исполнителями порядка работы с конфиденциальными документами.

Конвертование (пакетирование) конфиденциальных документов — совокупность технических приемов, предотвращающих несанкционированное тайное вскрытие конвертов (пакетов) и извлечение из них конфиденциальных документов, а также прочтение текста без извлечения документа и даже вскрытия конверта. Несанкционированно вскрытый конверт не может быть восстановлен, что сигнализирует об утрате документом конфиденциальности или его подмене. К. указанным приемам относятся: использование светонепроницаемых конвертов, имеющих также защиту от современных способов прочтения текста документа, надежное заклеивание клапанов конвертов для предотвращения «отпаривания» мест склейки, прошивание конверта и документа прочной нитью, опечатывание концов нити и мест склейки. При пересылке документов часто используется «двойное пакетирование», т.е. вкладывание опечатанного и прошитого конверта с грифом конфиденциальности в другой конверт, не имеющий указанных особенностей в оформлении. Это позволяет избежать проявления любопытства посторонних лиц к опечатанному конверту.

Контроль доступа — регулярные проверочные действия по определению-правомерности разрешений на доступ и доступа сотрудников фирмы и представителей других организационных структур в помещения фирмы, к конфиденциальным документам, делам, базам данных, компьютерам и средствам связи. Осуществляется службой безопасности фирмы и направлен на предотвращение или выявление фактов необоснованного разрешения на доступ, а также несанкционированного доступа в выделенные помещения, к защищаемой информации и документам, охраняемому оборудованию фирмы. При ведении контроля используются сведения, фиксируемые в учетных формах традиционных и электронных документов и дел, учетных формах степени осведомленности сотрудников в тайне фирмы, протоколах доступа к электронным базам данных, машинных журналах, учетных формах выдачи сотрудникам и посетителям идентификаторов (пропусков), учетных формах посещения выделенных помещений. Контроль доступа является также одной из основных функциональных обязанностей работников службы конфиденциальной документации.

Контроль эффективности системы защиты информации — анализ степени уязвимости конфиденциальной информации. Осуществляют в негосударственных структурах органы

государственной власти в порядке, определяемом Правительством Российской Федерации. На уровне фирмы собственный контроль эффективности системы защиты информации является функцией службы безопасности и проводится путем регулярного анализа, соответствия структуры системы защиты информации реальным и потенциальным угрозам безопасности конфиденциальной информации фирмы и соответствующей степени противодействия этим угрозам. Результатом контрольной работы становится разработка предложений по совершенствованию системы защиты информации, усложнению системы или ее упрощению вплоть до отказа от подобной системы. В основе указанных предложений должна лежать идея максимально возможного снижения степени уязвимости конфиденциальной информации.

Конфиденциальность (лат. confidentia — доверие) — доверительность, секретность. Неоглашаемая, доверительная, задушевная беседа, письмо, сообщение, полученное по доверенности, тайное общение, тайные переговоры, беседы, документирование с использованием тайнописи.

Конфиденциальность информации — синоним секретности информации. Вместе с тем термин широко используется исключительно для обозначения информационных ресурсов ограниченного доступа, не отнесенных к государственной тайне (подробнее см. Информация конфиденциальная).

Копирование и тиражирование конфиденциальных документов — расширение числа источников защищаемой информации. Осуществляется в условиях, гарантирующих сохранность всех используемых носителей и конфиденциальность информации. Условия предусматривают: наличие письменного разрешения полномочного должностного лица на снятие копии с документа или его размножение, учет изготовленных копий и размноженных экземпляров, учет печатных форм и коллегиальность их уничтожения, учет выдачи исполнителю документа, его копий и экземпляров. Копирование и размножение конфиденциальных документов осуществляется централизованно в службе конфиденциальной документации. Выполнение этих процедур на рабочих местах исполнителей не разрешается. Аналогичным образом копируются электронные документы, создаются их страховые и резервные копии.

Копия документа —документ, полностью воспроизводящий информацию оригинала документа и все его внешние признаки или часть их, не имеющий юридической силы. Копия части документа называется выпиской. Выделяют копии рукописные и машинописные, а также факсимильные, изготовленные с помощью копировальной техники.

Копия документа заверенная— копия документа, на которой в соответствии с установленным порядком проставляют необходимые реквизиты, придающие ей юридическую силу. Копия может быть нотариально заверенной или заверенной в установленных законом случаях соответствующим должностным лицом (например, работником отдела кадров). Копией является дубликат документа.

Копия конфиденциального документа страховая, резервная — воспроизведение на бумажном носителе электронного конфиденциального документа и (или) его электронной учетной формы, электронных описей документов с целью обеспечения сохранности информации в случаях утраты документов в компьютере по техническим причинам. Одновременно со страховыми копиями на бумажном носителе изготовляется на магнитном носителе резервная копия документа, учетной формы, описей. Объективно необходимое увеличение числа источников, содержащих конфиденциальную информацию, осложняет процесс ее защиты и может стать причиной утраты конфиденциальности информации.

Криптографический элемент системы защиты информации — комплекс способов и средств защиты конфиденциальной информации методами криптографии. Элемент включает: регламентацию использования различных криптографических методов в ЭВМ и локальных сетях; определение условий и методов криптографирования текста документа при передаче его по незащищенным каналам почтовой, телеграфной, телетайпной, факсимильной и электронной связи; регламентацию использования средств криптографирования переговоров по незащищенным каналам телефонной и радиосвязи; регламентацию доступа персонала в выделенные помещения с помощью идентифицирующих кодов, шифров.

Криптография — тайнопись, система разнообразных способов изменения формы отображения информации (текста, речи), позволяющих сделать содержание информации непонятным для лиц, не владеющих знанием использованного шифра. Криптографические методы представляют собой шифрование, кодирование, сжатие, расчленение (разнесение)

информации. Криптография входит составной частью в понятие криптологии, в которое включается также криптоанализ — дешифрование текста или речи известным ключом или без него.

Л

Лицензирование в области защиты информации — установленное законодательством право заниматься работами по защите информации для стороннего заказчика. Предоставляется организациям, имеющим на этот вид деятельности соответствующее разрешение (лицензию). Необходимость этого лицензирования определяется тем, то собственникам конфиденциальной информации нужна доброкачественная продукция, действительно обеспечивающая защиту информации. В то же время проведение работ по защите информации в собственных нуждах приобретения лицензии не требует.

М

Машинограмма—документ, изготовленный автоматически средствами вычислительной техники (например, с помощью принтера) на бумажном носителе в человекочитаемой форме и предназначенный для оформления в установленном порядке.

Методы защиты информации — выборочно применяемые универсальные и специфические способы (приемы, меры, мероприятия) реализации элементов системы защиты информации и входящих в них содержательных частей для формирования комплексной и индивидуальной структуры данной системы. К универсальным способам можно отнести: регламентацию процесса, выделение процесса, скрытие процесса или информации, ограничение доступа к процессу или информации, дезинформацию конкурента или злоумышленника, расчленение (дробление) информации, тайны, создание физических и иных препятствий на пути злоумышленника (рубежей защиты). Специфические способы обеспечивают индивидуализацию системы в зависимости от поставленных задач защиты информации в конкретной фирме.

Методы легального получения информации — вид «невинного шпионажа», отличающийся правовой безопасностью, но предопределяющий возникновение интереса к конкурирующей фирме, необходимости обнаружения или формирования и использования каналов несанкционированного доступа к ее ценной, конфиденциальной информации. В основе реализации методов лежит кропотливая аналитическая работа специалистов-экспертов над опубликованными и общедоступными материалами конкурирующей фирмы. Одновременно исследуется продукция фирмы, рекламные издания, сведения, полученные в процессе официальных или неофициальных бесед и переговоров с сотрудниками фирмы, материалы пресс-конференций, презентаций, научных симпозиумов, сведения, получаемые из информационных сетей. Легальные методы дают злоумышленнику основную массу необходимой, интересующей его информации и формулируют задачу по добыванию нелегальными методами отсутствующих сведений.

Методы нелегального получения информации — всегда носят незаконный характер и используются в целях несанкционированного доступа к защищаемой информации, которую невозможно получить легальными методами. В основе нелегального получения информации лежит поиск злоумышленником существующих в фирме и наиболее эффективных в конкретных условиях незащищенных организационных и технических каналов несанкционированного доступа к информации, формирование таких каналов при их отсутствии и реализация плана практического комплексного использования этих каналов. Нелегальные методы предполагают: воровство, копирование, продуманный обман, подслушивание разговоров, использование болтливости, безответственности и низкого профессионализма персонала, подделку идентифицирующих документов, взяточничество, склонение к сотрудничеству, подкуп, шантаж, использование болезненного состояния сотрудника, провоцирование персонала на ошибочные действия, инсценирование или организацию экстремальных ситуаций, применение различных криминальных приемов. При использовании нелегальных методов часто образуется агентурный канал добывания ценной, конфиденциальной информации. К нелегальным методам относятся: перехват информации объективно распространяемой по техническим каналам, визуальное наблюдение за помещениями фирмы и персоналом, анализ продуктов и объектов, содержащих следы защищаемой информации, анализ архитектурных особенностей объектов защиты, анализ отходов производства, мусора, выносимого из офиса, и др.

Н

Номенклатура конфиденциальных дел — документ, предназначенный для систематизации

заводимых в фирме конфиденциальных дел. Решает задачи учета формируемых дел (номенклатурного учета дел), обеспечения проверки наличия документов и дел, закрепления схемы разрешительной системы доступа сотрудников фирмы к делам, учета законченных сформированных дел (закрытых дел), учета движения, использования и уничтожения архивных документов и дел до передачи их в ведомственный архив (архив фирмы). В соответствии с этими задачами табличная часть номенклатуры имеет следующие специфические графы: гриф конфиденциальности дела, фамилия сотрудника (исполнителя), которому предоставлено право пользования делом, отметка о движении дела, отметка о проверке наличия дела.

Нормативно-методическое обеспечение системы защиты информации — комплекс документов, регламентирующих процесс функционирования системы защиты информации, сформированной в целях безопасности информации конкретной фирмы, а также регламентирующих функционирование службы безопасности этой фирмы. Включает ряд обязательных организационных, инструктивных и информационных документов, которые закрепляют принципы, требования и способы предотвращения или ограничения сферы реализации пассивных и активных угроз конфиденциальной информации. Важнейшими организационными документами являются: положение о службе безопасности, положение о службе конфиденциальной документации, должностные инструкции работников указанных служб и др. Технологические инструктивные документы представлены: перечнем сведений, составляющих тайну фирмы, инструкцией по обеспечению безопасности конфиденциальной информации, инструкцией по обработке, хранению и движению конфиденциальных документов и др. Информационные (методические, советующие, обучающие) документы — правила, требования, указания, методики, памятки и др., которые детализируют процессы защиты информации в отношении отдельных групп информации и документов, отдельных категорий сотрудников фирмы в конкретных типовых ситуациях.

Носитель конфиденциальной документированной информации (документа) — материальный объект, предназначенный для документирования (фиксирования, закрепления) и хранения на нем конфиденциальной информации в целях передачи ее во времени и пространстве. Носители могут быть традиционными бумажными или картонными: листы бумаги, ватмана, координатной бумаги, книги, тетради, журналы учета, картонные учетные карточки, неперфорированные и перфорированные бумажные ленты. Эти носители используются для нанесения на них информации рукописным, машинописным или автоматическим способами. К традиционным относятся также фотографические носители информации: фото- и кинопленка, фотобумага, слайды, микрофотопленки, фотографические фонограммы. Широкое современное и перспективное значение имеют технические магнитные носители документированной информации: магнитные ленты, диски, дискеты и др. для обеспечения работы ЭВМ, магнитные карты для идентификации личности человека, магнитные носители для видео- и аудиозаписи. В качестве носителей конфиденциальной информации используются также лазерные и иные диски, пластиковые карты и др. Носители могут быть чистыми, могут содержать черновую, первоначальную, неоформленную информацию, рабочие записи, могут иметь информацию в оформленном виде и являться документами. Чистые, оформленные носители конфиденциальной информации подлежат учету (см. Оформление и учет носителей конфиденциальной информации).

О

Обработка изданных документов — технологическая стадия, в процессе которой выполняются технологические этапы процедуры и операции по отправке документов адресатам или передаче внутренних документов для использования в управлении основной деятельностью фирмы. Осуществляется централизованно службой конфиденциальной документации в рамках традиционной или автоматизированной системы. Стадия обработки изданных документов делится на два этапа: а) этап передачи в службу конфиденциальной документации и обработки документов, предназначенных для отправки, и б) этап передачи в эту службу и обработки внутренних документов. Первый этап включает процедуры: получения от исполнителя всех экземпляров документа и материалов, возникших при его подготовке, а также инициативного документа, послужившего основанием для издания подготовленного документ та; уничтожения черновиков, вариантов и других потерявших ценность материалов; получения документа с другого вида учета (инвентарного, архивного и др.); конвертования (пакетирования) документа, оформления реестра или записи в разностной книге; внесения отметки в

учетную форму документа; отправления конвертов (пакетов), телексов, факсов и др.; внесения отметки службы доставки в реестр, разносную книгу и другие формы. Второй этап включает те же процедуры, но вместо процедур подготовки к отправке и отправки выполняются процедуры: передачи документа соответствующему руководителю или исполнителю; исполнения и возвращения документа от исполнителя; передачи документа на другие виды учета.

Обработка поступивших документов — технологическая стадия, в процессе которой выполняются процедуры проверки соответствия характеристик конфиденциальных документов записям в журнале учета пакетов, проверки комплектности и целостности документов, учета поступивших документов в соответствующих учетных формах, внесения учетного номера документа в журнал учета пакетов, ежедневного контроля полноты учета всех поступивших документов, распределения конфиденциальных документов по руководителям и исполнителям. Осуществляется централизованно службой конфиденциальной документации. При распределении документы делятся на группы: а) передаваемые на резолюцию конкретным полномочным руководителям с целью принятия решения и определения состава допускаемых к документу исполнителей; б) передаваемые непосредственно руководителям подразделений или исполнителям в соответствии с утвержденной схемой доступа к документам типового содержания без резолюции руководителя (см. также Передача конфиденциальных документов руководителям и исполнителям).

Обязательство о неразглашении конфиденциальных сведений — правовой документ, добровольное письменное согласие претендента на должность, сотрудника фирмы или иного лица на ограничение его права в отношении использования конфиденциальной информации фирмы. Одновременно в обязательстве (подписке) указанные лица предупреждаются об ответственности за разглашение этой информации. Состав конфиденциальных сведений, с которыми они будут работать, сообщается только после подписания обязательства. Целесообразно, чтобы обязательство подписывали все сотрудники фирмы и лица, связанные с фирмой деловыми отношениями, в том числе не имеющие отношения к конфиденциальным сведениям, но располагающие возможностью ознакомиться с ними при исполнении служебных обязанностей. Обязательство подписывается также увольняющимся сотрудником.

Ознакомление с конфиденциальным документом — процесс информирования сотрудника фирмы или иного заинтересованного лица, осуществляемый в соответствии с резолюцией полномочного руководителя на конфиденциальном документе, о принятом им решении или решении другой организационной структуры. Процесс завершается проставлением сотрудником визы ознакомления, но может потребоваться последующее составление другого документа или повторное обращение к этому документу. Ознакомление сотрудника с документом производится службой конфиденциальной документации. Сотрудник этой службы обязан предоставить для прочтения сотруднику только ту часть документа, которая указана в резолюции руководителя. Не допускается разрешать сотруднику знакомиться с текстом документа в полном объеме или делать выписки на неучтенном носителе. В технологическом отношении ознакомление с документом представляет собой первоначальную операцию исполнения или использования конфиденциального документа.

Опись конфиденциальных документов дела — перечень конфиденциальных документов, находящихся (подшитых) в деле, служащий для контроля их сохранности и комплектности. В описи (внутренней описи) дела указываются учетные номера документов, грифы конфиденциальности, даты подписания или утверждения, виды и краткое содержание документов, номера листов дела, соответствующих расположению документов в деле. Опись подшивается в начале дела и имеет самостоятельную нумерацию листов. Опись документов должна содержаться также в личных делах сотрудников, в папках текущего хранения неисполненных документов, предшествовать электронным документам массива, магнитного носителя, вестись персонально по каждому руководителю и исполнителю, работающим с конфиденциальными документами.

Опись конфиденциальных документов, находящихся у исполнителя — перечень документов и носителей информации, выданных сотруднику фирмы для работы. Предназначена для их учета, проверки сохранности (наличия) и контроля правильности использования и хранения.

Опись конфиденциальных документов фирмы — перечень конфиденциальных документов

фирмы. Ведется в некрупных фирмах, структурах малого бизнеса с небольшим количеством конфиденциальных документов, обрабатываемых в рамках существующей технологической системы, предназначенной для открытых документов, но обеспеченной минимальным составом методов защиты. Опись служит для дополнительного учета конфиденциальных документов, проверки их наличия и комплектности, своевременного снятия грифа конфиденциальности. Может иметь традиционную бумажную или электронную форму. В крупных фирмах ведется инвентарная опись законченных производством дел, картотек и журналов.

Организационный элемент системы защиты информации — комплекс направлений и методов управленческого, ограничительного и технологического характера, определяющих основы и содержание системы защиты, побуждающих персонал соблюдать правила защиты конфиденциальной информации фирмы. Организационные меры связаны с установлением режима конфиденциальности в фирме. Элемент включает в себя: формирование и регламентацию деятельности службы безопасности и службы конфиденциальной документации, организацию составления и регулярного обновления перечней конфиденциальной информации и документации фирмы; регламентацию разрешительной системы доступа персонала к конфиденциальной информации; регламентацию направлений и методов работы с персоналом, контроля соблюдения им правил зашиты информации; регламентацию технологической системы обработки и хранения конфиденциальных документов, ведение всех видов аналитической работы; регламентацию системы охраны фирмы и порядка приобретения, установки и эксплуатации инженерно-технических средств защиты информации и охраны; регламентацию действий персонала в экстремальных ситуациях и др. Организационная защита является стержнем, который связывает в единую систему все другие элементы.

Оригинал документа — первоначальный, единственный, уникальный документ. Может быть черновым и беловым документом и подлинником.

Ответственность персональная — одно из главных требований к организации функционирования системы защиты информации и обязательное условие обеспечения эффективности этой системы. Предусматривается, что полномочный руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность заданное разрешение. В свою очередь, каждый сотрудник фирмы (в том числе работник службы конфиденциальной документации), получающий для работы конфиденциальный документ, несет аналогичную ответственность сохранность носителя и конфиденциальность информации.

Оформление дел с конфиденциальными документами — комплекс технологических процедур обработки исполненных документов. Имеет отличительные особенности по сравнению с идентичной работой по оформлению дел с открытыми документами. Процедура оформления дела при его заведении дополнительно включает: указание на обложке дела грифа конфиденциальности и состава допущенных к делу исполнителей, оформление карточки учета разрешений и выдачи дела, подшивку вдело чистых бланков внутренней описи документов. Особенностями процедуры оформления дела при его формировании являются: внесение данных о подшиваемом документе во внутреннюю опись, нумерация листов документа в деле, прошнуровывание листов, внесение отметки о включении документа в дело в учетную форму документа. Процедура оформления дела при его закрытии в целом идентична процедуре подготовки открытых дел о сдаче в архив, но дополнительно выполняются следующие операции: опечатывание на заверительном листе концов шнурка, внесение дела в инвентарную опись законченных производством дел, картотек и журналов.

Оформление документа — проставление реквизитов, установленных правилами документирования.

Оформление и учет носителей конфиденциальной информации — этап стадии исполнения конфиденциального документа. Осуществляется заблаговременно, т.е. до начала составления документа. Назначение учета носителей (документов предварительного учета) состоит в том, чтобы обеспечить безопасность информации, контроль ее сохранности не только в подлиннике, но и во всех черновых материалах, вариантах и редакциях документа, отдельных записях. Основными задачами учета являются следующие: закрепление факта присвоения носителю (например, обычным листам бумаги, тетради, блокноту, дискете и т.п.) степени конфиденциальности; присвоение носителю учетного номера и включение его в справочно-информационный банк для обеспечения

контроля за использованием носителя и проверки его наличия; документирование фактов перемещения носителя между сотрудниками фирмы, закрепления персональной ответственности за его сохранность; контроль за работой исполнителя над документом и своевременным уничтожением носителя или его частей, потерявших практическое значение. В предпринимательских структурах предварительный учет бумажных носителей информации, как правило, не производится. Не ставятся на учет носители информации, предназначенные для составления документов, которые относятся к служебной и профессиональной тайне. Однако магнитные носители везде и в обязательном порядке ставятся на инвентарный (перечневый) учет, т.е. включаются в инвентарную опись и маркируются. Предварительный учет носителей целесообразен на уровне руководства фирмы, где концентрируется действительно ценная информация, обычно с грифом «Строго конфиденциально», а также при документировании технических и технологических новшеств.

Охрана информационных ресурсов открытого доступа — обеспечение безопасности ценной информации, являющейся интеллектуальной собственностью юридического или физического лица. Осуществляется нормами патентного, авторского и смежных прав, торговыми правилами и обычаями, а также использованием товарного знака, торговой марки, знака обслуживания, эмблемы предприятия.

П

Передача конфиденциальных документов руководителям и исполнителям — усложненный по сравнению с аналогичной стадией обработки открытых документов комплекс процедур, выполняемый службой конфиденциальной документации и предусматривающий как оперативное доведение документа до исполнителя, так и соблюдение действующей в фирме разрешительной системы доступа персонала к конфиденциальным документам, которая лежит в основе избирательности в доставке документированной информации руководителям и исполнителям, и порядка возложения или снятия с них персональной ответственности за документ. Следует учитывать, что пользователь (потребитель) конфиденциальной информации руководствуется указаниями руководителя при определении, какая информация ему нужна и какой информацией Он может пользоваться. Передача документов сопровождается выполнением следующих процедур: оформление в учетной форме факта передачи; рассмотрение документа руководителем; оформление и передача документа исполнителю или на другой участок службы конфиденциальной документации (см. также Обработка поступивших документов; Работа службы конфиденциальной документации с исполнителями). Передача документов между руководителями и исполнителями осуществляется только через службу конфиденциальной документации с обязательным фиксированием динамики изменения местонахождения документа. Передача документов руководителям без росписи или через секретарей, референтов, помощников не допускается.

Перечень конфиденциальных документов — систематизированный список Получаемых и издаваемых конфиденциальных документов фирмы, составляется ,на основе перечня конфиденциальных сведений. Предназначен для регламентации рационального состава конфиденциальных документов и их основных характеристик, в частности уровня грифа конфиденциальности сведений, состава сотрудников, допущенных к документу, минимально необходимого объема конфиденциальных сведений, включаемых в документ, сроков конфиденциальности документа и др. Перечень регулярно изменяется и дополняется в соответствии с исправлениями, вносимыми в перечень конфиденциальных сведений фирмы.

Перечень конфиденциальных сведений — классифицированный список типовой и конкретной ценной информации о проводимых работах, производимой продукции, научных и деловых идеях, технологических новшествах. Форма отнесения информации фирмы к категории защищаемой. В основе перечня обычно лежит типовой состав ценных сведений фирм данного профиля. Наличие перечня — одно из главных условий эффективного функционирования системы защиты информации. Перечень формируется индивидуально каждой фирмой в соответствий с рекомендациями специальной комиссии и утверждается первым руководителем фирмы. Перечень — это многоцелевой документ, предназначенный для: выделения конфиденциальных документов из общего потока документов, реализации разрешительной системы доступа персонала к конфиденциальным сведениям и документам, использования в качестве доказательства в суде при рассмотрении дел о краже ценной информации. При составлении перечня производится расчленение (дробление) тайны

фирмы на отдельные информационные элементы, известные разным лицам. Одновременно в перечне регламентируется срок конфиденциальности сведений, уровень грифа конфиденциальности и состав сотрудников, которым дано право пользоваться этими сведениями. Перечень является рабочим инструментом и должен постоянно обновляться и корректироваться в соответствии с динамикой изменений в деятельности фирмы. На основе перечни может составляться перечень конфиденциальных документов фирмы.

Перечень секретных сведений — наиболее распространенная в России форма засекречивания информации. Составляется отраслевыми и ведомственными органами управления на основе Закона Российской Федерации «О государственной тайне» и Перечня сведений, отнесенных к государственной тайне, утвержденных Президентом Российской Федерации и подлежащих обязательному опубликованию. Отраслевая принадлежность засекречиваемых сведений означает привязку их к определенной сфере производственной деятельности, ведомственная принадлежность — привязку сведений к органу государственной власти. Программно-целевое засекречивание сведений означает их принадлежность к целевым программам научно-исследовательских и опытно-конструкторских работ, охватывающих чаще всего несколько отраслей промышленности.

Персональные данные — информация о гражданах, лицах, особах, персонах, личностях, персоналиях, т.е. любая, в том числе недокументированная, информация, относящаяся к конкретному человеку. Субъектами персональных данных являются граждане РФ, иностранные граждане и лица без гражданства, находящиеся на территории России, к личности которых относятся соответствующие персональные данные. Персональные (личные) данные всегда входят в категорию конфиденциальной информации. Не допускается сбор, передача, уничтожение, хранение, использование и распространение информации о частной жизни, а равно информации, нарушающей личную, семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений физического лица без его согласия, кроме как на основании судебного решения. Запрещается ограничение прав граждан как результат использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности. Персональные данные находят отражение прежде всего в персональных и других документах кадровой службы, в информационно-документационной системе, обеспечивающей управление персоналом.

Подбор персонала для работы с конфиденциальной информацией — комплекс аналитических процедур, позволяющих убедиться в высоком уровне моральных, личных и профессиональных качеств претендента на должность, связанную с владением конфиденциальной информацией. Усложнение процесса подбора претендента на указанную должность связано с высокой степенью ответственности за принятие решения о допуске лица к тайне фирмы и наличием даже в больших фирмах достаточно ограниченного контингента сотрудников, работающих с конфиденциальной информацией. Аналитические процедуры включают:

тщательную проверку предоставленных кандидатами персональных документов, опрос авторитетных для фирмы лиц, лично знающих каждого кандидата, проведение с кандидатом ряда собеседований и при необходимости тестирований, отбор из нескольких кандидатов реального претендента на должность, подписание контракта о временной работе в целях более глубокого и всестороннего изучения качеств претендента. Такие же процедуры проводятся при переводе сотрудника фирмы на должность, связанную с владением конфиденциальной информацией.

Подлинник (официального) документа — первый или единичный экземпляр официального документа.

Подмена документа — противоправное действие, совершаемое сотрудником фирмы или иным лицом в целях сокрытия факта кражи или утери документа, его части (листа, приложения и др.), копии; представляет собой попытку снятия с себя подозрения или ответственности за утрату носителя и конфиденциальности информации. Осуществляется путем фальсификации и диктуется, как правило, чувством страха. Сотрудник или иное лицо, являющиеся злоумышленником или его сообщником, совершают подмену обдуманно и на профессиональном уровне.

Пользователь (потребитель) информационных ресурсов — лицо (субъект), обращающееся к информационной системе или посреднику за получением необходимой ему информации и пользующееся ею. Пользователь не может участвовать в проектировании, модернизации или эксплуатации, контроле эффективности системы защиты информации.

Посетитель — 1) лицо, которому необходимо решить определенный круг деловых или личных вопросов с руководителями и менеджерами фирмы; 2) лицо, совместно с которым полномочные лица вырабатывают определенные решения по направлениям деятельности фирмы.

Посетители — сотрудники фирмы делятся на:

• сотрудников, имеющих право свободного входа в кабинет руководителя в любое время рабочего дня (заместители руководителя, референты, секретари);

• сотрудников, работающих с руководителем в режиме вызова или решающих с ним деловые вопросы в часы приема по служебным делам (Нижестоящие руководители, эксперты, специалисты-менеджеры);

• сотрудников, инициирующих свой прием руководителем в часы приема по личным вопросам.

Посетители, не являющиеся сотрудниками фирмы, и в соответствии с характером их взаимоотношений с фирмой могут подразделяться на:

• лиц, не включенных в штат сотрудников, но входящих в качестве членов в коллективный орган управления деятельностью фирмы (акционеры, члены различных советов и др.);

• представителей государственных учреждений и организаций, с которыми фирма сотрудничает в соответствии с законом (работники различных инспекций, муниципальных органов управления, правоохранительных органов и др.);

• сотрудничающих с фирмой физических лиц и представителей предприятий и организаций, банков, рекламных агентств, торговых представительств, средств массовой информации (клиенты, партнеры, коммерсанты, инвесторы, спонсоры, журналисты и др.);

• представителей иных государственных и негосударственных структур, с которыми фирма не имеет деловых отношений;

• частных лиц.

Постороннее лицо — любое лицо, не имеющее непосредственного отношения к деятельности фирмы (работники коммунальных службы, экстремальной помощи, прохожие и др.), посетители фирмы, работники других организационных структур, а также сотрудники данной фирмы, не имеющие права доступа в определенное помещение, к конкретному документу, информации, базе данных, продукции. Каждое из указанных лиц может быть злоумышленником или его сообщником, агентом, но может и не быть им.

Право информационное — совокупность законодательных информационно-правовых норм, регулирующих общественные отношения в информационной сфере и являющихся гарантированным инструментом охраны интеллектуальной информационной собственности (информационного продукта) юридических и физических лиц.

Правовой элемент системы защиты информации — юридическое закрепление взаимоотношений фирмы и государства по поводу правомерности использования системы защиты информации, фирмы и персонала по поводу обязанности персонала соблюдать установленные собственником информации ограничительные и технологические меры защитного характера, а также ответственности персонала за нарушение порядка защиты информации. Правовой элемент включает: наличие в организационных документах фирмы, правилах внутреннего трудового распорядка, контрактах, заключаемых с сотрудниками, в должностных и рабочих инструкциях положений и обязательств по защите конфиденциальной информации: формулирование и доведение до сведения всех сотрудников фирмы положения о правовой ответственности за разглашение конфиденциальной информации, несанкционированное уничтожение или фальсификацию документов; разъяснение лицам, принимаемым на работу, положения о добровольности принимаемых ими на себя ограничений, связанных с выполнением обязанностей по защите информации.

Предписание — документ, предъявляемый командированным в фирму лицом. В документе указываются цель командирования и подлежащие выполнению задания, требующие ознакомления с определенным составом конфиденциальной информации и документов. Предписание составляется на бланке организации, командирующей данное лицо, подписывается первым руководителем и заверяется печатью этой организации. Разрешение на доступ командированного лица к конкретным конфиденциальным документам, делам и базам данных санкционирует первый руководитель фирмы в резолюции на предписании. Ознакомление командированного лица с конфиденциальными

сведениями должно происходить в присутствии сотрудника фирмы, назначенного в резолюции ответственным за работу командированного лица. Возможность командирования, его цели и фамилия командируемого лица, как правило, заранее согласовываются первыми руководителями фирм, организаций.

Проверка наличия документов, дел и носителей информации — установление реального соответствия имеющихся в наличии конфиденциальных документов, дел и носителей записям в учетных формах, их сохранности, целостности и комплектности, а также своевременное выявление фактов утраты конфиденциальных материалов и определение правильности выполнения процедур и операций по учету, хранению, исполнению и использованию этих материалов. В ходе проверки рассматриваются вопросы снятия с документов грифа конфиденциальности. Проверки могут быть регламентированными (периодическими) и нерегламентированными. Регламентированные проверки проводятся ежедневно (самопроверки исполнителей, проверки вторым сотрудником службы конфиденциальной документации), ежеквартально и по окончании календарного года. Квартальные и годовые проверки наличия проводятся специально назначаемой комиссией. Нерегламентированные проверки осуществляются при смене руководителей подразделений и направлений деятельности, увольнении сотрудников, по завершении экстремальной ситуации, выявлении факта возможной утраты носителя или разглашения информации.

Программно-аппаратный элемент системы защиты информации — комплекс специальных методов и средств защиты информации в автоматизированных системах и сетях. Элемент включает: автономные программы, обеспечивающие защиту информации и контроль защищенности информации; программы защиты информации, работающие в комплексе с программами обработки информации; программы защиты информации, работающие в комплексе с техническими (аппаратными) устройствами защиты информации (прерывающими работу ЭВМ при нарушении системы доступа, стирающими данные при несанкционированном входе в базу данных и др.). Составные части программно-аппаратной защиты, коды, пароли и т.п. атрибуты комплексной системы защиты вычислительной техники разрабатываются и меняются специализированной организацией. Применение пользователями собственных программ не допускается.

Противодействие злоумышленнику — целенаправленное создание неблагоприятных условий и трудно преодолимых препятствий (рубежей) для лица, пытающегося совершить несанкционированный доступ и овладение конфиденциальной информацией фирмы. Может быть пассивным и активным. При пассивном противодействии система защиты информации функционирует в обычном режиме, ведется плановая аналитическая и контрольная работа с источниками и каналами распространения информации, организационными и техническими каналами возможного несанкционированного доступа к конфиденциальной информации. Активное противодействие предполагает подключение дополнительных организационных и технических методов защиты информации (например, закрытие доступа к определенным категориям информации, организацию усиленной охраны здания и помещений, ограничение деловых связей фирмы и др.).

Р

Работа персонала с конфиденциальным документом — комплекс требований по соблюдению руководителями всех рангов и сотрудниками фирмы специальных ограничительных и технологических норм, предупреждающих утрату документа, носителя, дела или утрату конфиденциальности информации и в определенной степени гарантирующих информационную безопасность фирмы. Требования предусматривают: наличие у сотрудника оборудованного необходимым образом рабочего места, строгое соблюдение им разрешительной системы доступа к конфиденциальным документам, носителям и делам, учет во внутренней описи всех конфиденциальных материалов, находящихся у руководителя или исполнителя, правильное хранение документов на рабочем месте, своевременную, ежедневную сдачу документов в службу конфиденциальной документации, строгое исполнение запретительных пунктов соответствующей инструкции, немедленное информирование руководства фирмы об утрате документа или разглашении информации. На рабочем столе любого сотрудника фирмы всегда должен быть только тот документ и материалы к нему, с которыми он работает. Другие документы должны находиться в запертом сейфе (металлическом шкафу).

Работа с персоналом, обладающим конфиденциальной информацией — комплекс мер предупредительного, профилактического, текущего характера, предназначенных для приобретения персоналом устойчивых знаний и навыков выполнения действующих правил

защиты информации, а также для контроля за соблюдение персоналом требований обеспечения информационной безопасности фирмы. Включает в себя: обучение и систематическое инструктирование сотрудников, проведение регулярной индивидуальной воспитательной работы с персоналом, работающим с конфиденциальными сведениями и документами, постоянный контроль за работой этих сотрудников, аналитическую работу по изучению и учету степени осведомленности персонала в области конфиденциальных работ фирмы, проведение служебных расследований по фактам утраты конфиденциальных документов, нарушения персоналом требований по защите информации, совершенствование методики текущей работы с персоналом.

Работа службы конфиденциальной документации с исполнителями — ежедневная выдача и прием от исполнителя конфиденциального документа (комплекта документов или опечатанного кейса с документами), контроль за работой исполнителя с конфиденциальными документами. При выдаче документа проверяется в присутствии исполнителя: наличие разрешения на доступ данного сотрудника к конкретному документу (в резолюции, схеме доступа и др.), комплектность документа и физическая сохранность всех его частей. После проверки исполнитель расписывается в учетной карточке или карточке учета выдачи документа и вносит сведения о документе во внутреннюю опись документов, находящихся у исполнителя. Работник службы конфиденциальной документации вносит отметку в контрольный журнал о местонахождении документа (см. Учет местонахождения документа). При приеме документа от исполнителя проверяется: соответствие реквизитов документа данным, указанным в его учетной форме, комплектность документа, количество листов (перелистыванием), отсутствие подмены или порчи листов и других частей документа. Роспись сотрудника службы конфиденциальной документации в приеме документа ставится только после проведения указанной проверки. Проставляется роспись в учетной форме или карточке учета выдачи документа. Сотрудник делает также отметку о возврате документа во внутренней описи документов, находящихся у исполнителя. Одновременно в контрольный журнал вносится запись о новом местонахождении документа. Электронные документы передаются исполнителю в копии после получения от него росписи в бумажном экземпляре электронной учетной карточки документа или электронной подписи непосредственно в самой электронной учетной карточке, находящейся в компьютере службы конфиденциальной документации. При выдаче и приеме документа должна быть исключена возможность ознакомления с документом или его учетной формой посторонних лиц. Контроль правильности работы исполнителя с конфиденциальными документами на рабочем месте проверяется службой конфиденциальной документации не реже одного раза в квартал.

Разведка в бизнесе — аналитическая работа с использованием методов легального получения конфиденциальной информации, изучения устремлений и направленности интересов конкурентов и партнеров фирмы в рамках добросовестной конкуренции.

Разглашение конфиденциальной информации — несанкционированный выход конфиденциальных сведений и документов за пределы круга лиц, которым они были доверены или стали известны по службе. Разглашение (огласка, оглашение) информации происходит по вине персонала — случайно, ошибочно или умышленно, добровольно (инициативно) или под воздействием угроз, шантажа, применения наркотических средств, психотропных препаратов. Информацию разглашает всегда человек — устно, письменно, с помощью жестов, мимики, условных сигналов, лично или через посредников, с использованием средств связи и многими другими способами.

Раздробление тайны — классифицированное (иерархическое) дробление предметной совокупности конфиденциальной информации на тематические группы, отдельные элементы, части, известные разным сотрудникам фирмы. Разглашение отдельной части сведений в этом случае не имеет большого практического смысла.

Разрешительная (разграничительная) система доступа к информации — совокупность обязательных норм, устанавливаемых первым руководителем или коллективным органом руководства фирмой с целью закрепления за руководителями и сотрудниками права использования для выполнения служебных обязанностей выделенных помещений, рабочих мест, определенного состава документов и конфиденциальных сведений. Составная часть системы защиты информации. Система решает следующие задачи: ограничения и регламентации состава сотрудников, функциональные обязанности которых требуют знания тайны фирмы и работы с конфиденциальными документами; строгого

избирательного и обоснованного распределения документов и информации между сотрудниками; обеспечения сотрудника всем необходимым для реализации своих служебных функций (документами, делами, базами данных); беспрепятственного прохода сотрудника в здание фирмы, в конкретное рабочее помещение (рабочую зону), к выделенному ему офисному рабочему оборудованию и компьютеру; исключения возможности несанкционированного ознакомления посторонних лиц с конфиденциальной информацией; рационального размещения рабочих мест сотрудников, исключающего бесконтрольное использование ими защищаемой информации. Система включает в себя две составные части: а) допуск сотрудника к конфиденциальной информации и б) непосредственный доступ этого сотрудника к конкретным сведениям.

Расследование служебное — установление причин и лиц, виновных в разглашении ил и утечке информации, утрате документа, носителя или конфиденциальности информации, утраты продукции, содержащей ценные новшества, и других грубых нарушениях правил защиты информации. Проводится сотрудниками службы безопасности фирмы и предназначено для выяснения всех обстоятельств и их последствий, связанных с конкретным фактом. В ходе расследования устанавливаются причины случившегося и виновные лица. По результатам расследования делаются выводы о мере ответственности виновных лиц, даются рекомендации по устранению причин случившегося и исключению подобных фактов в будущем. При необходимости к расследованию привлекаются частные детективные агентства.

Режим — совокупность ограничительных правил, мероприятий, норм, обеспечивающих контролируемый доступ и пребывание на определенной территории, в здании, помещениях, регулирующих порядок ознакомления с защищаемой информацией и документами, предпринимаемых в целях информационной безопасности фирмы. Базируется на разрешительной системе доступа.

Режим конфиденциальности — комплекс мер, входящих в состав действующей в фирме системы защиты информации и обеспечивающих особый правовой статус организации работы сотрудников фирмы. Осуществляется и контролируется службой безопасности фирмы. Включает в себя: разрешительную систему доступа, пропускной режим, особые правила приема на работу сотрудников и текущей работы с персоналом, учет осведомленности каждого сотрудника в тайне фирмы, контроль соблюдения сотрудниками инструкций по защите информации, выполнение охранных мероприятий, в том числе в рабочее время, функционирование специальных технологических систем обработки и хранения конфиденциальных документов и электронной информации, ведение аналитической работы.

Режим пропускной — ограничение на право входа на территорию, в здание или помещения фирмы и регламентация порядка выхода из них. Распространяется на въезд и выезд транспортных средств. Предусматривает также ограничение на право вносить (выносить) или ввозить (вывозить) определяемые руководством фирмы предметы, оборудование и т.п. без специального разрешения полномочных должностных лиц. Ограничивается право сотрудников вносить на территорию фирмы личные вещи, которые могут стать каналом утраты конфиденциальной информации (фотоаппараты, видео- и аудиотехнику, средства связи, дискеты, объемные сумки, кейсы и др.). Пропускной режим реализуется системой пропусков — постоянных, временных, разовых, материальных, транспортных, которые предъявляются на контрольно-пропускном пункте. Наличие пропуска дает право находиться в здании и определенных помещениях фирмы, получать необходимые для работы документы, дела, дискеты, выносить (вывозить) с территории фирмы указанные в пропуске предметы. Пропуска в зависимости от их категории могут быть различной формы, цвета, иметь полосы, снабжаться фотокарточкой владельца и иными идентифицирующими признаками, содержать указание на ограничения в перемещении по зданию. Для контроля за выполнением порядка доступа в помещения фирмы наиболее удобны пропуска-идентификаторы, носимые сотрудниками и посетителями на одежде.

Реквизит документа — обязательный элемент оформления официального документа (вид документа, его автор, дата, подпись и др.).

С

Секрет — см. Тайна.

Секретность — ограничение, накладываемое собственником, на доступ к информации, документам, делам, базам данных, продукции, оборудованию, транспорту, на вход и нахождение в определенной зоне (территории), здании, помещениях.

Сертификация систем и средств защиты информации — аналитические действия по определению эффективности систем защиты информационных ресурсов, качества программных, аппаратных и иных средств защиты. Выполняется специализированной организацией, имеющей соответствующую лицензию. В соответствии с положительными результатами анализа выдается сертификат, удостоверяющий возможность использования указанных систем и средств защиты для обеспечения информационной безопасности фирмы.

Система защиты информации — совокупность направлений, методов, средств и мероприятий, снижающих уязвимость информации и препятствующих несанкционированному доступу к информации, ее разглашению или утечке. Главными требованиями к организации эффективного функционирования системы являются: персональная ответственность руководителей и сотрудников за сохранность носителя и конфиденциальность информации, регламентация состава конфиденциальных сведений и документов, подлежащих защите, регламентация порядка доступа персонала к конфиденциальным сведениям и документам, наличие специализированной службы безопасности, обеспечивающей практическую реализацию системы защиты и нормативно-методического обеспечения деятельности этой службы. Основной характеристикой системы является ее комплексность, т.е. наличие в ней обязательных элементов, охватывающих все направления защиты информации. Соотношение элементов и их содержания обеспечивает индивидуальность построения системы защиты информации конкретной фирмы, ее неповторимость и необходимый заданный уровень защиты с учетом ценности информации и стоимости системы. Элементами системы являются: правовой, организационный, инженерно-технический, криптографический и программно-аппаратный. В каждом элементе защиты могут быть реализованы на практике только отдельные содержательные части в зависимости от поставленных задач защиты в крупных и некрупных фирмах различного профиля, малом бизнесе. Структура системы зависит как от объема и ценности защищаемой информации, так и от характера возникающих угроз безопасности информации, требуемой надежности защиты и стоимости системы.

Система охраны здания, помещений, транспорта и персонала — комплекс организационных и технических мероприятий, реализующих одну из основных функций службы безопасности фирмы. Состав и содержание мероприятий зависят от профиля и объемов деятельности фирмы. Мероприятия включают в себя: аналитическую работу по выявлению потенциальных и реальных угроз охраняемым объектам, степени их опасности, расчет рациональной численности и организацию работы персонала охраны, приобретение, установку и эксплуатацию технических средств охраны, сигнализирования и идентификации, контроль эффективности указанных мероприятий. Действенность охраны в полной мере зависит от профессионализма и качества работы персонала службы охраны и его взаимодействия с указанными техническими средствами. Технические средства не подменяют персонал охраны. Охрана может быть круглосуточной, ночной и эпизодической. В фирмах с большими объемами конфиденциальной информации, наличием незапатентованных новшеств, реализованных в продукции, и в других подобных случаях целесообразна круглосуточная охрана. В неохраняемых фирмах эпизодический вид охраны вводится при выявлении реальной угрозы фирме, ее продукции, информации и персоналу. Этот вид охраны может быть круглосуточным или ночным. Индивидуальная охрана персонала вне здания фирмы осуществляется в зависимости от степени осведомленности сотрудников в тайнах фирмы, а также при перевозке конфиденциальных документов, материальных ценностей, при возникновении реальных угроз отдельным сотрудникам от криминальных элементов.

Служба безопасности — самостоятельное структурное подразделение фирмы, обеспечивающее экономическую безопасность ее функционирования. В негосударственных структурах подобная служба создается по усмотрению руководящего органа фирмы. Наличие подобной службы является одним из главных условий эффективного функционирования системы защиты информации. Основными задачами службы являются: ведение всех направлений аналитической работы и маркетинговых исследований, планирование работы по обеспечению экономической безопасности фирмы, разработка, эксплуатация и регулярное обновление системы защиты информации, обеспечение режима конфиденциальности проводимых фирмой работ, контроль эффективности используемых мер безопасности и определение направлений их совершенствования. Единообразия в построении служб безопасности нет. Основными подразделениями службы могут быть: информационно-аналитическая группа; группа маркетинговых исследований; группа

обеспечения внешней безопасности; группа конфиденциальной документации; группа режима и охраны; группа инженерно-технической защиты информации; контрольная группа. В некрупных фирмах и малом бизнесе функции службы безопасности выполняет менеджер по безопасности или выборочно референт первого руководителя. Деятельность службы безопасности должна сопровождаться необходимым нормативно-методическим обеспечением. Любая информация и документация, образующаяся или используемая в деятельности службы безопасности, является конфиденциальной.

Служба конфиденциальной документации — самостоятельное подразделение фирмы или подразделение службы безопасности, его статус зависит от ценности и объемов конфиденциальной документации фирмы. Служба предназначена для решения задач и выполнения функций обработки, хранения и организации рассмотрения, исполнения, использования и движения конфиденциальных документов. В состав службы в крупной фирме входят следующие функциональные группы (участки): группа учета поступивших документов; группа учета носителей конфиденциальных документов; группа учета подготовленных документов; группа учета номенклатурных дел; группа инвентарного учета; группа изготовления документов; копировально-множительная группа; экспедиционная группа; архив; контрольно-методическая группа. В некрупных фирмах функции службы конфиденциальной документации выполняет управляющий делами, менеджер по документации (деловой и технической), референт первого руководителя фирмы или один из сотрудников службы открытой документации (канцелярии, секретариата). Обработку документов, содержащих служебную информацию ограниченного распространения (документов с грифом «Для служебного пользования»), осуществляет структурное подразделение, которому поручена обработка открытой документации.

Собеседование — устное общение с кандидатами на вакантную должность или сотрудником фирмы. Проводится, как правило, по заранее подготовленному вопроснику работниками (экспертами) службы персонала или службы безопасности: при приеме граждан (или переводе сотрудников) на должности, связанные с владением конфиденциальными сведениями (собеседования по предоставленным документам, по профессиональным и биографическим фактам с целью определения прежде всего личных и моральных качеств гражданина, выявления возможных злоумышленников, реальных причин желания работать на фирме и др.); при увольнении сотрудника (собеседование о недопустимости разглашения конфиденциальных сведений фирмы и др.); в процессе работы сотрудника в фирме (собеседования по итогам обучения или инструктирования в области защиты информации, при обнаружении фактов разглашения информации и др.). Собеседование может дополняться тестированием, анкетированием и другими методами психологического анализа личности.

Собственник информационных ресурсов — субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения указанным объектом.

Составление текста конфиденциального документа — документирование защищаемой информации. Требует соблюдения специальных правил, основными из которых являются: объем конфиденциальных сведений, включаемых в документ, должен быть минимальным и определяться реальной ситуацией; документ всегда должен касаться только одного вопроса (темы), что необходимо для четкого функционирования разрешительной системы доступа к конфиденциальной информации; организационные, распорядительные, плановые, отчетные и другие подобные документы должны иметь функциональные персонифицированные приложения-задания, что позволяет не доводить эти документы в полном объеме до исполнителей; конфиденциальные показатели (формулы, рецептуры, выводы, результаты наблюдений, описания технологических процессов, результатов опытов и др.) должны фиксироваться в документе только один раз и не повторятся в других документах; не допускаются в неконфиденциальных документах намеки на наличие конфиденциальных сведений или их описание в произвольной форме; не допускается включение в неконфиденциальные документы сведений, составляющих интеллектуальную собственность или коммерческую тайну других фирм или лиц, без их согласия. При пересылке конфиденциальных документов обычной почтой или по незащищенным каналам связи целесообразно произвести шифрование текста.

Сохранность конфиденциального документа, носителя — одна из главных задач системы защиты информации. Обеспечивается совокупностью правовых, разрешительных и технологических мер. Правовые меры предусматривают персональную ответственность руководителей за принятие правильного решения по доступу сотрудника к документу и

сотрудников за целостность полученного для работы конфиденциального документа на любом носителе. Разрешительные (ограничительные, режимные) меры предусматривают регламентацию минимального состава сотрудников, имеющих право работать с документом, получать для работы чистый учтенный носитель информации. К числу технологических мер относятся наличие комплекса учетных операций на всех стадиях движения документа, носителя, передача документов сотрудникам в соответствии с утвержденной разрешительной системой доступа, регламентация порядка работы персонала с документами, хранение документов на бумажных и магнитных носителях в условиях, исключающих их порчу или доступ к ним посторонних лиц.

Справочно-информационный банк данных автоматизированный — структурированная совокупность сведений о документах, хранящихся в памяти ЭВМ. Имеет следующие основные электронные массивы: инвентарную опись традиционных (бумажных), машиночитаемых, электронных и иных конфиденциальных документов фирмы с указанием их местонахождения (см. Учет местонахождения документа); массивы учетных карточек документов по видам учета; массив учетных карточек выдачи документов по видам учета; опись рабочего и архивного массивов конфиденциальных документов по каждому компьютеру; массив учетных карточек магнитных носителей с перечислением документов, записанных на каждом носителе; опись документов, находящихся у конкретных исполнителей. Учетную и страховую функцию, а также функцию обеспечения персональной ответственности за сохранность документов могут выполнять следующие традиционные массивы, формируемые на основе распечаток (машинограмм) электронных массивов: страховая учетная валовая картотека бумажных экземпляров электронных карточек документов; картотека «За исполнителями» (для внесения росписи за получение и возврат документа); картотека учетных карточек магнитных носителей информации. Кроме того, ведется комплект постоянно обновляемых и достоверных дубликатов, резервных копий всех магнитных носителей, на которых записаны сведения о документах или сами документы, а также машинный журнал (протокол) учета работы ЭВМ и выполняемых действий с документами. При функционировании указанного банка данных в структуре защищенной локальной сети и оперировании при передаче документов электронной подписью количество обеспечивающих традиционных массивов может быть сокращено.

Справочно-информационный банк данных по конфиденциальным документам — структурированная совокупность применяемых учетных форм. Предназначен для контроля за сохранностью документов, накопления и систематизации исходных данных о документах, актуализации массивов информации — внесения в учетные формы рабочих сведений в процессе исполнения или использования документов, обеспечения контроля их исполнения и проверки наличия. Банк может быть традиционным (см. Картотека учетная) и автоматизированным.

Средства защиты информации — технические, криптографические, программные и другие средства, входящие в структуру отдельных элементов системы защиты информации и предназначенные для обеспечения защиты сведений, составляющих тайну фирмы, а также средства, в которых они реализованы, или предназначены для контроля эффективности системы защиты информации.

Средства несанкционированного доступа к информации — специально изготовленные технические средства промышленного шпионажа: приборы, оборудование, системы приборов и средств связи, предназначенные для создания контакта с источником конфиденциальной информации или каналом объективного распространения информации и образования технического канала утечки этой информации (видео- и аудиооборудование, бинокли, лазерные приборы, радиозакладки и др.).

Сроки конфиденциальности информации — временной период ограничения доступа персонала и иных лиц к конфиденциальной информации. Характеризуется большим разбросом во времени — от нескольких часов до нескольких лет. Основная масса конфиденциальной документированной информации после окончания исполнения работы с документами или наступления определенного события теряет свою ценность и конфиденциальность. Для документированной информации, сохранившей конфиденциальность после указанных моментов, период конфиденциальности может быть кратковременным или долговременным в зависимости от ценности информации. К документам долговременного периода конфиденциальности относятся, например, программы и планы развития бизнеса, технологическая документация ноу-хау и др.

Документы кратковременного периода конфиденциальности имеют оперативное значение для деятельности фирмы, например переписка по заключению контракта, факсы о поступлении груза и др. Период конфиденциальности документов определяется по перечню конфиденциальных сведений фирмы и зависит от специфики ее деятельности. При этом не следует отождествлять два разных понятия — срок хранения документов и период их конфиденциальности. Хотя конфиденциальные документы характеризуются и тем и другим понятием.

Стадия в структуре документопотока — относительно самостоятельная составная функциональная часть документопотока, включающая в себя типовой состав технологических процедур и операций, которые выполняются с документом на данной стадии. Подробнее см. Структура потоков (документопотоков) конфиденциальных документов.

Степень конфиденциальности информации — характеристика закрытости сведений и уровня ограничения доступа к ним персонала. Определяется ценностью информации и фиксируется на документе грифом ограничения доступа.

Структура потоков (документопотоков) конфиденциальных документов — комплекс содержательных элементов процесса движения документов в офисе. Отличается от совокупности технологических стадий (функциональных элементов), составляющих потоки открытых документов. Входной документопоток включает в себя следующие стадии обработки конфиденциальных документов, прием, учет и первичная обработка поступивших пакетов, конвертов; учет поступивших документов и формирование справочно-информационного банка данных по документам; предварительное рассмотрение и распределение поступивших документов (см. Обработка поступивших документов); рассмотрение документов руководителями и передача документов на исполнение в другие участки службы конфиденциальной документации; ознакомление с документами исполнителей, исполнение документов. Выходной и внутренний документопотоки включают в себя следующие стадии: исполнение документов; контроль исполнения документов; обработка изданных документов; систематизация исполненных документов в дела (см. Номенклатура конфиденциальных дел), формирование и закрытие дел; подготовка и передача дел в ведомственный архив. Все документопотоки могут включать дополнительные стадии: инвентарный учет документов, дел и носителей информации, не включенных в номенклатуру дел, копирование и тиражирование документов, уничтожение документов, дел и носителей информации, проверка наличия документов, дел и носителей информации. Стадии, формирующие тот или иной документопоток практически реализуются совокупностью процедур и операций, составляющих определенную технологическую систему обработки и хранения конфиденциальных документов.

Тайна — скрытое, неизвестное, неведомое, нечто, скрываемое от других, известное не всем. Синоним тайны — секрет. Секрет — то, что держится в тайне, скрывается от других, тайный способ, скрытая причина. Держать втайне, в секрете — значит защищать сведения о чем-то, защищать информацию. Тайна должна быть в безопасности. Выделяются две глобальные предметные сферы тайны: а) тайны природы, объективные тайны — тайны вселенной, тайны рождения и смерти, тайны Земли и др. и б) тайны людей, субъективные тайны — тайны государства, личности, профессии, производства, тайны мастерства, тайна интеллектуального труда, женские секреты и др. Тайна всегда имеет информационную форму.

Тайна государственная — защищаемые государством сведения в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение (утрата) которых может нанести ущерб безопасности Российской Федерации. Необходимость отнесения сведений к государственной тайне определяется министерствами и ведомствами в соответствии с разграничением полномочий между ними и с помощью специальных экспертных комиссий.

Тайна коммерческая (предпринимательская) — конфиденциальные сведения, не являющиеся государственными секретами и связанные с производством, управлением, финансированием и другой деятельностью предпринимательских структур и направлений подобной деятельности, утрата которых может нанести ущерб деловым интересам этих структур, собственникам и владельцам ценных информационных ресурсов, интеллектуальной собственности.

Тайна личная — сведения о частной жизни граждан, персональные данные о них, сохранение которых втайне гарантируется Конституцией Российской Федерации. Утрата

конфиденциальности указанных сведений может нанести моральный, материальный или иной ущерб физическому лицу. Сведения защищаются как самим физическим лицом, так и любыми государственными и негосударственными структурами.

Тайна негосударственная — защищаемые в соответствии с законодательством собственником или владельцем информационные ресурсы ограниченного доступа, утрата которых может нанести деловой, экономический, моральный или иной ущерб, потерю престижа юридическим или физическим лицам. К негосударственной тайне относят: служебную, коммерческую (предпринимательскую), личную, семейную тайну, технологические новшества предприятий, профессиональную тайну и др.

Тайна профессиональная — секретные и конфиденциальные сведения, составляющие государственную или негосударственную тайну юридических и физически лиц, но защищаемые другими полномочными учреждениями, которым эти сведения стали известны в силу их профессиональной деятельности. Профессиональная тайна включает: тайну предприятий связи и транспорта, банковскую, врачебную тайну, тайну налоговых органов, тайну страхования, нотариальную, адвокатскую тайну, тайну органов ЗАГС, тайну исповеди. Одной из главных задач является защита персональных данных граждан, личной и семейной тайны. К профессиональной тайне мы относит также тайну мастерства.

Тайна семейная — тайна нескольких физических лиц, членов семьи. Близко примыкает к личной тайне, но не тождественна ей по составу защищаемых сведений.

Тайна служебная — конфиденциальные сведения, входящие в понятие информационных ресурсов ограниченного доступа и относящиеся к служебной деятельности государственных учреждений, организаций и предприятий. Доступ к этим сведениям ограничен в интересах обеспечения безопасности информации указанных структур. Подобные сведения не подлежат широкому распространению, оглашению или опубликованию в средствах массовой информации и используются исключительно в целях решения управленческих или производственных задач, например проекты готовящихся документов, рабочие инструкции и др. Состав сведений, составляющих служебную тайну, определяется руководством учреждений, организаций и предприятий. Отнесением к служебной тайне защищаются персональные данные, концентрируемые в службах персонала (отделах кадров) государственных и негосударственных структур. К служебной информации ограниченного распространения не могут быть отнесены: законодательные акты, устанавливающие правовой статус государственных органов, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации; сведения о чрезвычайных ситуациях; описание структуры органа исполнительной власти, его функций, направлений и форм деятельности, а также адрес; порядок рассмотрения и разрешения заявлений и обращений граждан и юридических лиц; сведения об исполнении бюджета; документы, накапливаемые в открытых фондах библиотек и архивов.

Тайнопись — см. Криптография.

Технические средства охраны, сигнализации и идентификации — специальные сооружения, оборудование и приборы, создающие препятствия на пути злоумышленника и оповещающие персонал охраны о попытке несанкционированного проникновения в здание фирмы, хранилища, другие охраняемые, выделенные помещения, к компьютерам, средствам связи. Включают физические препятствия (заборы, решетки на окнах, контрольно-пропускные пункты и др.), средства визуального наблюдения и видеозаписи (телевизионные системы), сигнальные системы различного типа, оповещатели о повреждениях средств охраны и др. В состав указанных средств входят также оповещатели о задымлении в помещениях и возгорании, технические средства идентификации персонала при организации пропускного режима: кодовые замки, магнитные и иные карты, биологические идентификаторы.

Технологическая система обработки и хранения конфиденциальных документов — упорядоченный комплекс организационных и технологических процедур и операций, обеспечивающих служб и технических средств, предназначенных для практической реализации задач, стоящих пред функциональными элементами (стадиями) документопотока. Технология обработки и хранения конфиденциальных и открытых документов базируется на единой научной и методической основе, призванной решить задачи обеспечения документированной информацией управленческие и производственные процессы. Одновременно технологическая система обработки и хранения

конфиденциальных документов решает и другую не менее важную задачу — обеспечение защиты носителей информации и самой информации от потенциальных и реальных угроз их безопасности. Данная система распространяется не только на управленческую (деловую) документацию, но и на конструкторские, научно-технические и другие документы, документированную информацию, записанную на любом типе носителей информации, документы, хранящиеся в ведомственном архиве. Технология обработки документов долговременного срока (периода) конфиденциальности имеет усложненный характер, в то время как документы кратковременного периода конфиденциальности обрабатываются и хранятся по упрощенной схеме и могут не выделяться из технологической системы обработки открытых документов при наличии в этой системе минимальных защитных, контрольных и аналитических элементов. Система может быть традиционной, т.е. делопроизводственной, ручной (см. Делопроизводство конфиденциальное), автоматизированной или смешанной. Смешанные системы предполагают разнообразные варианты совмещения традиционной и автоматизированной систем при обработке документов. Они особенно широко используются в обработке конфиденциальных документов.

Технологическая система обработки и хранения конфиденциальных документов автоматизированная — комплекс организационных и технологических процедур и операций с документами, выполняемый на базе вычислительной техники и средств связи. Система, как и традиционная, делопроизводственная, обеспечивает конкретные потребности персонала в конфиденциальной информации. В силу специфики конфиденциальных документов автоматизированные системы делопроизводственной ориентации в большинстве случаев имеют информационно-справочный характер и оперируют исходными и рабочими данными о документах. Особенностями автоматизированной технологии обработки и хранения конфиденциальных документов являются: обязательное наличие иерархической системы разграничения доступа к информации, хранящейся как в машинных массивах, так и на магнитных носителях вне ЭВМ; закрепление за каждым пользователем строго определенного состава массивов электронной информации и магнитных носителей; сохранение информационной базы учетной функции и функции персональной ответственности за целостность носителя и конфиденциальность информации за традиционной технологией с использованием распечаток на бумажном носителе электронных учетных карточек и описей документов; обязательный учет местонахождения и движения всех электронных документов, находящихся как в ЭВМ, так и на магнитных носителях вне ЭВМ, и др.

Технология информационная защищенная — совокупность комплексных технологических систем, организационных структур, ограничительных методов и технических средств, предназначенных для традиционной и (или) автоматизированной обработки конфиденциальной информации и документов, решающих задачи информационного обеспечения управленческой и производственной деятельности в жестких условиях информационной безопасности обрабатываемых информационных ресурсов.

У

Увольнение сотрудников, обладающих конфиденциальной информацией — процедура, имеющая ряд особенностей, связанных с необходимостью получения определенных гарантий, что увольняемое лицо не будет разглашать информацию, к которой имело доступ, или не будет использовать ее в своих целях. К этим особенностям можно отнести: проверку наличия и сдачи по описи всех числящихся за увольняемым лицом документов, дел и носителей информации, собеседование увольняемого лица с сотрудником службы безопасности или службы персонала по обязательствам, связанным с сохранением тайны фирмы, подписание этим лицом обязательства о неразглашении конфиденциальных сведений после увольнения. До истечения срока конфиденциальности сведений, с которыми работал уволившийся сотрудник, его деятельность в другой фирме находится под контролем службы безопасности.

Угроза безопасности конфиденциальной информации — единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы конфиденциальной информации создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию. Причиной, способствующей наступлению неблагоприятных для информации событий или возникновению дестабилизирующих воздействий (опасностей), является выявленная злоумышленником уязвимость интересующей его ценной информации.

Подобные события, воздействия возникают случайно или преднамеренно при наличии санкционированного или несанкционированного канала доступа к конфиденциальной информации. Основными угрозами безопасности информации можно назвать следующие: несанкционированный доступ, противоправное использование, модификация, уничтожение, подмена, фальсификация, гибель или порча документов при стихийном бедствии и др.

Уничтожение документов, дел и носителей информации — комплекс технологических приемов и правил, исключающих возможность ознакомления посторонних лиц с уничтожаемыми конфиденциальными материалами или подмены материалов. Указанный порядок предусматривает: коллегиальность принятия решения об уничтожении документов и самого процесса уничтожения; документирование (актирование) подготовки к уничтожению и уничтожения документов; внесение комиссией отметок об уничтожении в акт и учетные формы только после фактического уничтожения документов. Чистые носители информации, а также носители, содержащие черновики и проекты документов, испорченные носители уничтожаются без составления акта.

Установление грифа конфиденциальности — этап стадии исполнения конфиденциалыюго документа на любом носителе. В наибольшей безопасности находится информация, не зафиксированная (недокументированная) на каком-либо носителе. Угрозы информации появляются как только возникает мысль о необходимости ее документирования. В связи с этим система защиты должна начинать функционировать не после издания конфиденциального документа, а заблаговременно, т.е. до момента нанесения на чистый лист бумаги первых письменных знаков текста будущего документа. Для реализации мысли о создании документа решаются вопросы: является ли данная информация конфиденциальной и, если является, то какой уровень грифа ограничения доступа к ней персонала должен быть ей присвоен. Своевременное установление грифа ограничения доступа позволяет обеспечить относительно надежную защиту документированной информации. В основе установления уровня грифа конфиденциальности лежат перечни конфиденциальных сведений и конфиденциальных документов фирмы, требования партнеров по работе. Система грифования (маркирования) документов не гарантирует сохранность носителя и конфиденциальность информации, однако позволяет четко организовать технологию работу с документами и, в частности, сформировать разрешительную систему доступа к документам персонала.

Утечка конфиденциальной информации — неконтролируемый выход конфиденциальной информации за пределы фирмы или охраняемой зоны. Связана с возможным перехватом информации злоумышленником с помощью технических средств разведки (см. Средства несанкционированного доступа к информации), формированием технических каналов утечки информации.

Утрата информацией конфиденциальности — переход информации в категорию общедоступной, известной конкуренту, информации открытого доступа. Санкционированной может быть только одна причина — снятие с традиционного или электронного документа грифа конфиденциальности в соответствии с установленными в фирме правилами. Несанкционированных причин может быть несколько, но все они являются следствием утраты конфиденциальности информации.

Утрата конфиденциального документа, носителя — безвозвратное несанкционированное исчезновение, не восстанавливаемое повреждение или гибель документа, дела, базы данных, файла, любого типа носителя, содержащих конфиденциальную информацию, происшедшие в результате экстремальной ситуации или случайной причины (ошибочных действий персонала при работе с ЭВМ, ошибочного уничтожения документа, дела и др.). Утрата может быть спровоцирована злоумышленником (введение в заблуждение сотрудника фирмы, кража, уничтожение, подмена документа и др.). В результате ошибочных действий персонала злоумышленник может получить доступ к нужному ему документу, носителю или делу. Утрата документа, носителя в большинстве случаев приводит к утрате информацией конфиденциальности.

Утрата конфиденциальной информации — результат безответственных действий персонала (опубликование конфиденциальных сведений, включение этих сведений в открытый документ, их разглашение и др.), нарушения разрешительной системы доступа к. конфиденциальной информации (переход конфиденциальной информации к лицу, не имеющему права владения ею, и др.), утраты документа, носителя или их временного нахождения у постороннего лица, их копирования, целенаправленных действий злоумышленника (провоцирование персонала на ошибочные или безответственные

действия, получение информации от сообщника — сотрудника фирмы, перехват информации, предаваемой по незащищенным каналам связи, и др.). Опасность утраты конфиденциальной информации наблюдается на всех стадиях и этапах движения документов, при выполнении любых управленческих и технологических процедур и операций. Утрата конфиденциальной информации всегда приводит к утрате информацией конфиденциальности.

Учет архивных документов — установление количества и состава архивных документов в единицах учета и фиксация принадлежности каждой единицы учета к определенному комплексу и общему их количеству в учетных документах.

Учет инвентарный — фиксирование состава и сведений о конфиденциальной технической документации, сброшюрованных документах, документах выделенного хранения и других документах на любом носителе и не включаемых в номенклатуру дел. В предпринимательских структурах на инвентарный (списочный, перечневый) учет, как правило, ставятся носители информации (документы предварительного учета), а также законченные производством дела, учетные журналы и картотеки. Журнал или картотека инвентарного учета ведутся на протяжении нескольких лет. Инвентарный номер проставляется на деле, носителе, альбоме и др. в правом верхнем углу обложки, титульного листа, футляра, оболочки.

Учет конфиденциальных документов — фиксирование исходных и рабочих сведений о документе, его комплектности и целостности всех элементов, контроле местонахождения документов и доступа к ним персонала, проверке реального наличия документов и результатов аналитической работы по осведомленности персонала с содержанием документов. Учет конфиденциальных документов всегда ведется централизованно в службе конфиденциальной документации и включает следующие процедуры: индексирование документов, первичная регистрация исходных сведений о документе, формирование картотек, ежедневная проверка правильности регистрации документов и их наличия. В предпринимательских структурах целесообразно вести следующие виды учета конфиденциальных документов и дел: учет пакетов (конвертов), содержащих конфиденциальные ^ документы, а также учет поступления Незаконвертованных документов, документов, поступивших по телеграфной, электронной почте и факсимильной связи с грифом конфиденциальности (пакетный учет); пакетный учет документов, не имеющих грифа конфиденциальности, но отнесенных с документам ограниченного доступа в перечне конфиденциальных документов данной фирмы; учет поступивших (входящих, входных) документов; учет подготовленных отправляемых и внутренних документов; инвентарный учет; номенклатурный учет дел (см. Номенклатура конфиденциальных дел). Учет конфиденциальных документов может быть традиционным (журнальным, карточным) и автоматизированным.

Учет местонахождения документа — обязательное требование к ведению справочно-информационного банка данных по документам, обеспечивающее постоянный контроль наличия документа и позволяющее последовательно фиксировать фамилии сотрудников, несущих персональную ответственность за сохранность носителя и конфиденциальность информации. Отметка о местонахождении документа ставится в контрольном журнале или на втором экземпляре учетной карточки документа (см. Учетные формы конфиденциальных документов). Отметка содержит дату и фамилию исполнителя или работника служим конфиденциальной документации, который расписался в учетной форме за no-is лучение документа.

Учет носителей конфиденциальной информации, документов предварительного учета — см. Оформление и учет носителей конфиденциальной информации.

Учет осведомленности сотрудника в тайне фирмы — фиксирование каждого обращения к конфиденциальному документу, ознакомления с ним сотрудника в любой форме (в том числе случайное, несанкционированное). Отражается в учетной карточке документа и на самом документе в виде соответствующей отметки и росписи лица, обращавшегося к документу. Этот факт указывается также в карточке учета осведомленности сотрудника втайне фирмы. По факту несанкционированного ознакомления с документом проводится служебное расследование.

Учет пакетов, конвертов («пакетный учет») — фиксирование сведений о составе поступивших пакетов с документами. Обеспечивает контроль сохранности, целостности и комплектности документов; документированное удостоверение факта получения пакета с конфиденциальным документом от службы доставки с целью предотвращения утраты

документа после вскрытия пакета; формирование исходной учетной базы для последующей регистрации поступившего документа и стадий его движения; контроль соответствия количества поступивших документов количеству документов, переданных на регистрацию; установление связи исходящего номера поступившего документа с его регистрационным номером и номером в передаточной учетной форме; предотвращение утраты частей документа за счет неполного изъятия документа из пакета; исключение возможности ознакомления работников службы конфиденциальной документации с документами, составляющими особую ценность или имеющими помету «Лично»; установление возможного факта несанкционированного вскрытия пакета на пути его следования до адресата; обеспечение проверки наличия документов, зарегистрированных в журнале (описи) учета пакетов. В журнал (опись) учета пакетов вносятся также незаконвертованные и электронные документы с целью решения указанных выше задач. При работе с пакетами выполняются следующие процедуры: прием пакетов, учет пакетов, распределение по участкам службы конфиденциальной документации, вскрытие пакетов и изъятие конфиденциальных документов, выделение конфиденциальных документов из общего потока неконфиденциальных документов, внесение этих документов в журнал учета пакетов, закрытие журнала учета пакетов.

Учет подготовленных документов — см. Изготовление конфиденциального документа.

Учет поступивших документов — фиксирование сведений о каждом поступившем документе на любом носителе. Технологически тесно связан с учетом поступивших пакетов и незаконвертованных документов. Учету подлежат все зарегистрированные в журнале (описи) учета пакетов конфиденциальные документы независимо от предполагаемого срока (периода) их конфиденциальности. Технология традиционного и автоматизированного учета мало отличается от аналогичной технологии регистрации открытых документов. При вводе в автоматизированный банк данных реквизитов и текста конфиденциального документа дополнительно выполняются следующие процедуры: изготовление на учтенном носителе страховой и резервной копий документа; обозначение на бумажном документе или сопроводительном письме к машиноориентированному документу (дискете и т.п.) отметки о вводе документа в базу данных с указанием его учетного номера; подшивка бумажного документа вдело в соответствии с номенклатурой дел службы конфиденциальной документации и помещение страховой или резервной дискеты (в том числе поступившей дискеты) в ячейку места хранения.

Учетные формы конфиденциальных документов — журнальные (перечневые, списочные), карточные, формы в виде инвентарных описей документов, номенклатур. Могут изготовляться на бумажном, картонном носителе или быть в электронном виде и высвечиваться на экране дисплея. В учетных формах фиксируются факты регистрации исходных сведений о документе, факты переноса информации с бумажного носителя на магнитный, факты регистрации рабочих сведений о документе, факты изменения местонахождения документа и др. Учетные формы должны отражать весь «жизненный цикл» документа в данной фирме. Особенностью карточных учетных форм конфиденциальных документов является необходимость постоянного контроля их сохранности. С этой целью факт заполнения карточки фиксируется в специальном контрольном журнале, в котором указывается номер карточки и отражается динамика изменения местонахождения документа (см. Учет местонахождения документа). В целях исключения из технологии учета журнальной формы может заполняться на документ второй экземпляр карточки, который помещается в валовую (нумерационную) картотеку и выполняет функцию контрольного журнала (см. Картотека учетная). Помимо основных существуют также промежуточные (рабочие) учетные формы — передаточный журнал для регистрации факта передачи документа и его карточки с одного участка на другой службы конфиденциальной документации, внутренняя опись документов, находящихся у исполнителя, карточка учета выдачи документа, карточка разрешения и учета выдачи дела и др. При автоматизированном учете ведутся учетные описи документов или электронных учетных карточек, хранящихся в массивах или на магнитных носителях.

Уязвимость информации — объективное свойство информации подвергаться различного рода воздействиям (опасностям, угрозам), нарушающим ее целостность, достоверность и конфиденциальность. Воздействия носят дестабилизирующий по отношению к информации характер и приводят к утрате носителя конфиденциальной информации или утрате конфиденциальности информации. Уровень уязвимости информации находится в прямой

зависимости от степени совершенства применяемой в фирме системы защиты информации, перекрытия этой системой всей сферы возможных угроз и предполагаемых каналов несанкционированного доступа к информации.

Ф

Фальсификация документов — изготовление и использование в каких-либо целях ложного документа, в том числе злоумышленной подмены подлинного документа в целом или его отдельных частей поддельными, изготовленными для приобретения незаконных прав, выполнения противоправных действий в отношении фирмы или ее персонала. К фальсифицированным относятся также так называемые фиктивные документы — документы, не существующие в подлинном виде (финансовые и банковские документы, контракты и др.). При невнимательных или безответственных действиях персонала эти документы принимаются как подлинники. Фальсификация может быть частичной, например подмена в документе отдельных листов с изменением текста, исправление дат, подделка подписи, печати, допечатывание фиктивного текста перед подписью руководителя. Частичная фальсификация выполняется путем подчистки существующих сведений и впечатывания (вписывания) новых, исправления сведений с помощью корректирующей жидкости, использования копировальной техники и другими способами. При фальсификации документов часто используются подлинные бланки документов, организационная техника фирмы, подлинные печати и штампы. Фиктивные документы иногда имеют подлинную подпись руководителя, которая была поставлена в результате его невнимательности или введения в заблуждение.

Формирование конфиденциальных дел — комплектование документов в дела в соответствии с их систематизацией в номенклатуре конфиденциальных дел. Осуществляется всегда централизованно в службе конфиденциальной документации. Формирование и хранение дел с конфиденциальными документами (конфиденциальных дел) на рабочих местах сотрудников фирмы не разрешается. При формировании конфиденциальных документов в дела должна соблюдаться разрешительная система доступа персонала к делам, документам и электронной информации, обеспечиваться взаимосвязь местонахождения документа в деле с его предыдущими учетными формами и номерами, строго выполняться инструктивные требования по обеспечению сохранности дел и документов. Дело (том) может быть закрыто только после исполнения и подшивки в него всех документов, относящихся к данному делу и году. В дело включаются только конфиденциальные документы. После снятия грифа конфиденциальности документ перемещается в аналогичное по заголовку дело открытого доступа. При этом нумерация листов дела сохраняется, но отсутствующие листы оговариваются во внутренней описи конфиденциальных документов дела с указанием причины изъятия документа и его нового местонахождения. Такая же отметка делается в учетной форме документа. Аналогичным образом осуществляется изъятие электронного документа из архивного массива компьютера службы конфиденциальной документации. После изъятия из дела последнего документа, с которого снят гриф конфиденциальности, обложка дела с описью документов продолжает храниться на протяжении указанного в номенклатуре срока и затем уничтожается. Отметка об уничтожении вносится в номенклатуру дел соответствующего года.

Формуляр документа — набор реквизитов официального письменного документа, расположенных в определенной последовательности.

Формуляр-образец — модель построения документа, устанавливающая область применения, форматы, размеры полей, требования к построению конструкционной сетки и основные реквизиты.

Х

Хранение конфиденциальных документов и дел — нахождение документов и дел в специальном хранилище, обеспечивающем их сохранность. Осуществляется службой конфиденциальной документации в отношении неисполненных и исполненных документов. Документы хранятся в папках, на которых указывается их целевое назначение: фамилии сотрудников фирмы, которым направляются документы, или наименование предстоящих действий, процедур и операций (подшивка вдело, отправление и т.п.). Каждая папка должна иметь опись находящихся в ней документов. Хранить документы в россыпи в ящиках столов, в шкафах и сейфах не допускается. Аналогичным образом хранят неисполненные документы в рабочее время сотрудники фирмы. По окончании рабочего дня они должны все документы сдать в службу конфиденциальной документации. Текущие и

архивные конфиденциальные дела хранятся в службе конфиденциальной документации и при необходимости выдаются исполнителям. Выдача дел фиксируется в учетной карточке разрешений и выдачи. Дела хранятся в сейфах, металлических шкафах, которые всегда должны быть заперты. На внутренней стороне дверцы шкафа, сейфа должна быть наклеена опись хранимых архивных дел или номенклатура дел текущего года с указанием расположения дел на каждой полке и очередностью эвакуации дел при экстремальных ситуациях. Дела располагаются в последовательности их нумерации. Магнитные носители хранятся по тому же принципу в вертикальном положении, в футлярах и специальных ячейках.

Ш

Шифр — совокупность условных знаков для преобразования информации в вид, исключающий ее восстановление (дешифрование и прочтение) в условиях отсутствия у злоумышленника ключа для раскрытия шифра.

Шифрование — криптографическое (математическое, алгоритмическое) преобразование информации с целью получения шифрованного текста или устной речи (см. также Криптография).

Шпионаж — похищение, добывание, собирание и передача с целью корыстного использования или выдачи конкуренту (противнику) сведений, составляющих тайну.

Шпионаж промышленный — получение предпринимателем самостоятельно или с помощью соответствующих специалистов (злоумышленников), обманным или иным незаконным путем конфиденциальной информации с целью овладения ею для достижения технического, технологического или коммерческого преимущества, банкротства конкурента. Экономическая сущность промышленного шпионажа — экономия средств на разработку новой идеи, продукции, за счет кражи нужной информации у конкурента. Один из основных видов недобросовестной конкуренции.

Шпионаж экономический — широкое понятие, которое охватывает такие виды шпионажа, как промышленный, коммерческий, научно-технический, производственный и др. Его результат — получение экономическим сообществом приоритетных позиций в сферах производства, банковского дела, торговли, управления рынком товаров и услуг.

Э

Экспертиза ценности документов — отбор документов на государственное хранение или установление сроков хранения на основе принятых критериев.

Экстремальная (чрезвычайная) ситуация — явление, событие, нарушающее нормальное функционирование фирмы, работу персонала, создающее опасность для целостности и сохранности здания, помещений, оборудования и документации фирмы, угрожающее жизни и здоровью сотрудников. Экстремальные ситуации объективного характера связаны со стихийными бедствиями (ураганами, наводнениями и др.), неуправляемыми процессами, военными действиями, кризисами, авариями энергоснабжения и водоснабжения и другими подобными событиями. Экстремальные ситуации могут быть случайного (фатального) характера — возгорание оборудования и коммуникаций, разрушение конструкций, а также связаны с неосторожностью и безответственностью персонала (возгорания от неосторожного обращения с огнем, курения на рабочих местах, неумелой эксплуатации оборудования и др.). Субъективный характер носят экстремальные ситуации, которые умышленно спровоцированы злоумышленником или его сообщником: поджег, взрыв, задымление помещений, организация паники, силовое вооруженное проникновение в здание криминальных элементов и др. В отношении отдельных сотрудников фирмы также могут быть организованы злоумышленные действия, включающие: шантаж, взятие в заложники, физическое или психическое воздействия, кражи близких родственников и др. Локализация и ликвидация экстремальных ситуаций осуществляется правоохранительными органами, службами экстремальной помощи при содействии руководства фирмы и службы безопасности (см. также Действия персонала в экстремальных ситуациях). Ликвидация экстремальных ситуаций только сотрудниками фирмы не допускается, так как эта работа требует специальных знаний и умений.

Ю

Юридическая сила документа — свойство официального документа, сообщаемое ему действующим законодательством, компетенцией издавшего его органа и установленным порядком оформления. Предполагает наличие в документе основных реквизитов (обозначения автора, вида документа, его даты, текста), а также наличие для данного вида документа состава удостоверения его подлинности — подписи, грифов утверждения

или согласования, виз, печати, отметки о заверении копии).

ОСНОВНЫЕ ОПЕРАЦИОННЫЕ ТЕХНОЛОГИЧЕСКИЕ СХЕМЫ ОБРАБОТКИ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ

1. Прием, первичная обработка, предварительное рассмотрение и распределение поступивших документов

Процедура приема пакетов:

а) получение от курьера пакетов (или незаконвертованного документа) и сдаточного документа (реестра, разностного журнала, расписки и т.п.);

б) проверка правильности доставки пакетов и целостности упаковки, печатей и наклеек;

в) проверка соответствия содержания реквизитов на пакете и в сдаточном документе;

г) подсчет количества принятых пакетов;

д) проставление в сдаточном документе отметки о приеме пакетов.

Процедура учета пакетов:

а) внесение в журнал учета пакетов (пакетно-контрольный журнал) сведений о количестве поступивших пакетов и проставление росписи курьера, доставившего пакеты, с удостоверением росписи штампом службы доставки;

б) возвращение курьеру экземпляра сдаточного документа;

в) внесение в журнал по каждому поступившему пакету исходных сведений о вложенных в него документах (или исходных сведений о незаконвертованном документе).

Процедура распределения и вскрытия пакетов:

а) передача по принадлежности пакетов, не подлежащих вскрытию на входящем участке;

б) передача пакетов для вскрытия руководителю службы документации или уполномоченному лицу;

в) вскрытие пакетов, конвертов;

г) проверка соответствия содержания реквизитов на пакете и в документе, подсчет количества листов;

д) проверка наличия приложений (если они имеются), их комплектности и соответствия содержания их реквизитов и количества листов данным, указанным в сопроводительном письме;

е) скрепление листов документа и передача его на регистрацию, в том числе на другие участки службы документации.

Процедура закрытия журнала учета пакетов:

а) проставление учетных входящих номеров поступивших документов в журнале учета пакетов;

б) проставление ежедневной итоговой записи об общем количестве зарегистрированных документов в журнале учета пакетов.

Процедура выделения ценных и конфиденциальных документов фирмы:

а) просмотр всех документов входного потока, не имеющих грифа обозначения ценности или конфиденциальности (бумажных, машиночитаемых, электронных, факсимильных и др.);

б) сравнение содержания (темы) поступивших документов с перечнем сведений, работ и документов фирмы, подлежащих защите;

в) проставление на выделенных документах грифа ограничения доступа или обозначения ценности, указанного в перечне;

г) внесение в журнал учета пакетов исходных сведений о выделенных документах.

2. Традиционный учет поступивших документов и формирование справочно-информационного банка данных по документам

Процедура индексирования документов:

а) проставление входящего штампа на основном документе и приложениях, на документах, присланных во временное пользование, на сопроводительном письме к магнитному носителю информации (дискете, диску и т.п.);

б) определение входящего номера документа: при журнальной и карточной регистрации документов (внесение отметки в контрольный журнал);

в) проставление во входящем штампе номера документа, даты и количества листов;

г) проставление регистрационных сведений в приложениях;

д) проставление входящего номера документа в журнале учета пакетов (пакетно-контрольном журнале);

е) добавление к входящему номеру идентифицирующего индекса (номера дела по номенклатуре).

Процедура первичной регистрации исходных сведений о документе:

а) заполнение граф журнала учета (или описи) поступивших документов или заполнение учетной карточки (при заполнении описи — внесение исходных сведений в регистрационно-контрольную карточку открытых документов для обеспечения справочной картотеки);
б) проверка соответствия исходных данных в журнале или карточке, контрольном журнале и на документе;
в) проставление в журнале учета пакетов отметки о возврате документа, зарегистрированного за исходящим номером, внесение отметки в регистрационную карточку документа;
г) проверка правильности регистрации документов, переданных по журналу учета пакетов на другие участки службы документации, внесение в журнал номеров этих документов и количества листов;
д) подкалывание учетной карточки входящего учета к документу.

Процедура формирования картотек:

а) распределение карточек по картотекам;
б) внесение отметки о местонахождении документа в контрольный журнал;
в) фиксирование в карточке росписи за получение документа;
г) помещение карточки в картотеку;
д) поиск сведений о документах и выдача ответов на запросы по документам;
е) ведение (актуализация) картотеки.

Процедура ежедневной проверки правильности регистрации документов и их наличия:

а) подсчет и сравнение количества полученных и зарегистрированных документов;
б) проставление в журнале учета пакетов отметки о правильности закрытия всех позиций, итоговой записи;
в) проверка правильности регистрации каждого документа;
г) проверка правильности закрытия всех позиций в журнале учета пакетов, наличия двух росписей за документы, переданные на другие участки службы документации;
д) проверка правильности внесения отметок о возвращенных документах;
е) проверка правильности внесения отметок по документам, присланным во временное пользование и не взятых на входящий учет;
ж) проверка наличия документов по незакрытым позициям журнала учета пакетов;
з) проставление штампа проверки под итоговой записью;
и) проверка полноты изъятия документов из пакетов и уничтожение пакетов.

3. Автоматизированный учет поступивших документов и формирование справочно-информационного банка данных по документам

Процедура подготовки поступивших документов к вводу в ЭВМ:

а) внесение исходящих номеров поступивших документов в журнал учета работы ЭВМ (традиционный или электронный машинный журнал, протокол) из журнала учета пакетов (пакетно-контрольного журнала) с указанием даты и росписи оператора ЭВМ службы конфиденциальной документации;
б) проставление на бумажных документах (в том числе сопроводительных письмах) штампа отметки для автоматического поиска документа;
в) проставление на бумажных документах, подлежащих переносу на машинный носитель, а также в сопроводительных письмах к документам, записанным на дискете, штампа (надписи) для внесения в них в дальнейшем необходимых сведений;
г) регистрация магнитного носителя при поступлении документа, записанного на дискете;
д) распределение документов на группы в соответствии с уровнем их конфиденциальности и другим признаком ограничения доступа для раздельного ввода в ЭВМ;
е) формирование составных частей поискового (учетного) индекса документа;
ж) получение указания администратора банка данных службы конфиденциальной документации, в какую часть рабочего массива вводить данный документ (директорию, файл).

Процедура ввода исходных сведений о поступивших документах в автоматизированный банк данных:

а) вывод на экран чистой матрицы учетной карточки документа за очередным (повторно не воспроизводимым) порядковым номером, внесение индекса документа;
б) заполнение на экране с бумажного документа зон и граф матрицы учетной карточки;

в) автоматическое (или с помощью клавиатуры) заполнение учетной карточки на электронный документ, записанный на дискете или поступивший по защищенной линии электронной почты;
г) внесение в учетную карточку документа учетных номеров и даты регистрации машинных носителей (диска, дискет и т.п.), на которых записаны исходные сведения о документе;
д) автоматическое внесение необходимых сведений в электронную валовую опись конфиденциальных документов и (или) электронную опись (контрольный журнал) учетных карточек документов, проверка правильности внесенных сведений;
е) рукописное или автоматическое внесение в машинный журнал (протокол) отметки о заполнении комплекта электронных учетных форм, заверенную росписью оператора;
ж) внесение в журнал учета пакетов номеров зарегистрированных документов, заверение отметки росписью оператора;
з) проставление на бумажном документе необходимых сведений во входящем штампе основного документа (или сопроводительного письма) и на приложениях, а также в штампе отметки для автоматического поиска документа;
и) ввод в электронный документ, поступивший по линии электронной почты, указанных выше сведений;
к) контроль правильности внесенных сведений;
л) помещение поступивших бумажных документов и электронных на дискете в рабочую папку сотрудника участка, возвращение электронных документов, поступивших по линии электронной почты, в предварительный массив компьютера участка.

Процедура ввода в автоматизированный банк данных электронных документов и аналогов бумажных документов:

а) выполнение всех операций процедуры 2, внесение соответствующей записи в машинный журнал (протокол), учитывая, что сведения о документах, поступивших по линии электронной почты, факсу и т.п., также внесены в журнал учета пакетов и машинный журнал;
б) ввод документа (в том числе и сопроводительного письма) на бумажной основе или записанного на дискете в соответствующий рабочий массив с помощью технических средств, перенос электронного документа, поступившего по линии связи, из специального предварительного массива в рабочий массив;
в) проставление на каждом листе электронного документа грифа конфиденциальности и учетного номера документа, электронной подписи (или ежедневного кода) оператора и даты ввода документа в рабочий массив;
г) автоматическое (или с помощью клавиатуры) внесение данных о местонахождении документа в электронную учетную карточку документа и электронную опись документов или учетных карточек с указанием его адреса в массиве и номеров машинных носителей (дисков, дискет и т.п.), проставление электронной подписи оператора;
д) контроль автоматического внесения сведений о вновь поступивших документах в электронную опись рабочего массива электронных документов, находящихся в базе данных компьютера участка, и учетную карточку (опись документов) соответствующего машинного носителя; допечатка информации и проставление росписи в бумажном экземпляре учетной карточки носителя;
е) контроль правильности внесения документа в рабочий массив и фактического наличия его на машинном носителе в полном объеме и целостности, закрытие документа от несанкционированного доступа;
ж) изготовление на учтенной дискете страховой копии документа, поступившего полиции электронной почты, внесение соответствующей записи и росписей в электронный и бумажный экземпляры учетной карточки (описи) носителя;
з) обозначение на бумажном документе или сопроводительном письме к дискете отметки о вводе документа в базу данных с указанием его учетного (поискового) номера;
и) подшивка бумажного документа в дело в соответствии с номенклатурой дел службы конфиденциальной документации и помещение страховой дискеты в ячейку места хранения;
к) внесение в машинный журнал (протокол) сведений о выполненных операциях, проставление росписи оператора;
л) передача электронных документов на компьютер (сервер) администратора банка данных службы конфиденциальной документации под роспись администратора в машинном

журнале оператора (для внесения отметок о доступе к документу персонала и проведения других операций по закрытию информации, регистрация действий в рабочем журнале администратора);
м) фиксирование в электронной учетной карточке письменного указания начальника службы конфиденциальной документации администратору банка данных о дальнейшем движении документа;
и) внесение в машинный журнал (протокол) администратора сведений о выполненных операциях, проставление росписи администратора.

Процедура распечатки на бумажном носителе учетных сведений о поступивших документах:

а) выполнение технических операций по распечатке (изготовлению машинограмм): бумажного аналога (экземпляра) электронной учетной (страховой) карточки документа со всеми отметками и при необходимости в зависимости от принятой технологии — карточки выдачи документа и ежедневной части описи зарегистрированных поступивших документов;
б) подтверждение подлинности бумажного экземпляра электронной карточки росписью на ней руководителя участка с проставлением печати службы конфиденциальной документации и даты;
в) внесение отметок о производстве распечаток в электронную учетную карточку документа с указанием даты и электронной подписи оператора;
г) включение бумажного экземпляра электрон ной учетной карточки документа в валовую (страховую) картотеку;
д) внесение в машинный журнал (протокол) сведений о выполненных операциях, проставление росписи оператора.

Процедура ежедневной проверки правильности регистрации документов и их наличия:

а) подсчет количества поступивших и зарегистрированных документов;
б) проверка закрытия всех позиций журнала учета пакетов, проставление в журнале росписи второго сотрудника участка;
в) проверка соответствия записей в журнале учета пакетов и машинном журнале (протоколе), проставление в машинном журнале росписи второго сотрудника участка;
г) проверка правильности заполнения и полноты включения исходных сведений о документах во все электронные описи и учетные карточки, проставление в формах электронной подписи второго сотрудника участка;
д) проверка фактического наличия всех зарегистрированных документов в рабочих массивах и на машинных носителях, проверка полноты, комплектности и целостности всех элементов документа, наличия необходимых отметок, защитных меток, проставление электронной подписи второго сотрудника в опись рабочего массива компьютера участка и электронной учетной карточке каждого машинного носителя.

4. Оформление и учет носителей конфиденциальной информации

Процедура первичного оформления носителя:

а) нумерация листов, прошивка и опечатывание носителя;
б) выполнение специфических операций по оформлению каждого вида носителя;
в) проставление регистрационного штампа предварительного учета и количества листов, грифа конфиденциальности;
г) внесение заверительных надписей;
д) проверка целостности и качества технических носителей информации, надежности их заводской упаковки;
е) перемотка ленточных носителей на рабочие кассеты, установление точной длины ленты и отсутствия повреждений, склеек, закрытие и опечатывание кассеты.

Процедура традиционной или автоматизированной регистрации носителей:

Традиционная регистрация носителей:

а) заполнение на носителе строки в журнале регистрации и учета движения карточек (контрольном журнале) или внесение исходных сведений о носителе в журнал учета носителей;
б) внесение исходных сведений о носителе в учетную карточку;
в) подкалывание карточки к носителю.

Автоматизированная регистрация носителей:

а) заполнение на экране карточки учета и выдачи носителя за очередным Порядковым номером (для магнитных носителей карточка одновременно выполняет функцию описи

документов, записанных на носителе), иногда в зависимости от принятой технологии — автоматическое заполнение дополнительной карточки учета выдачи носителя;
б) проверка правильности и полноты заполнения карточки;
в) автоматическое внесение новых сведений в электронную опись носителей или электронную опись (контрольный журнал) учета движения карточек, проверка правильности внесенной записи;
г) перенесение на регистрируемый магнитный носитель копии электронной учетной карточки для ведения описи записанных документов;
д) распечатка на принтере электронной учетной карточки носителя (для страховой валовой картотеки), распечатка для магнитного носителя второго, дополнительного экземпляра бумажного аналога карточки для выдачи исполнителю вместе с носителем;
е) внесение отметки о распечатке бумажного экземпляра в электронную учетную карточку носителя;
ж) подтверждение подлинности бумажных экземпляров электронной карточки росписью руководителя участка с проставлением печати и даты;
з) изготовление (при необходимости) страховых и резервных экземпляров магнитного носителя с внесением соответствующих записей в электронный и бумажные экземпляры учетной карточки основного носителя;
и) внесение в машинный журнал (протокол) сведений о выполненных операциях, проставление росписи сотрудника участка.

Процедура окончательного оформления носителя:

а) проставление в штампе предварительного учета на носителе регистрационного номера;
б) проставление регистрационного номера на всех листах носителя;
в) маркировка технического носителя (проставление регистрационного номера, окрашивание элементов, скрепляющих корпус технического носителя).

Процедура выдачи документов предварительного учета исполнителям:

При традиционной регистрации носителя:

а) проверка правильности оформления носителя и соответствия учетных данных в журнале (карточке) и на носителе;
б) заполнение соответствующих граф в журнале или учетной карточке или карточке учета выдачи;
в) проверка исполнителем правильности оформления носителя и записей в учетной форме;
г) внесение отметки о выдаче носителя (его местонахождении) в журнал;
регистрации и учета движения карточек;
д) выдача носителя исполнителю под роспись в заполненной учетной форме;
е) постановка учетной карточки в картотеку «За исполнителями»;
ж) внесение исполнителем сведений о носителе во внутреннюю опись документов, находящихся у исполнителя.

При автоматизированной регистрации носителя:

а) поиск и вывод на экран дисплея учетной карточки носителя;
б) проверка правильности оформления носителя и соответствия учетных данных в карточке и на носителе;
в) заполнение соответствующих граф электронной учетной карточки о выдаче носителя;
г) допечатка на принтере указанных сведений в бумажных экземплярах электронной учетной карточки и карточке учета выдачи носителя (в зависимости от принятой технологии) и заверение их росписью сотрудника участка;
д) проверка исполнителем правильности оформления носителя и записей в учетных формах;
е) автоматическое внесение в электронную опись носителей, зарегистрированных на участке, или электронную опись учета движения учетных карточек фамилии исполнителя, который расписался за получение документа;
ж) автоматическое внесение сведений о носителе в электронную опись документов, дел и носителей, выданных конкретным исполнителям на данном участке службы конфиденциальной документации (здесь и далее — при необходимости, в зависимости от принятой технологии); допечатка на принтере в традиционной внутренней описи документов, находящихся у исполнителя, строки с исходными сведениями о выданном носителе; возвращение внутренней описи исполнителю;

з) выдача носителя исполнителю под роспись в бумажном экземпляре электронной учетной карточки; выдача магнитного носителя вместе со вторым бумажным экземпляром его учетной карточки;
и) постановка оставшегося на участке бумажного экземпляра электронной учетной карточки носителя в страховую картотеку; постановка карточки учета выдачи носителя (если она предусмотрена технологией) в картотеку «За исполнителями»;
к) возвращение электронной учетной карточки в рабочий массив;
л) внесение в машинный журнал (протокол) сведений о выполненных операциях, проставление росписи оператора.

Процедура выдачи исполнителям дополнительных листов:

а) оформление (маркировка) дополнительных листов;
б) поиск традиционных или электронных учетных форм и их бумажных аналогов;
в) внесение сведений о дополнительных листах в традиционные или электронные учетные карточки основного носителя;
г) допечатка на принтере в бумажном экземпляре электронной учетной Карточки вновь внесенной информации и заверение внесенных сведений росписью сотрудника участка;
д) автоматическое внесение сведений о дополнительных листах в электронную опись носителей, выданных конкретным исполнителям; допечатка (или внесение самим исполнителем) в традиционную внутреннюю опись документов, находящихся у исполнителя, строки с исходными сведениями о дополнительных листах; возвращение внутренней описи исполнителю;
е) выдача дополнительных листов исполнителю под роспись в бумажном экземпляре учетной карточки или карточке учета выдачи;
ж) возвращение традиционной учетной карточки в картотеку «За исполнителями» или постановка бумажного экземпляра электронной учетной карточки носителя в страховую картотеку;
з) возвращение электронной учетной формы в рабочий массив;
и) внесение в машинный журнал (протокол) сведений о выполненных операциях, проставление росписи сотрудника участка.

Процедура приема от исполнителей документов предварительного учета:

При традиционной регистрации носителя:

а) поиск соответствующей записи в журнале или поиск карточки в картотеке «За исполнителями»;
б) сравнение исходных и рабочих записей в карточке и на носителе;
в) проверка количества листов носителя, отметок о списании листов в спецблокноте, количественных характеристик технических носителей;
г) проверка целостности всех листов, их сохранности (пролистывание носителя), осмотр технического носителя;
д) роспись сотрудника участка документов предварительного учета за прием носителя в учетной форме и внутренней описи исполнителя;
е) внесение отметки в журнал регистрации и учета движения учетных карточек о новом местонахождении носителя;
ж) помещение носителя и учетной формы в места их хранения.

При автоматизированной регистрации носителя:

а) поиск и вывод на экран дисплея учетной карточки носителя;
б) сравнение исходных и рабочих записей в электронной карточке-носителе;
в) проверка количества листов носителя, отметки о списании листов спецблокноте, количественных характеристик технических носителей;
г) проверка целостности всех листов, их сохранности (пролистывание носителя), осмотр технического носителя;
д) при приеме магнитного носителя информации — просмотр носителя на экране дисплея, внесение в электронную учетную карточку (опись документов) носителя (в том числе записанную на самом носителе) сведений, внесенных исполнителем в бумажный экземпляр учетной карточки, проверка реального наличия этих документов, допечатка этих сведений в страховой бумажный экземпляр карточки и проставление росписи в двух бумажных экземплярах карточки;
е) заполнение граф электронной учетной карточки о приеме носителя от исполнителя;
ж) автоматическое внесение в электронную опись носителей или электронную опись учета движения учетных карточек нового местонахождения носителя;

автоматическое внесение этой информации в электронную опись носителей, выданных конкретным исполнителям;
з) допечатка на принтере в бумажном экземпляре электронной учетной карточки отметки о приеме носителя, роспись сотрудника участка; допечатка отметки о приеме носителя во внутреннюю опись документов, находящихся у исполнителя, возвращение внутренней описи исполнителю;
и) помещение одного бумажного экземпляра электронной учетной карточки в страховую картотеку, другого — в футляр вместе с носителем;
к) возвращение электронной карточки в рабочий массив;
л) внесение в машинный журнал (протокол) сведений о выполненных операциях, проставление росписи сотрудника участка.

5. Изготовление конфиденциальных документов

Процедура приема черновика документа от исполнителя:

а) получение руководителем участка изготовления документов от исполнителя бумажного черновика или учтенной дискеты (с бумажным экземпляром учетной карточки — описи документов, записанных на носителе) с черновиком подготовленного документа или получение оформленного черновика по защищенной линии связи от компьютера исполнителя;
б) проверка наличия на черновике письменного разрешения на изготовление проекта документа, подписанного полномочным руководителем;
в) проверка реального наличия на магнитном носителе (дискете) черновика одного документа и соответствия его данным, указанным в бумажном экземпляре учетной карточки носителя, заверение соответствия росписями исполнителя и сотрудника участка;
г) проверка наличия всех реквизитов и частей документа, обозначения фамилии исполнителя;
д) подсчет количества листов черновика;
е) внесение отметки о получении носителя (рабочей или стенографической тетради, дискеты и т.п.) во внутреннюю опись документов, находящихся у исполнителя.

Процедура традиционной или автоматизированной регистрации черновика:

Традиционная регистрация проекта документа:

а) внесение исходных сведений о черновике в журнал учета черновиков и проектов документов;
б) резервирование машинописного номера (регистрационного номера этапа изготовления) проекта документа в контрольном журнале учета карточек подготовленных документов или определение этого номера по валовой картотеке учетных карточек (если на документ заполняется два экземпляра карточки); при использовании единой нумерации документов на участке изготовления и участке учета подготовленных документов — одновременное резервирование аналогичного номера в контрольном журнале участка учета подготовленных (изданных) документов;
в) проставление машинописного номера на титульном листе и (или) листах Черновика (в электронный черновик документа учетный номер вносится с клавиатуры ЭВМ или автоматически), на чистом бланке учетной карточки подготовленного документа и в журнале учета черновиков и проектов документов;
г) изъятие листов черновика из спецблокнота и фиксирование изъятия каждого листа на корешке или в контрольном листе спецблокнота;
д) возврат спецблокнота исполнителю;
е) вкладывание в черновик или подкалывание к листам черновика пронумерованной учетной карточки подготовленного документа;
ж) передача черновика документа для печати машинистке (оператору ЭВМ) под роспись в журнале учета черновиков и проектов документов.

Автоматизированная регистрация проекта документа:

а) заполнение на экране ЭВМ учетной карточки подготовленного документа и внесение в карточку очередного единого порядкового номера по участку изготовления и участку учета подготовленных (изданных) документов;
б) автоматическое внесение новых сведений в электронную опись (контрольный журнал) учетных карточек подготовленных документов, проверка правильности внесенной записи;
в) проставление машинописного номера на листах черновика;
г) изъятие листов из спецблокнота, оформление изъятия на корешке (или в контрольном

листе) спецблокйота, возвращение спецблокнота исполнителю;
д) распечатка на бумажном носителе страхового экземпляра учетной карточки подготовленного документа;
е) внесение отметки о распечатке в электронную учетную карточку документа;
ж) подтверждение подлинности бумажного экземпляра электронной карточки росписью руководителя участка изготовления документов с проставлением печати и даты;
з) передача черновика для печатания оператору ЭВМ под роспись в бумажном экземпляре электронной учетной карточки;
и) внесение в машинный журнал (протокол) сведений о выполненных операциях, проставление росписи руководителя участка изготовления документов.

Процедура печатания и выдачи проекта документа исполнителю:

При традиционной регистрации проекта документа:

а) заполнение необходимых граф пронумерованной учетной карточки подготовленного документа;
б) печатание на пишущей машинке или с помощью персональной ЭВМ текста и реквизитов документа с учетом требований государственного стандарта;
в) обозначение на нижнем поле напечатанного комплекта экземпляров каждого листа документа учетного (машинописного) номера;
г) обозначение на оборотной стороне последнего листа всех экземпляров документа учетного (машинописного) номера, грифа конфиденциальности, количества отпечатанных (изготовленных) экземпляров, при необходимости их целевого назначения, фамилии исполнителя, индекса машинистки (оператора) и даты печатания (изготовления) документа;
д) передача отпечатанного проекта документа, черновика и учетной карточки руководителю участка изготовления документов;
е) проверка правильности и комплектности отпечатанного проекта документа, его соответствия черновику;
ж) заполнение соответствующих граф в учетной карточке и роспись руководителя участка в карточке или журнале учета черновиков;
з) при изготовлении документа на дискете — внесение сведений о нем в электронный и бумажный экземпляры учетной карточки (описи документов) носителя, заверение записи в бумажном экземпляре карточки росписями руководителя участка и исполнителя; при необходимости изготовление страховой копии документа на другой дискете;
и) проверка исполнителем комплектности и правильности изготовления проекта документа, просмотр дискеты, если документ был изготовлен на этом носителе;
к) выдача исполнителю всех экземпляров проекта документа и черновика под роспись в учетной карточке подготовленного документа;
л) передача учетной карточки (и дискеты со страховой копией проекта документа) на участок изданных документов (исходящий участок);
м) при журнальной системе учета документов — передача отпечатанного проекта документа и черновика на исходящий участок для регистрации в журнале учета подготовленных документов;
и) при журнальной системе учета документов — выдача исполнителю отпечатанного проекта документа и черновика под роспись в журнале учета подготовленных документов на исходящем участке.

При автоматизированной регистрации проекта документа:

а) печатание бумажного документа, оформление специфических реквизитов или изготовление документа на учтенной дискете;
б) передача отпечатанного документа и черновика руководителю участка изготовления документов;
в) при поступлении от исполнителя дискеты с подготовленным проектом документа (без черновика) или передачи готового проекта документа по линии защищенной компьютерной связи — их регистрация руководителем участка (без перепечатывания) с заполнением указанных выше учетных форм;
г) проверка правильности и комплектности изготовленного проекта документа, его соответствия черновику;
д) заполнение соответствующих граф и зон электронного экземпляра учетной карточки подготовленного документа, проставление электронной подписи руководителя участка;
е) автоматическое внесение сведений об отпечатанном проекте документа в электронную

опись документов, выданных конкретным исполнителям;
допечатка на принтере строки о выданном проекте документа и черновике в традиционную внутреннюю опись документов, находящихся у исполнителя;
возвращение описи исполнителю;
ж) допечатка на принтере информации, внесенной в электронную учетную карточку, в бумажный экземпляр этой карточки, заверение внесенных сведений росписью руководителем участка;
з) если документ изготовлен на дискете — внесение сведений о нем в электронный экземпляр учетной карточки (описи документов) носителя, автоматическая допечатка на принтере внесенной записи в бумажный экземпляр этой описи, заверение записи росписями руководителя участка и исполнителя; при необходимости изготовление страховой копии документа на другой дискете;
и) выдача исполнителю изготовленного проекта документа и черновика под роспись в бумажном экземпляре электронной учетной карточки; проверка исполнителем состава полученных документов, просмотр дискеты;
к) выдача исполнителю магнитного носителя (дискеты), содержащего черновик документа, вместе с бумажным экземпляром учетной карточки носителя (описью) и допечатанной в карточке отметкой об изготовлении проекта документа;
л) выдача исполнителю проекта документа, изготовленного с бумажного носителя на дискете, аналогично указанным выше пунктам;
м) передача исполнителю изготовленного проекта документа и черновика или возвращение ему зарегистрированного проекта документа, полученных руководителем участка полиции защищенной компьютерной связи, осуществляется также по этой линии связи с предварительной передачей исполнителем своей электронной подписи, фиксированием ее в электронной учетной карточке передаваемого документа и автоматическим внесением соответствующей записи в электронную опись массива документов компьютера исполнителя;
и) передача бумажного экземпляра учетной карточки подготовленного документа и электронной карточки на участок изданных документов;
о) уничтожение в базе данных компьютера участка изготовления документов всех материалов по изготовлению данного документа и самого документа кроме записей в электронных описях;
п) внесение в машинный журнал (протокол) сведений о выполненных операциях, проставление росписи руководителя участка изготовления документов.

Процедура перепечатывания отдельных листов и документа в целом:

а) получение от исполнителя отдельных листов или документа в целом для перепечатывания;

б) получение с участка изданных документов традиционной учетной карточки или электронной (на дискете или по линии защищенной компьютерной связи) и бумажного экземпляра электронной учетной карточки подготовленного документа; внесение соответствующих отметок в карточки и опись, контрольный журнал;
в) внесение отметок в учетные формы о перепечатывании отдельных листов без изменения общего количества листов в документе;
г) внесение отметок в учетные формы о перепечатывании отдельных листов с изменением общего количества л истов в документе;
д) допечатка на принтере в бумажный экземпляр электронной учетной карточки соответствующих сведений, заверенных росписью руководителя участка изготовления документов;
е) заполнение новых учетных форм при полном перепечатывании документа;
ж) внесение дополнений и изменений в электронную опись документов, выданных конкретным исполнителям, допечатка необходимых сведений в традиционную внутреннюю опись документов, находящихся у исполнителя;
з) выдача отдельных листов и документа исполнителю под роспись в бумажном экземпляре электронной учетной карточки;
и) возвращение традиционной или электронной учетной карточки и ее бумажного аналога на участок изданных документов;
к) уничтожение в базе данных участка изготовления документов всех материалов по перепечатыванию отдельных листов и документа в целом кроме записи в электронных описях;

л) внесение в машинный журнал (протокол) сведений о выполненных операциях, проставление росписи руководителя участка изготовления документов.

Процедура снятия копий с документа, производства выписки и изготовления дополнительных экземпляров документа:

а) получение документа от исполнителя или от сотрудника соответствующего участка;

б) получение учетной карточки документа (традиционной или электронной и ее бумажного экземпляра) с соответствующего участка;

в) проверка наличия на документе разрешения полномочного руководителя на снятие копии или производство выписки, изготовление дополнительных экземпляров документа;

г) внесение отметки о получении документа во внутреннюю опись документов, находящихся у исполнителя;

д) выполнение на каждую копию или выписку операций процедур 2 и 3;

е) внесение отметки о снятии копии или производстве выписки в учетные формы основного документа;

ж) внесение отметки о дополнительно размноженных экземплярах в учетные формы основного документа;

з) внесение соответствующих отметок в основной документ;

и) внесение дополнений и изменений в электронную опись документов, выданных конкретным исполнителям, допечатка необходимых сведений во внутреннюю опись документов, находящихся у исполнителя;

к) выдача копии, выписки или дополнительно размноженных экземпляров исполнителю под роспись в традиционной карточке или бумажном экземпляре электронной учетной карточки выписки, копии или основного документа;

л) возвращение исполнителю основного документа под роспись в учетной карточке документа или с уничтожением расписки;

м) возвращение сотруднику соответствующего участка учетных форм документов, а также основного документа и его учетной формы, если документ был получен не от исполнителя;

и) передача традицией ной учетной карточки или электронной карточки и ее бумажного аналога, заполненных при изготовлении выписки или копии документа, на участок изданных документов;

о) уничтожение в базе данных компьютера участка изготовления документов всех материалов по изготовлению копий, выписок и дополнительных экземпляров документа, кроме записей в электронных описях;

п) внесение в машинный журнал (протокол) сведений о выполненных операциях, проставление росписи руководителем участка изготовления документов.

Процедура передачи учетных карточек изготовленного документа на участок изданных документов:

При традиционной регистрации проекта документа:

а) проверка соответствия сведений о подготовленном документе в учетной карточке и контрольном журнале учета карточек;

б) проверка наличия росписи исполнителя в карточке за полученный проект документа;

в) передача карточки сотруднику участка изданных документов;

г) уничтожение перепечатанных листов документа;

д) внесение отметки о новом местонахождении документа в контрольный журнал учета карточек.

При автоматизированной регистрации проекта документа:

а) проверка правильности оформления электронной учетной карточки и ее бумажного аналога (распечатки), их соответствия;

б) проверка наличия росписи исполнителя за полученный проект документа в бумажном экземпляре учетной карточки;

в) проверка уничтожения в базе данных участка изготовления документов всех электронных документов и материалов, связанных с изготовлением документов, кроме записи в электронной описи учетных карточек документов и электронной описи документов, выданных исполнителям, внесение соответствующей отметки в бумажный экземпляр карточки, заверенной второй росписью;

г) уничтожение перепечатанных листов документа;

д) передача бумажного экземпляра электронной карточки сотруднику участка изданных документов, передача электронной карточки на компьютер этого участка;

е) внесение отметки о новом местонахождении карточки в электронную опись учетных карточек участка изготовления документов;
ж) внесение в машинный журнал (протокол) обоих участков сведений о выполненных операциях, проставление росписей руководителей обоих участков.

6. Учет подготовленных конфиденциальных документов

Процедура получения учетной карточки с участка изготовления конфиденциальных документов:

При традиционной регистрации документов:

а) получение с участка изготовления документов учетных карточек основного документа и приложений;
б) проверка правильности оформления карточки и наличия росписи исполнителя;
в) совместно с сотрудником участка изготовления документов уничтожение перепечатанных листов документа, внесение отметки об уничтожении в карточку;
г) роспись за получение карточки в журнале учета карточек участка изготовления документов;
д) регистрация карточки в контрольном журнале участка изданных документов с указанием фамилии исполнителя, у которого находится документ (в зависимости от технологии — новый номер проекту документа может не присваиваться, а карточка регистрируется в контрольном журнале за единым номером двух участков, но при обязательном наличии последовательности этих номеров в журнале);
е) включение учетной карточки в картотеку «За исполнителями».

При автоматизированной регистрации документов:

а) получение с участка изготовления документов электронной карточки документа (по линии защищенной компьютерной связи или на дискете) и бумажного экземпляра этой карточки;
б) проверка правильности оформления карточки и наличия росписи исполнителя в бумажном экземпляре карточки;
в) совместно с сотрудником участка изготовления документов уничтожение перепечатанных листов документа, внесение отметки об уничтожении в экземпляры карточки, проставление росписей в бумажном экземпляре;
г) роспись сотрудника участка изданных документов за получение карточки в передаточном журнале и проставление электронной подписи в электронной описи учетных карточек участка изготовления документов;
д) регистрация карточки — внесение записи о полученной учетной карточке в электронную опись учетных карточек участка изданных документов, с указанием фамилии исполнителя, у которого находится документ (новый номер документу не присваивается, сохраняется единый порядковый номер, полученный документом при его изготовлении);
е) внесение сведений о документе в электронную опись документов, выданных конкретным исполнителям;
ж) включение электронной учетной карточки в рабочий массив базы данных компьютера, бумажного экземпляра — в страховую картотеку;
з) уничтожение информации на дискете, если она использовалась для передачи электронной карточки документа на данный участок, внесение соответствующей отметки в электронный и бумажный экземпляры учетной карточки носителя (опись документов носителя);
и) внесение в машинный журнал (протокол) участка изданных документов сведений о выполненных операциях, проставление росписи сотрудника участка.

Процедура получения документа от исполнителя:

а) получение от исполнителя подписанного руководителем документа или (и) сопроводительного письма к нему (традиционного на бумажной основе или электронного на дискете или переданного по линии защищенной компьютерной связи) и всех конфиденциальных материалов, относящихся к этому документу (в том числе входящего документа, черновика подготовленного документа и т.п.);
б) автоматическая запись документа, поступившего по защищенной линии компьютерной связи, на учтенную дискету;
в) проверка соответствия учетных данных на документе, в приложениях и учетных карточках, проверка правильности оформления реквизитов, комплектности и полноты документа;
г) проверка соответствия учетных данных черновика записи в учетной карточке

документа;
д) проверка реального наличия документа на дискете и отсутствия там других документов и записей, соответствия документа сведениям, внесенным в электронную учетную карточку (опись) носителя и бумажный экземпляр этой карточки, заверенный исполнителем; внесение отметки о проверке в бумажный экземпляр карточки (описи), заверенной росписью сотрудника участка;
е) внесение отметки о получении документа в традиционную или электронную учетную карточку, допечатка на принтере отметки о получении документа в бумажный экземпляр электронной карточки;
ж) роспись сотрудника участка за получение документа в традиционной учетной карточке или бумажном экземпляре электронной карточки;
з) направление исполнителю полиции защищенной компьютерной связи копии электронной карточки переданного документа с электрон ной подписью сотрудника участка за получение документа;
и) уничтожение черновика подготовленного документа, внесение отметки об уничтожении в традиционную или электронную учетную карточку, допечатка отметки в бумажный экземпляр электронной карточки и проставление росписей исполнителя и сотрудника участка;
к) уничтожение дискеты с записью информации черновика, внесение отметки об уничтожении в бумажный экземпляр учетной карточки (опись) носителя, заверение отметки росписями исполнителя и сотрудника участка; передача карточки на участок документов предварительного учета или инвентарный участок;
л) проставление отметки об уничтожении черновика на копии документа, подшиваемой вдело;
м) роспись сотрудника участка за получение документа и всех материалов во внутренней описи документов, находящихся у исполнителя;
н) автоматическое внесение в электронную опись массива документов компьютера исполнителя и электронную опись документов участка, находящихся у конкретных исполнителей, отметки о списании документов, полученных от исполнителя;
о) изготовление на учтенной дискете страховой копии документа, записанного на дискете, и распечатка на принтере ЭВМ двух экземпляров копии сопроводительного письма при изготовлении его на дискете, заверение копий;
п) проставление в бланке документа (или сопроводительного письма) даты издания (подписания) и индекса (исходящего учетного номера по контрольному журналу или электронной описи участка с добавлением предусмотренных технологией поисковых обозначений) отправляемого документа; проставление тех же сведений на бумажной копии отправляемого документа или сопроводительного письма;
р) дополнение учетного номера изданного внутреннего (распорядительного, организационного, протокола и т.д.) документа очередным порядковым номером традиционной регистрации каждого отдельного вида документа или индексом дела, в котором будет храниться документ;
с) передача отправляемого документа для подготовки к отправке; помещение страховой копии документа на дискете в ячейку места хранения;
т) систематизация внутренних документов и подготовка их к передаче на исполнение;
у) внесение отметки о новом местонахождении документа в контрольный журнал (при традиционной регистрации) или в электронную опись учетных карточек участка;
ф) внесение в машинный журнал (протокол) сведений о выполненных операциях, проставление росписи сотрудника участка.

Процедура получения документов с других участков службы конфиденциальной документации:

а) получение традиционного или электронного (на дискете или по линии" защищенной связи) документа с соответствующего участка службы конфиденциальной документации;
б) автоматическая запись документа, поступившего по линии защищенной компьютерной связи, на учтенную дискету;
в) получение при необходимости вместе с документом традиционного сопроводительного письма;
г) получение вместе с документом традиционной или бумажного аналога электронной учетной карточки; при наличии защищенной линии компьютерной связи — получение копии электронной карточки;

д) проверка наличия разрешения полномочного руководителя на отправку документа;
е) выполнение проверочных и сравнительных действий с документом, сопроводительным письмом и учетными формами; проверка реального наличия документа на дискете и отсутствия на ней других неучтенных документов, проверка наличия необходимой отметки и росписи в электронном и бумажном экземплярах учетной карточки (описи);
ж) роспись за получение документа и учетной карточки в передаточном журнале (при передаче документа по линии защищенной связи — проставление электронной подписи в электронной карточке и возвращение ее в компьютер соответствующего участка);
з) автоматическое внесение отметки о необходимости уничтожения копии документа в электронную опись массива электронных документов, находящихся в компьютере участка, с которого поступил документ по линии связи;
и) распечатка на принтере ЭВМ двух экземпляров копии сопроводительного письма, изготовленного на дискете, содержащей сам документ; заверение копий;
к) оформление бланка документа или сопроводительного письма;
л) передача отправляемого документа для подготовки к отправке;
м) внесение в машинный журнал (протокол) сведений о выполненных операциях, проставление росписи сотрудника участка.

Процедура передачи изданных внутренних документов на рассмотрение, исполнение и другие участки службы конфиденциальной документации:

При традиционной регистрации документов:

А) Выдача документа исполнителю:

а) выдача документа соответствующему исполнителю под роспись в учетной карточке подготовленного (изданного) документа;
б) внесение фамилии исполнителя в контрольный журнал;
в) включение учетной карточки в картотеку «За исполнителями»;

Б) Возвращение документа от исполнителя:

а) проверка целостности и комплектности документа, наличие отметки об исполнении;
б) роспись сотрудника участка за получение документа в учетной карточке документа и внутренней описи документов, находящихся у исполнителя;
в) передача документа по назначению (на другой участок службы конфиденциальной документации).

В) Передача документов на другие участки службы конфиденциальной документации:

а) внесение сведений о документе в передаточный журнал;
б) передача документа вместе с учетной карточкой сотруднику соответствующего участка под роспись в передаточном журнале;
в) внесение в контрольный журнал участка изданных документов отметки о новом местонахождении документа;
г) получение от сотрудника соответствующего участка учетной карточки с отметкой о выполненных действиях с документом;
д) роспись за полученную карточку в передаточном журнале;
е) проверка заполнения всех необходимых граф (позиций) карточки и включение ее в отработанную картотеку (справочную картотеку исполненных документов).

При автоматизированной регистрации документов:

А) Передача документа исполнителю:

а) внесение отметки в электронную учетную карточку о выдаче традиционного или электронного документа исполнителю;
б) допечатка на принтере в бумажный экземпляр электронной учетной карточки сделанной отметки;
в) при выдаче документа на дискете — проверка сведений, записанных в электронной учетной карточке на дискете, проверка комплектности документа и отсутствия на дискете неучтенных документов, внесение отметки в бумажный экземпляр учетной карточки (описи) носителя, роспись сотрудника участка и исполнителя;
г) копирование дискеты на чистый учтенный страховой (резервный) магнитный носитель, внесение необходимых сведений и росписей сотрудника участка и исполнителя в электронный и бумажный экземпляры учетной карточки (описи) этого носителя;
д) автоматическое внесение отметки о новом местонахождении документа в электронную опись карточек участка изданных документов;
е) автоматическое внесение в электронную опись документов, выданных конкретным исполнителям, записи о выдаче документа, допечатка в традиционную внутреннюю опись

документов, находящихся у исполнителя, сведений о выданном документе;
ж) выдача документа исполнителю под роспись в бумажном экземпляре электронной учетной карточки;
з) включение бумажного экземпляра учетной карточки в страховую картотеку участка; помещение страховой копии документа на дискете в ячейку места хранения;
и) внесение в машинный журнал (протокол) сведений о выполненных операциях, проставление росписи сотрудника участка.

Б) Передача исполнителю электронной копии документа по каналу защищенной связи:

а) изготовление копии документа на учтенной страховой (резервной) дискете, внесение необходимых сведений и подписи сотрудника участка в электронный и бумажный экземпляры учетной карточки (описи) носителя, помещение дискеты в ячейку места хранения;
б) внесение отметки о передаче документа исполнителю в электронную учетную карточку подготовленного (изданного) документа;
в) передача электронной учетной карточки исполнителю по каналу защищенной компьютерной связи;
г) внесение исполнителем в электронную учетную карточку электронной подписи за передаваемый ему документ и возвращение карточки в компьютер участка изданных документов;
д) автоматическое внесение отметки о передаче нового документа в электронную опись массива документов компьютера исполнителя;
е) передача копии электронного документа и копии электронной учетной карточки в базу данных компьютера исполнителя;
ж) автоматическое внесение отметки о местонахождении электронной копии документа в электронные описи учетных карточек и массива электронных документов участка изданных документов, внесение отметки в подлинник электронного документа; заверение всех отметок электронными подписями сотрудника участка;
з) автоматическое внесение сведений о переданном документе в электронную опись документов участка, выданных конкретным исполнителям;
и) внесение исполнителем записи (рукописным способом или с помощью принтера) во внутреннюю опись документов, находящихся у исполнителя;
к) внесение в машинный журнал (протокол) сведений о выполненных операциях, проставление росписи сотрудника участка.

В) Возвращение документа от исполнителя:

а) получение от исполнителя бумажного документа, дискеты;
б) поступление на компьютер участка изданных документов (при обмене документами полиции защищенной компьютерной связи) электронной карточки документа с отметкой об исполнении документа и отметкой (номером и датой акта) об уничтожении копии документа в базе данных компьютера исполнителя, заверенных электронными подписями полномочного должностного лица и уполномоченного службы конфиденциальной документации;
в) поиск экземпляров электронной и бумажной карточки документа;
г) сравнение учетных данных и проверка целостности и комплектности документа;
д) сравнение состава документов, записанных на дискете, с электронным и бумажным экземплярами учетной карточки (описи) носителя, внесение отметки и росписей сотрудника участка и исполнителя;
е) проверка наличия на документе отметки об исполнении, заверенной на бумажном документе традиционными росписями, на электронных — электронными подписями (или при записи документа на дискете наличие Возможности проставления традиционных росписей в бумажном экземпляре учетной карточки);
ж) внесение отметки о возврате документа в электронную карточку с проставлением электронной подписи сотрудника участка и допечатка отметки с проставлением росписи этого сотрудника в бумажном экземпляре электронной учетной карточки, бумажном экземпляре учетной карточки дискеты и внесение росписи сотрудника во внутреннюю опись документов, находящихся у исполнителя;
з) внесение отметки о новом местонахождении документа в электронную опись карточек участка изданных документов и электронную опись документов, выданных конкретным исполнителям;
и) при возврате электронной карточки документа, переданного по защищенной линии

компьютерной связи, внесение отметки о возврате карточки:
в электронные описи учетных карточек документов участка и массива электронных документов компьютера участка изданных документов, в подлинник Электронного документа, в электронную опись массива документов компьютера исполнителя, заверение отметок электронной подписью сотрудника участка;
к) внесение в машинный журнал (протокол) сведений о выполненных операциях, проставление росписи сотрудника участка;
л) передача документов на другие участки службы конфиденциальной документации.

Г) Передача документа на другие участки службы конфиденциальной документации:

а) внесение отметки в электронную учетную карточку о передаче традиционного или электронного документа на соответствующий участок;
б) допечатка на принтере сделанной отметки в бумажный экземпляр электронной учетной карточки;
в) при передаче документа на дискете — проверка сведений, записанных в электронной учетной карточке на дискете, проверка комплектности документа и отсутствия на дискете неучтенных документов, внесение отметки в бумажный экземпляр учетной карточки (описи) носителя, роспись сотрудника участка;
г) передача бумажного документа или документа на дискете вместе с учетной карточкой на соответствующий участок службы конфиденциальной документации;
д) при передаче документа на дискете — одновременная передача дискеты со страховой (резервной) копией документа;
е) роспись сотрудника соответствующего участка в передаточном журнале за получение документа, страховой дискеты и бумажных экземпляров учетных карточек; передача электронного экземпляра учетной карточки при наличии защищенной компьютерной линии связи с проставлением электронной подписи сотрудника соответствующего участка в электронной описи карточек участка изданных документов;
ж) уничтожение в электронном массиве компьютера участка изданных документов копий электронных учетных карточек документов и дискет (подлинники вместе с бумажными экземплярами были переданы на соответствующий участок вместе с документами и дискетами);
з) внесение отметки о новом местонахождении документа в электронную опись учетных карточек участка изданных документов;
и) получение от сотрудника соответствующего участка подлинника электронной и бумажного экземпляра учетной карточки документа с отметкой о выполненных действиях с документом;
к) роспись за получение бумажного экземпляра карточки в передаточном журнале, за электронную карточку — проставление сотрудником участка изданных документов электронной подписи в электронной описи учетных карточек соответствующего участка;
л) проверка заполнения всех необходимых граф (позиций) учетной карточки;
м) включение электронного экземпляра учетной карточки в архивный массив базы данных компьютера участка изданных документов, включение бумажного экземпляра этой карточки в страховую валовую картотеку отработанных карточек (картотеку исполненных документов);
н) внесение в машинный журнал (протокол) сведений о выполненных операциях, проставление росписи сотрудника участка изданных документов.

Д) Передача документов на другие участки службы конфиденциальной документации по каналу защищенной компьютерной связи:

а) внесение отметки в электронную учетную карточку о передаче документа на соответствующий участок;
б) передача в компьютер соответствующего участка подлинников документа и учетной карточки;
в) проставление сотрудником соответствующего участка электронной подписи в электронной описи учетных карточек участка изданных документов;
г) уничтожение в массивах подлинников электронного документа и электронной учетной карточки, а также записи о документе в электронной описи массива электронных документов участка изданных документов; внесение отметки и электронных подписей в опись учетных карточек участка изданных документов;
д) внесение отметки о местонахождении документа в электронную опись учетных карточек;

е) возвращение в компьютер участка изданных документов подлинника учетной карточки документа с отметкой о выполненных действиях с документом;
ж) внесение электронной подписи сотрудника участка изданных документов за получение карточки в электронную опись учетных карточек соответствующего участка;
з) проверка заполнения всех необходимых граф (позиций) карточки и ее распечатка на бумажном носителе, заверение копии росписью руководителя участка изданных документов и печатью (штампом) участка;
и) включение электронного экземпляра учетной карточки в архивный массив базы данных компьютера участка изданных документов, включение бумажного экземпляра этой карточки в страховую валовую картотеку отработанных карточек (картотеку исполненных документов);
к) внесение в машинный журнал (протокол) сведений о выполненных операциях, проставление росписи сотрудника участка изданных документов.

7. Проверка наличия документов, дел и носителей информации

Процедура подготовки месячной, квартальной и годовой проверки:

а) составление рабочих планов, планов-графиков проверок;
б) формирование и утверждение состава сотрудников для осуществления проверки;
в) при наличии автоматизированного учета документов распечатка за проверяемый период времени на бумажном носителе по каждому участку службы конфиденциальной документации:
• электронной валовой описи конфиденциальных документов и (или) электронной описи (контрольного журнала) учетных карточек документов;
• электронной описи массива подлинников электронных документов, находящихся в компьютере участка;
• электронной описи магнитных носителей (дискет, дисков и т.п.), информация с которых не подлежит переносу в массив электронных документов компьютера участка;
• электронной описи магнитных носителей со страховыми и резервными копиями всех электронных документов участка (внесенных в компьютер или хранящихся на магнитных носителях отдельно от компьютера);
• электронной описи архивных магнитных носителей, содержащих электронные документы временного срока хранения;
• электронной описи бумажных документов, перенесенных в электронный массив компьютера участка или перенесенных на магнитный носитель, хранящийся отдельно от компьютера;
• электронной описи рабочих магнитных носителей, предназначенных, например, для промежуточного хранения документов, поступивших по электронной почте;
• электронной описи документов, дел и носителей, выданных исполнителям, в том числе по каналу защищенной компьютерной связи;
• при необходимости — электронных экземпляров номенклатуры дел и журнала учета законченных производством дел, картотек и журналов.
г) при наличии автоматизированного учета документов распечатка за проверяемый период времени на бумажном носителей по каждому исполнителю:
• электронной описи документов, находящихся у исполнителя (бумажных, на магнитном носителе и документов, переданных полиции защищенной компьютерной связи), учтенных носителей информации;
• электронной описи массива копий электронных документов, переданных по линии связи или введенных с дискеты и находящихся в компьютере исполнителя, а также документов, составляемых (изготовляемых) исполнителем на компьютере;
• электронной описи рабочих магнитных носителей информации, предназначенных для ежедневной перезаписи массива конфиденциальной информации, находящейся в компьютере исполнителя, и сдачи в службу конфиденциальной документации;
• электронной описи магнитных носителей с документами, не подлежащими переносу в электронный массив компьютера исполнителя (поступившими, изданными, переданными для согласования и т.п.);
• электронной описи учтенных чистых магнитных носителей.
д) заверение бумажных экземпляров описей росписью руководителя участка;
е) распределение (группировка) бумажных экземпляров учетных карточек документов по указанным выше описям;
ж) объединение бумажных экземпляров описей, составленных на разных участках в

разрезе исполнителей, в единый блок по каждому исполнителю;
з) передача подготовленных материалов председателю проверочной комиссии под роспись в передаточном журнале;
и) внесение в машинный журнал (протокол) сведений о выполненных операциях, проставление росписи руководителя участка.

Выполнение операций процедуры ведения проверки на участке службы конфиденциальной документации:

а) проверка соответствия учетных данных в бумажных экземплярах учетных карточек и бумажных экземплярах распечатанных описей;
б) проверка соответствия учетных данных документа и данных на него, указанных в бумажных экземплярах учетных форм;
в) проверка правомерности внесения различных отметок в учетные формы, наличия двух росписей (электронных подписей), а также номеров и дат оправдательных документов на отправку, перевод на другой вид учета, уничтожение документа в целом или его части;
г) установление количества изготовленных и фактического наличия экземпляров и листов документа, страховых, рабочих и резервных копий электронного документа;
д) полистный просмотр электронных документов в массиве компьютера и на магнитных носителях, хранимых отдельно от ЭВМ, установление сохранности и комплектности документов, соответствия их состава учетной карточке (описи) носителя, отсутствия несанкционированных копий и правильности оформления процесса уничтожения электронных документов и магнитных носителей;
е) обнаружение по описям (контрольному журналу) и учетным карточкам отсутствующих или не представленных к проверке документов, розыск документов (экземпляров, листов документа, приложений и т.п.);
ж) проверка правильности ведения всех традиционных и электронных учетных форм, описей, своевременности и правильности внесения в них необходимых текущих записей, отметок и росписей (электронных подписей);
з) проверка наличия и оформления дел, их соответствия номенклатуре дел, правильности выполнения процедуры закрытия дел и регистрации в журнале учета законченных производством дел, картотек и журналов; проверка наличия и регистрации учетных картотек и журналов;
и) проверка правильности работы сотрудников участка с бумажными и электронными документами, носителями информации всех типов, правильности хранения документов, дел и носителей, правильности работы с информацией и документами, находящимися в компьютере.

Выполнение операций процедуры ведения проверки на рабочих местах исполнителей:

а) проверка наличия в рабочей папке (спецчемодане), сейфе и компьютере исполнителя документов, числящихся за исполнителем по всем видам учета независимо от сроков регистрации документов;
б) проверка соответствия данных документа данным на него, указанных в бумажном экземпляре учетной карточки, а также данным в соответствующей описи, проверка отсутствия у исполнителя документов, не указанных в описи;
в) полистный просмотр бумажных документов и дел, проверка сохранности всех элементов документа;
г) полистный просмотр электронных документов в массиве компьютера и на магнитных носителях, хранимых отдельно от ЭВМ, установление сохранности и комплектности документов, соответствия их состава учетной карточке (описи) носителя, отсутствия несанкционированных копий и незарегистрированных документов, правильности оформления процесса уничтожения копий электронных документов и магнитных носителей;
д) проверка правильности ведения записей и допечаток во внутренней описи документов, находящихся у исполнителя, соответствия состава документов внутренней описи и описи, составленной на участках службы документации;
е) обнаружение по описям и учетным карточкам документов и носителей информации, не представленных исполнителем к проверке, розыск документов (экземпляров, листов, приложений и т.п.);
ж) проверка правильности работы исполнителя с бумажными и электронными документами, носителями информации всех типов, правильности хранения документов в рабочее время, своевременности и полноты сдачи их по окончании рабочего дня на хранение в службу конфиденциальной документации, правильности работы с информацией, находящейся в

компьютере;
з) проверка наличия необходимых условий для работы с конфиденциальной информацией и документами на рабочем месте исполнителя (оборудование рабочего места).

Процедура оформления и анализа результатов проверки:

а) внесение отметок о проведении проверки на участке службы конфиденциальной документации в электронные и бумажные экземпляры учетных карточек документов и носителей информации, номенклатуру дел и журнал учета законченных производством дел, картотек и журналов;
б) составление, подписание и утверждение акта проверки наличия документов на участках службы документации;
в) фиксирование результатов проверки наличия документов у исполнителей в специальном журнале службы конфиденциальной документации;
г) сдача председателем комиссии полученных ранее бумажных экземпляров электронных описей, контрольных журналов и учетных карточек на соответствующие участки службы конфиденциальной документации по передаточному журналу;
д) помещение учетных карточек и контрольных журналов в места их хранения;
е) уничтожение по акту бумажных экземпляров электронных описей;
ж) анализ результатов проведенной проверки наличия документов и выполнения всеми сотрудниками правил работы с конфиденциальными документами, выработка предложений по совершенствованию организации и технологии обработки и хранения документов;
з) проведение служебного расследования по обнаруженным фактам отсутствия документов, дел и носителей информации, экземпляров, листов и других элементов документа;
и) информирование руководства предприятия о результатах проведенной проверки и разработанных мерах совершенствования работы с конфиденциальными документами;
к) установление сроков ликвидации выявленных недостатков в работе с документами и необходимости проведения повторной проверки.

8. Уничтожение документов, дел и носителей информации

Процедура подготовки документов и дел к уничтожению:

а) выделение документов, дел и носителей информации, подлежащих уничтожению по различным причинам;
б) получение письменного разрешения на уничтожение от руководителей структурных подразделений предприятия;
в) систематизация документов, дел и носителей информации по способам документирования факта уничтожения.

Процедура оформления акта на уничтожение документов:

а) включение отдельной позицией в акт каждого отобранного к уничтожению традиционного документа или дела (тома), документа или дела на магнитном или ином техническом носителе;
б) оформление в акте итоговой записи, подписание итоговой записи сотрудниками, составившими акт;
в) проведение проверки наличия и комплектности документов и дел, включенных в акт;
г) согласование, подписание и утверждение акта, рассматриваемого членами экспертной комиссии;
д) согласование, подписание и утверждение акта, не рассматриваемого членами экспертной комиссии.

Процедура уничтожения документов по акту:

а) проверка специальной комиссией наличия документов, дел (томов), магнитных и других технических носителей, включенных в акт, их комплектности и соответствия записям в акте;
б) физическое уничтожение специальной комиссией документов, дел (томов) и технических носителей информации;
в) внесение в акт и учетные карточки документов записи об уничтожении, роспись членов комиссии, производивших уничтожение.

Процедура уничтожения документов и носителей информации без составления акта:

а) разрывание листов, разрушение магнитного или иного технического носителя в присутствии исполнителя или второго сотрудника участка;
б) накапливание остатков носителей в опечатываемом ящике (урне);
в) физическое уничтожение несколькими сотрудниками остатков носителей;

г) внесение отметок об уничтожении в учетные формы документов и носителей.

СПИСОК ЛИТЕРАТУРЫ

Конституция Российской Федерации // Российская газета. 1993. 25 дек.
Закон Российской Федерации «О конкуренции и ограничении монополистической деятельности на товарных рынках» от 22.03.91 с изменениями и дополнениями от 21.04.95.
Закон Российской Федерации «О безопасности» от 05.03.92.
Закон Российской Федерации «О правовой охране программ для электронных вычислительных машин и баз данных» от 23.09.92. Ст. 2325.
Закон Российской Федерации «О товарных знаках, знаках обслуживания и наименованиях мест происхождения товаров» // Ведомости СНД РФ и ВС РФ. 1992. №42. Ст. 2322.
Закон Российской Федерации «О частной детективной и охранной деятельности в Российской Федерации» от 11.03.92.
Патентный Закон Российской Федерации // Ведомости СНД РФ и ВС РФ. 1992. №42. Ст. 2319.
Закон Российской Федерации «Об авторском праве и смежных правах» от 09.06.93 (в ред. от 19.07.95) // Собрание законодательства Российской Федерации. 1995. № 30. Ст. 2866.
Закон Российской Федерации «О государственной тайне» от 21.07.93 с изменениями и дополнениями от 06.10.97 // Собрание законодательства Российской Федерации. 1997. №41. Ст. 4673.
Закон Российской Федерации «Об информации, информатизации и защите информации» от 25.01.95 // Собрание законодательства Российской Федерации. 1995. № 8. Ст. 609.
Гражданский кодекс Российской Федерации// 1996. Ст. 155.
Уголовный кодекс Российской Федерации. — М., 1996.
Кодекс законов о труде Российской Федерации. По состоянию на 31 марта 1997 г. - М.: ИНФРА-М-НОРМА, 1997.
Указ Президента Российской Федерации от 20.01.94 № 170 «Об основах государственной политики в сфере информатизации».
Указ Президента Российской Федерации «Об утверждении перечня сведений конфиденциального характера» от 06.03.97 № 188.
Указ Президента Российской Федерации «Концепция национальной безопасности Российской Федерации» от 10.01.2000 № 24//Собрание законодательства Российской Федерации. 2000. № 2. Ст. 170.
Постановление Правительства РСФСР «О перечне сведений, которые не могут составлять коммерческую тайну» от 05.12.91 № 3.
ГОСТ Р 6.30-97 Унифицированные системы документации. Система организационно-распорядительной документации. Требования к оформлению документов. — М.: Изд. стандартов, 1997.
ГОСТ Р 50922-96 Защита информации. Основные термины и определения. — М.: Изд. стандартов, 1996.
Основные правила работы ведомственных архивов. — М.: Главархив СССР, 1988.
***
Агапов А.В. Основы федерального информационного права России. — М.: Экономика, 1995.
Андрианов В.И. и др. «Шпионские штучки» и устройства для защиты объектов и информации: Справочное пособие. — СПб.: Лань, 1996.
Андрианов В.И., Соколов А.В. «Шпионские штучки 2», или Как сберечь свои секреты. — СПб.: Полигон, 1997.
Белов В.В., Виталиев Г.В., Денисов Г.М. Интеллектуальная собственность. Законодательство и практика его применения: Учеб. пособие. — М.: Юристь, 1997.
Бержье Ж. Промышленный шпионаж. — М.: Междунар. отношения, 1972.
Боттом Н.Р., Галлати Р.Р.Дж. Экономическая разведка и контрразведка: Практическое пособие. — Новосибирск, 1994.
Владимиров В. Секреты экономической разведки // Бизнес и безопасность. 1995. №1.
Вус М.А., Морозов В.П. Информационно-коммерческая безопасность: Защита коммерческой тайны. — СПб.: Дом коммерческих бумаг, 1993.
Гавриш В. Практическое пособие по защите коммерческой тайны. — Симферополь: Таврия,

1994.
Герасименко В.А. Защита информации в автоматизированных системах обработки данных. — М.: Энергоатомиздат, 1994.
Герасименко В.А., Гришаев С.П., Павлов Д.В. и др. Основы защиты коммерческой информации и интеллектуальной собственности. — М.: Научно-информационная внедренческая фирма «ЮНИС», 1991.
Иванков П.Н. Информационно-аналитическое обеспечение работы службы безопасности предприятия // Системы безопасности связи и телекоммуникаций. 1996. №6.
Информационно-коммерческая безопасность/Защита коммерческой тайны: Пособие. — М. — СПб., 1993.
Киселев А.Е., Чаплыгин В.М., Шейкин М.С. Коммерческая безопасность. — М.: ИнфоАрт, 1993.
Коммерческая тайна предприятия /А.Н. Трунов. — М.: ОКБ «Прогресс», 1993.
Крысин А.В. Безопасность предпринимательской деятельности. — М.: Финансы и статистика, 1996.
Кураков Л.П., Смирнов С.Н. Информация как объект правовой защиты. — М.: Гелиос, 1998.
Мироничев С. Коммерческая разведка и контрразведка или промышленный шпионаж в России и методы борьбы с ними. — М.: Дружок, 1995.
300
Организация и современные методы защиты информации / Под общей ред. С.И. Диева, А.Г. Шаваева. — М.: Концерн «Банковский Деловой Центр», 1998.
Организация работы с документами: Учебник/ В.А. Кудряев, И.К. Корнеев, Г.Н. Ксандопуло и др. - М.: ИНФРА-М, 1998.
Практика защиты коммерческой тайны в США: Руководство по защите деловой информации. — М.: СП «Крокус-Интернейшнл», 1990.
Ронин Р. Своя разведка: Практическое пособие. — Минск: Харвест, 1998.
Руководство по организации защиты информации коммерческой тайны. Ч. 1, 2, 3. — М.; Минатомпром СССР, 1991.
Сверчков Л. М. Интеллектуальная собственность и коммерческая тайна в законодательных актах России // Вопросы защиты информации. 1992. Вып. 1 (22).
Сверчков Л.М., Чурляев Ю.А. Защита коммерческой тайны в производственно-предпринимательской деятельности предприятия. — М.: ЦИПКАП, 1991.
Стенюков М.В. Документы. Делопроизводство: Практическое пособие по документационному обеспечению деятельности предприятия. —М.: ПРИОР, 1995.
Степанов Е.А. Конфиденциальные документы и особенности защищенного документооборота // Классификаторы и документы. 1995. № 3—4.
Степанов Е.А. Предпосылки защиты и механизм утечки конфиденциальной информации//Секретарское дело. 1998.№ 1.
Степанов Е.А. Организация доступа персонала к конфиденциальным документам // Секретарское дело. 1998. № 2.
Степанов Е.А. Особенности документирования конфиденциальной информации//Секретарское дело. 1998. № 3.
Степанов Е.А. Безопасность информационных ресурсов //Делопроизводство. 1998. №2.
Степанов Е.А. Изготовление, издание и обработка подготовленных конфиденциальных документов//Секретарское дело. 1998. № 4.
Степанов Е.А. Формирование конфиденциальных документов в дела и работа с делами//Секретарское дело. 1999. № 1.
Степанов Е.А., Степанова Е.Е. Технология традиционного и автоматизированного учета конфиденциальных документов//Делопроизводство. 1998. № 1.
Технические средства, применяемые в охранной деятельности. — М.: Школа охраны «Баярд», 1995.
Торокин А.А. Основы инженерно-технической защиты информации. — М.: Ось-89,1998.
Федоткин С., Бураев Ю. Сборник материалов по основам организации охранной деятельности. — М., 1996.
Халяпин Д.Б., Ярочкин В.И. Основы защиты промышленной и коммерческой информации. Термины и определения. — М.: ИПКИР, 1992.
Халяпин Д.Б., Ярочкин В.И. Основы защиты информации: Учеб. пособие. — М.: ИПКИР, 1994.

Шиверский А.А. Защита информации: проблемы теории и практики. — М.: Юристь, 19%.
Экономическая разведка и контрразведка: Практическое пособие. — Новосибирск, 1994.
Ярочкин В.И. Служба безопасности коммерческого предприятия. Организационные вопросы. — М.: Ось-89, 1995.
Ярочкин В.И. Безопасность информационных систем. — М.: Ось-89, 1996. Ярочкин В.И. Коммерческая информация фирмы. Утечка или разглашение конфиденциальной информации? — М.: Ось-89, 1997.
Ярочкин В.И. Система безопасности фирмы. — М.: Ось-89, 1997.
Ярочкин В.И., Шевцова Г.А. Словарь терминов по безопасности информации. — М.: Ось-89, 1996.