СОДЕРЖАНИЕ

ВВЕДЕНИЕ……………………………………………………………………......... 3

1. «ТЕХНОЛОГИЯ РАБОТЫ С ДОКУМЕНТАМИ ОГРАНИЧЕННОГО ДОСТУПА»…………………………………………………………………………. 7

1.1 Виды конфиденциальной информации: государственная, банковская, налоговая и служебная тайны……………………... ……………… …………….. 7

1.2 Технология работы с документами ограниченного доступа в документационном обеспечении управления …………………………………... 12

1.3 Особенности архивной работы документов ограниченного доступа.…………………………………………………………………………….. 33

1.4 Особенности изъятия и уничтожения документов, дел ограниченного доступа в документационном обеспечение управления……………………….. 37

2. ТЕХНОЛОГИЯ РАБОТЫ С ДОКУМЕНТАМИ ОГРАНИЧЕННОГО ДОСТУПА В ФГОУ СПО «ПРИМОРСКИЙ ПОЛИТЕХНИЧЕСКИЙ КОЛЛЕДЖ»……………………………………………………………………….. 40

2.1 Краткая характеристика, и структура ФГОУ СПО «Приморский политехнический колледж»………………………………………………………. 41

2.2 Описание структурного подразделения и рабочего места специалиста…... 43

2.3 Составление, изготовление и издание конфиденциального документа в ФГОУ СПО «Приморский политехнический колледж»……………………….. 50

2.4 Учет, хранение и использование носителей конфиденциальной информации в ФГОУ СПО «Приморский политехнический колледж»……………………… 58

3. АНАЛИЗ ТЕХНОЛОГИИ РАБОТЫ С ДОКУМЕНТАМИ ОГРАНИЧЕННОГО ДОСТУПА В ФГОУ СПО «ПРИМОРСКИЙ ПОЛИТЕХНИЧЕСКИЙ КОЛЛЕДЖ»……………………..…………………….. 60

3.1. Учет документов ограниченного доступа в Приморском политехническом колледже…………………………………………………………………………… 61

3.2. Архивная работа с документами ограниченного доступа в Приморском политехническом колледже………………………………………………………. 62

ЗАКЛЮЧЕНИЕ……………………………………………………………………. 63

БИБЛИОГРАФИЯ………………………………………………………………… 64

ВВЕДЕНИЕ

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. Одна из главных составных частей экономической безопасности - информационная безопасность.

Безопасность ценной документируемой информации (документов) определяется степенью ее защищенности от последствий экстремальных ситуаций, в том числе стихийных бедствий. А также пассивных и активных попыток злоумышленника создать потенциальную или реальную угрозу (опасность) несанкционированного доступа к документам с использованием организационных и технических каналов, в результате чего могут произойти хищение и неправомерное использование злоумышленником информации в своих целях, ее модификация, подмена, фальсификация, уничтожение.

Документируемая информация, используемая предпринимателем в бизнесе и управлении предприятием, организацией, банком, компанией или другой структурой (далее - фирма), является его собственной или частной информацией, представляющей для него значительную ценность, его интеллектуальной собственностью.

Ценность информации может быть стоимостной категорией, характеризующей 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 информации может также отражать ее перспективное научное, техническое или технологическое значение.

Ценная информация охраняется нормами права, товарным знаком или включается в категорию информации, составляющей тайну фирмы.

Состав ценной информации фиксируется в специальном перечне, определяющем период (срок) и уровень (гриф) ее конфиденциальности (т. е. недоступности для всех), список сотрудников фирмы, которым предоставлено право использовать эти сведения в работе.

Перечень, основу которого составляет типовой состав защищаемых сведений фирм данного профиля, 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 о каждой работе фирмы.

Дополнительно может составляться перечень документов, в которых эти сведения отражаются (документируются). В перечень включаются также документы, не содержащие защищаемую информацию, но представляющие ценность для фирмы и подлежащие охране. Перечни формируются индивидуально каждой фирмой в соответствии с рекомендациями специальной комиссии и утверждаются первым руководителем фирмы. Эта же комиссия регулярно вносит текущие изменения в перечни в соответствии с динамикой выполнения фирмой конкретных работ.

Коммерческая ценность информации, как правило, недолговечна и определяется временем, необходимым конкуренту для выработки той же идеи или ее хищения и воспроизводства, опубликования и перехода информации в категорию общеизвестных. Степень ценности информации и надежность ее защиты находятся в прямой зависимости.

Несмотря на то, что конфиденциальность является синонимом секретности, этот 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.

Под конфиденциальным документом понимается необходимым образом оформленный носитель документированной информации, содержащий сведения, которые относятся к негосударственной тайне и составляют интеллектуальную собственность юридического или физического лица. Обязательным признаком конфиденциального документа является наличие в нем информации, подлежащей защите.

Следует учитывать, что основная масса конфиденциальных документов после окончания их исполнения или работы с ними теряет свою ценность и конфиденциальность.

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.

Документы долговременного периода конфиденциальности (программы и планы развития бизнеса, технологическая документация ноу-хау, изобретения до их патентования 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.

Общественная опасность противоправных действий в области конфиденциальных документов, выражается в том, что нарушения могут привлечь за собой нарушение деятельности системы управления и контроля различных (включая жизнеобеспечивающих) объектов, серьезные нарушения работы с документами ограниченного доступа.

В этой связи был принят Федеральный Закон РФ «о коммерческой тайне» № 98-ФЗ, 15 июля 2004 года, где был установлен режим коммерческой тайны в отношении сведений о неразглашении конфиденциальной информации.

Практическим работникам службы документационного обеспечения управления необходимо владеть знаниями в области ограничения доступа к конфиденциальным документам, которым установлен настоящий Федеральный Закон.

Цель данной дипломной работы – изучение технологии работы с документами ограниченного доступа.

Для этого были поставлены следующие задачи:

* изучение основных понятий по данному вопросу, а именно понятие организации работы с документами в области конфиденциальности ;
* изучение технологии учета и рассмотрения поступивших конфиденциальных документов;
* Изучение архивной работы документов ограниченного доступа;
* На практическом примере рассмотреть конкретную информацию, касающуюся документов ограниченного доступа.

1. ТЕХНОЛОГИЯ РАБОТЫ С ДОКУМЕНТАМИ ОГРАНИЧЕННОГО ДОСТУПА

1.1. Виды конфиденциальной информации: государственная, банковская, налоговая и служебная тайны

Некоторые документы ограниченного доступа несут информацию о государственной тайне.

Государственная тайна — это защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-разыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации согласно Закону РФ от 21.07.1993 № 5485-1 «О государственной тайне». Положения Закона обязательны для исполнения на территории РФ и за ее пределам органами представительной, исполнительной и судебной власти, местного самоуправления, предприятиями, учреждениями и организациями, независимо от их организационо-правовой формы и формы собственности, должностными лицами и гражданами РФ, взявшими на себя обязательства либо обязанными по своему статусу исполнять требования законодательства РФ о государственной тайне.

По степени важности сведений государственные секреты делятся на государственную тайну и служебную тайну. Государственную тайну составляют сведения, разглашение (передача, утечка и т.д.) которых может оказать отрицательное воздействие на качественное состояние военно-экономического потенциала страны или повлечь другие тяжкие последствия для обороноспособности, государственной безопасности, экономических и политических интересов страны. Служебную тайну составляют охраняемые государством сведения в любой области науки, техники, производства и управления, разглашение (передача, утечка и т.д.) которых, может нанести ущерб интересам государства.

Перечень сведений отнесенных к государственной тайне, утвержден Указом Президента РФ от 30.11.1995 № 1203 (в ред. от 29.05.2002).

В организациях государственной и негосударственной формы собственности встречаются документы, которые могут нести в себе информацию открытую и информацию с ограниченным доступом, помеченную грифами «Конфиденциально», «Для служебного пользования», «Коммерческая тайна», «Секретно» и т.п. Коммерческая тайна – это конфиденциальная информация, позволяющая её обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду. К информации, составляющей коммерческую тайну, относится: научно – техническая, технологическая, производственная, финансово – экономическая, иная информация (в том числе составляющая секреты производства (ноу-хау), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности её третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введён режим коммерческой тайны. Одним из критериев отнесения информации к коммерческой тайне является возможность получения экономической выгоды от её разглашения или использования. К коммерческой тайне относятся, прежде всего, идеи, изобретения, открытия, технологии, индивидуальные детали коммерческой деятельности, позволяющие успешно конкурировать и т.п. :

Действительная или потенциальная коммерческая ценность информации в силу неизвестности её третьим лицам; Отсутствие свободного доступа к этой информации на законном основании; Принятие обладателем информации необходимых мер к охране её конфиденциальности.

Определение сведений, составляющих коммерческую тайну предприятия; Обеспечение порядка их защиты; Обеспечение строго контроля за допуском персонала к секретным документам; Точное установление того, кто конкретно из руководства или служащих предприятия организует и контролирует секретное делопроизводство, наделение их соответствующими полномочиями; Разработка инструкции (памятки) по работе с секретными документами, ознакомление с нею соответствующих работников организации; Контроль за принятием соответствующими служащими письменных обязательств о сохранении коммерческой тайны предприятия; Введение системы материального и иного стимулирования служащих предприятия, имеющих доступ к её секретам; Внедрение в повседневную практику механизмов и технологий защиты коммерческой тайны организации; Личный контроль со стороны руководителя организации, внутренней службы безопасности и секретного делопроизводства. Если эти условия не будут выполнены, то у предприятия не будет законных оснований для привлечения к ответственности работников за разглашение или передачу сведений, составляющих коммерческую тайну, так как владелец информации, составляющей коммерческую тайну, вправе потребовать в судебном порядке возмещения убытков, причинённых её разглашением или выплату компенсации в размере, установленном решением суда. Также к документам ограниченного доступа (конфиденциальные документы) можно отнести документы, содержащие банковскую тайну.

Банк гарантирует тайну банковского счета и банковского вклада, операций по счету и сведений о клиенте (ст. 857 ГК РФ).

Сведения, составляющие банковскую тайну, могут быть предоставлены только самим клиентам или их представителям. Государственным органам и их должностным лицам такие сведения могут быть предоставлены исключительно в случаях и в порядке, предусмотренных законодательством РФ.

В соответствии со ст. 26 Федерального закона от 02.12.1990 № 395-1 «О банках и банковской деятельности» (в ред. от 02.11.2004) кредитная организация, Банк России гарантируют тайну об операциях, о счетах и вкладах своих клиентов и корреспондентов. Все служащие кредитной организации обязаны хранить тайну об операциях, счетах и вкладах ее клиентов и корреспондентов, а также об иных сведениях, устанавливаемых кредитной организацией, если это не противоречит федеральному закону.

Справки по операциям и счетам юридических лиц и граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, выдаются кредитной организацией им самим, судам и арбитражным судам (судьям), Счетной палате РФ, органам государственной налоговой службы и налоговой полиции, таможенным органам РФ в случаях, предусмотренных законодательными актам об их деятельности, а при наличии согласия прокурора — органом предварительного следствия по делам, находящимся в их производстве.

Справки по счетам и вкладам физических лиц выдаются кредитной организацией им самим, судам, а при наличии судебного решения — органом предварительного следствия по делам, находящимся в их производстве.

Справки по счетам и вкладам в случае смерти их владельцев выдаются: кредитной организацией — лицам, указанным владельцем счета или вклада в сдельном кредитной организацией завещательном распоряжении; нотариальными конторами — по находящимся в их производстве наследственным делам о вкладах умерших вкладчиков, а в отношении счетов иностранных граждан — иностранным консульским учреждениям.

На денежные средства и иные ценности юридических и физических лиц, находящихся на счетах и во вкладах или на хранении в кредитной организации, может быть наложен арест не иначе как судом и арбитражным судом, судьей, а также по постановлению органов предварительного следствия при наличии санкции прокурора.

При наложении ареста на денежные средства, находящихся на счетах и во вкладах, кредитная организация незамедлительно по получении решения о наложении ареста прекращает расходные операции по данному счету (вкладу) в пределах средств, на которые наложен арест.

Взыскание на денежные средства и иные ценности физических и юридических лиц, находящиеся на счетах и во вкладах или на хранении в кредитной организации, может быть обращено только на основании исполнительных документов в соответствии с законодательством РФ.

Без распоряжения клиента списания денежных средств, находящихся на счете, допускается по решению суда, а также в случаях, установленных законом или предусмотренных договором между банком и клиентом (п. 2 ст.854 ГК РФ)

В организациях, которые работают в сфере налогообложения ,используются документы ограниченного доступа, содержащие в себе налоговую тайну.

Налоговую тайну составляют любые полученные налоговым органом, органами внутренних дел, органом государственного внебюджетного фонда и таможенным органом сведения о налогоплательщике, за исключением сведений:

* разглашенных налогоплательщиком самостоятельно или с его согласия;
* об идентификационном номере налогоплательщика;
* о нарушениях законодательства о налогах и сборах и мерах ответственности за эти нарушения;
* предоставляемых налоговым (таможенным) или правоохранительным органам других государств в соответствии с международными договорами (соглашениями), одной из сторон которых является Российская Федерация, о взаимной сотрудничестве между налоговыми (таможенным) или правоохранительными органами (в части сведений, представленных этими органами) (ст. 102 части первой Налогового кодекса РФ).

1.2. Технология работы с документами ограниченного доступа

в документационном обеспечении управления

Документы ограниченного доступа требуют к себе несколько иного подхода на стадии делопроизводства в отличие от документов несекретного характера, не носящих в себе какую-либо тайну. Работник организации должен работать только с теми сведениями и документами, содержащими какую-либо тайну, к которым он получил доступ в силу трудовых обязанностей, знать, какие конкретно сведения подлежат защите, а также строго соблюдать правила пользования ими. Работник также должен знать, кому из сотрудников организации разрешено работать со сведениями, составляющими тайну, к которым он сам допущен, и в каком объеме эти сведения могут быть доведены до этих сотрудников.

При увольнении работника, имеющего отношение к документам ограниченного доступа, в обязательном порядке проводится проверка наличия числящихся за ним документов. Только после этого производится отметка в его обходном листе. Если же работник временно отсутствует (болезнь, отпуск, командировка и т.п.), передача числящихся за ним документов другим работникам производится по решению начальника подразделения с отражением в журнале учета или по акту.

Документы ограниченного доступа по номенклатуре определяются в дела. На обороте обложки дела или на отдельном листе, хранящемся в деле, указывается список сотрудников, которым разрешено ознакомление с делом. Изменения в эти списки вносятся с разрешения начальника режимного отдела (службы безопасности) по представлению начальников структурных подразделений.

При пользовании делами, в которых имеются документы ограниченного доступа, необходимо иметь в виду, что дела должны возвращаться в тот же день лицами, которым они были выданы для работы. В случае необходимости производства копий с документов ограниченного доступа обязательно должен вестись журнальный учет производства копий.

Чрезвычайным происшествием в организации считается недостача (утрата) документов ограниченного доступа, выявленная в ходе ежегодной проверки наличия документов, дел и картотек. Такую проверку необходимо проводить по окончании года (как правило, в I квартале года), независимо от того, где и у кого документы находятся, и от времени их поступления. Проверка проводится специальной комиссией, назначаемой приказом руководителя организации, в составе не менее 3 работников из числа лиц, имеющим прямое отношение к проверяемым документам и соответствующий допуск к данным работам, с обязательным включением в ее состав работников режимного отдела (службы безопасности).

При незначительном количестве таких документов, циркулирующих в организации, проверка может производиться руководителем конкретного подразделения или по его указанию одним из работников этого подразделения и работником режимного отдела (службы безопасности).

В ходе проверки анализируется движение (поступление, отправка, размножение и уничтожение) документов с ограниченным доступом, произошедшее за проверяемый год, а также проводится сверка учетных данных с фактическим наличием документов. При проверке используются журналы учета документов, расписки, реестры, акты на уничтожение документов и другие учетные формы, в том числе и те, в которых зарегистрировано размножение документов. По результатам проверки составляется акт, который утверждается руководителем подразделения и докладывается руководителю организации.

Наиболее существенным отличием технологии обработки и хранения конфиденциальных документов от технологии и хранения документов открытых, которое составляет основу процесса защиты конфиденциальных документов от любого вида угроз по организационным и техническим каналам, мы считаем многоступенчатый учет всех процедур и операций, выполняемых с документом.

Учет (регистрация) открытых документов в первую очередь преследует цель включения документа в справочно-информационную систему для целей справочной и поисковой работы по документам и контроля исполнения поручений и заданий, содержащихся в документе.

Учет конфиденциальных документов, прежде всего, преследует цель сохранности документов и фиксирования их местонахождения.

Итак, основная цель учета конфиденциальных документов — обеспечение их физической сохранности, комплектности и целостности, контроль за доступом к ним персонала, проверка реального наличия документов и аналитическая работа по осведомленности персонала о содержании документов.

Справочная работа и контроль исполнения документов, хотя относятся к стадиям обработки документов, часто не являются основными технологическими процессами. В отличии от открытых документов конфиденциальные документы (на любом носителе) учитываются сразу при поступлении или перед изготовлением первого варианта беловика, т.е. до рассмотрения, распределения или согласования, подписания.

При ведении учета конфиденциальных документов возможно возникновение следующих опасных ситуаций:

* выпадение документа из учетной системы за счет ошибочных или злоумышленных действий работника;
* отсутствие фиксируемого контроля за документом при переходе его от одной технологической стадии движения и процедуры обработки к другой;

утечка информации по техническим каналам;

* использование работниками традиционной или автоматизированной технологии, не предназначенной для технологии и хранения конфиденциальных документов, или самодельной, непрофессиональной технологии;
* нарушение порядка выполнения учетных операций и ведения справочно-информационного банка данных по документам;

Основной способ защиты информации при указанных угрозах — строгая регламентация специализированных технологических процедур учета и контроль за соблюдением работниками и персоналом утвержденных руководством организации требований и правил.

Учет конфиденциальных документов предназначен для:

* фиксирования факта поступления пакета с документами, отдельного бумажного или машинопечатного документа, или документа, поступающего из электронной или факсимильной почты;
* Фиксирования факта регистрации исходных сведений о документе и включения его в справочно-информационный банк данных по документам;
* фиксирования факта переноса информации с бумажного документа на машинный носитель, факта включения документа в электронную базу данных и факта помещения бумажного документа в соответствующие дело;
* фиксирования факта перемещения документа в процессе его рассмотрения и исполнения;
* фиксирования местонахождения документа в любой момент времени в период исполнения документа при его архивном хранении;
* фиксирования факта регистрации исходных сведений о подготовленном документе;
* фиксирования факта начала и окончания составления, изготовления и издания документа;
* фиксирования в машинном журнале всех действий, которые выполняются с электронными документами в базе данных;

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, поступающих по телеграфной, электронной почте и факсимильной связи с грифом конфиденциальности (пакетный учет);
* пакетный учет поступления документов, не имеющих графа конфиденциальности, но отнесенных к документам ограниченного доступа в перечне данной фирмы;
* Учет подготовленных исходящих и внутренних документов;
* инвентарный учет документов;
* номенклатурный учет документов.

Следовательно, в предметном и технологическом аспектах учет конфиденциальных документов значительно отличается от регистрации открытых документов и делится на ряд видов, что определяется необходимостью защиты документов от тех угроз, которые могут стать причиной несанкционированного доступа злоумышленника к тайне фирмы.

Традиционный учет отличается надежностью и распространяется на документы, которые имеют любой вид носителя — бумажный, технический, а также на электронные документы.

При любом виде учета конфиденциальных документов выполняются следующие процедуры: индексирование документов; первичная регистрация исходных сведений о документе; последующая запись рабочих сведений о документе; формирование справочно-информационного банка данных по документам; ведение справочно-информационного банка данных; контроль процесса полноты и правильности регистрации документов, сохранности документов и учетных форм.

Основой индексирования конфиденциального документа является валовая нумерация всего потока документов в течении календарного года.

Подобная индексация гарантирует сохранность записи исходных сведений о документе — ни один номер не может исчезнуть и не одна карточка не может выпасть из систематизированного по номерам массива. К номеру документа может добавляться смысловой индекс, идентифицирующий дело в котором будет храниться документ.

Сведения, включаемые в учетную форму при регистрации конфиденциальных документов, всегда разделяются на два блока:

* фиксирующий постоянные сведения о документе;
* фиксирующий переменные, текущие, рабочие сведения о движении и местонахождении документа.

Форма учетной карточки конфиденциального документа отличается от регистрационно-контрольной карточки открытого документа не только большим количеством граф, но и их взаимосвязью в отражении пути движения документа.

При карточной учетной форме на каждый конфиденциальный документ заполняется один-два экземпляра регистрационной карточки.

При заполнении одного экземпляра карточки она учитывается в контрольном 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 напротив учетного номера документа указывается фамилия исполнителя, расписавшегося в карточке за его получение.

При заполнении двух экземпляров все указанные сведения фиксируются во втором экземпляре карточки, а функцию контрольного журнала выполняет валовая учетная картотека. Перемещение конфиденциальных документов и учетных карточек между работниками фиксируются в передаточном журнале.

В некрупных компаниях, имеющих небольшой объем таких 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 своевременным снятием грифа конфиденциальности. Перемещаются и хранятся эти документы отдельно от документов всего потока.

Значительное место в обработке конфиденциальных документов занимает инвентарный (списочный, перечневый) учет.

На инвентарный учет берутся следующие конфиденциальные документы:

* не включенные в номенклатуру дел и неподлежащие подшивке в дела;
* изъятые по какой-либо причине из дела, переведенные на выделенное хранение и образовавшие самостоятельное дело;
* технические носители информации;

Картотека инвентарного учета конфиденциальных документов ведется непрерывно.

Автоматизированный учет конфиденциальных документов предусматривает следующие процедуры:

* подготовка документов к вводу в ЭВМ;
* ввод исходных сведений о документах в автоматизированный банк данных;
* ежедневная проверка правильности регистрации документов и их наличия;
* изготовление на учетной дискете страховой копии документа, поступившего по линии электронной почты;
* подшивка бумажного документа и бумажной копии электронного документа в дело в соответствии с номенклатурой дел и помещение страховых дискет в ячейку места хранения.

На основе применяемых традиционных и электронных регистрационных форм создается справочно-информационный банк данных, 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 и проверки их наличия.

Задачи справочно-инормационного банка данных решаются с помощью двух обязательных технологических элементов:

* формирование банка;
* ведение (актуализация) банка.

Банк может бать традиционным и автоматизированным.

Традиционный справочно-информационный банк данных независимо от вида учета включат в себя:

* журналы учета документов по видам учета или учетную валовую картотеку с разделами неисполненных и исполненных 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;
* справочную картотеку на исполненные документы, в которой освободившиеся экземпляры карточек располагаются по корреспондентам или другому для исполнения признаку;
* конфиденциальную картотеку по распорядительным документам;
* контрольную картотеку, в которой дополнительные экземпляры карточек располагаются по срокам исполнения документов.

Автоматизированный справочно-информационный банк данных по конфиденциальным документампринципиально не отличается от аналогичных систем, оперирующих открытой информацией и документами и широко использующихся фирмами. 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 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 пользователями, подлежит фиксированию в учетной форме, машинном журнале и подтверждается подписью одного или двух сотрудников.

Заключительная процедура любой технологической системы учета конфиденциальных документов — контроль процесса регистрации и сохранности документов и учетных форм.

Цель процедуры — ежедневная проверка вторым работником службы соответствия состава документов, подлежащих учету, составу реально учетных 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.

В открытом делопроизводстве поступившие в организацию пакеты, конверты и другие почтовые отправления никогда не ставятся на индивидуальный учет, а возможная утеря конверта с документами или некомплектность документа в конверте обычно не являются предметом большого беспокойства. Иначе обстоит дело с поступающими пакетами и конвертами, содержащими конфиденциальные документы.

Правильная организация работы с этими пакетами и предотвращение последующей реальности опасности утраты этих документов и несанкционированного ознакомления с ними становится крайне актуальной задачей. Основу ее решения составляет выполнение комплекса технологических процедур: прием пакетов, их учет, распределение и вскрытие пакетов, выделение из общего документопотока ценных и конфиденциальных документов, закрытие журнала учета пакетов.

Поступающие пакеты, конверты до их вскрытия и незаконвентированные документы должны быть зарегистрированы в традиционном или электронном журнале учета пакетов.

После завершения традиционного или автоматизированного учета поступивших конфиденциальных документов они передаются для работы руководителям и сотрудникам организации.

Процедура распределения поступивших документов предназначена для определения рационального пути дальнейшего движения документа в соответствии с его функциональной принадлежностью и местом в разрешительной системе доступа к конфиденциальным документам.

Разрешительная система доступа — это совокупность обязательных норм и требований, устанавливаемых первым руководителем или коллективным органом руководства фирмы с целью закрепления за руководителями и сотрудниками права использования для выполнения служебных обязанностей специализированных помещений и рабочих мест, определенного состава конфиденциальных документов и сведений.

Доступ к конфиденциальной информации представляет собой практическую реализацию делегированного сотруднику руководством организации права работать с подобной информацией, т.е. допуска сотрудника к тайне организации.

Доступ санкционируется полномочным должностным лицом в отношении конкретной информации и конкретного сотрудника. Такой доступ называется санкционированным, разрешенным и законным.

Разрешение на доступ к конфиденциальным сведениям всегда является строго персонифицированным (индивидуальным) и делается руководителем только в письменном виде — в виде резолюций на документе, приказа, утверждающего схему именного или должностного доступа к конкретным группам информации, утвержденного руководителем списка-разрешения на обложке дела и т.п.

Особенность информационного обслуживания потребителей конфиденциальной информации состоит в том, что не потребитель определяет, какая информация ему нужна и какой информацией он может пользоваться, а полномочный руководитель.

Поэтому тайна организации должна быть разделена на несколько частей, известных разным сотрудникам и соответствующих функциональной структуре организации, причем ценность информации снижается по мере доведения ее до отдельных исполнителей низшего звена. В этом случае тайну организации в целом может знать крайне ограниченный круг должностных лиц, и разглашение отдельной ее части не наносит серьезного ущерба делам организации.

Иерархическая последовательность доступа к информации реализуется по принципу «чем выше ценность конфиденциальных сведений, тем меньше сотрудников могут их знать». Существует твердое правило: сотрудники организации, которым руководитель не адресует документ, не только не имеет права доступа к нему, но и не должны знать о существовании такого документа и исходных данных о нем.

Реализация системы доступа к традиционным и электронным документам основывается на анализе их содержания, которое является главным критерием однозначного определения, кто из руководителей, кому из исполнителей, как, когда и с какими категориями документов разрешит ознакомиться или работать.

Любое обращение к конфиденциальному документу, ознакомление с ним в любой форме обязательно фиксируется в учетной карточке документа и на самом документе в виде соответствующей отметки и подписи лица, который обращался к документу. Этот факт указывается также в карточке учета осведомленности сотрудника в тайне фирмы.

Доступ к конфиденциальным базам и файлам *—* завершающий этап доступа сотрудника организации к компьютер. Если этот сотрудник — злоумышленник, то можно считать, что самые серьезные рубежи защиты охраняемой электронной информации он успешно преодолел. В конечном счете, не «взламывая» базу данных, он может просто унести компьютер или вынуть из него и унести жесткий диск.

Технологический процесс учета конфиденциальных документов включает в себя ряд процедур, обязательных для любого вида учета и любого типа технологических систем обработки и хранения этих документов.

Под исполнением конфиденциально документа понимается процесс документирования управленческих решений и действий, результатов выполнения руководителями и сотрудниками организации поставленных заданий, поручений, а также реализации функций, закрепленных за ними в должностных инструкциях.

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.

Процесс ознакомления с конфиденциальным документом — это информирование сотрудника организации ли другого заинтересованного лица, осуществляемое в соответствии с резолюцией полномочного руководителя на конфиденциальном документе, о принятом этим руководителем решении или решении другой организационной структуры.

Общеизвестно, что в наибольшей безопасности находится конфиденциальная информация, не зафиксированная на каком-либо носителе, ценная информация немедленно подвергается угрозе при возникновении необходимости ее документирования.

В связи с этим система защиты конфиденциальной информации должна начать функционировать не после издания (подписания) конфиденциального документа, а заблаговременно, т.е. до создания будущего документа. Прежде чем создать документ, следует установить, является ли данная информация конфиденциальной и какой уровень грифа конфиденциальности ей должен быть присвоен в случае положительного ответа.

Своевременное установление грифа конфиденциальности должны составлять: перечень конфиденциальных сведений организации, требования партнеров, а также перечень конфиденциальных документов организации.

Система грифования (маркирования) документов не гарантирует сохранность информации, однако, позволяет четко организовать работу с документами, в частности сформировать систему доступа к документам персонала.

Гриф конфиденциальности, или гриф ограничения доступа к традиционному, машинопечатному или электронному документу представляет собой реквизит 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:

* 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;
* Этот уровень достаточно редкий — грифы «Строго конфиденциально», «Строго конфиденциальная информация», «Конфиденциально. Особый контроль».

На документах, содержащих сведения, отнесенные к служебной тайне, ставится гриф «Для служебного пользования».

Написание грифа ограниченного доступа, указываемого на документе не сокращается. Под обозначением грифа указываются номер экземпляра документа, срок действия грифа и иные условия его снятия.

Гриф располагается в соответствии с ГОСТ Р 6.30-2003 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: «Лично», «Только в руки», «Только адресату», «Лично в руки». При регистрации конфиденциального документа к его номеру добавляется обозначение грифа конфиденциальности, например: 37к, 89ск, 97дсп.

Документы и информация, конфиденциальные в целом, в своей массе, как правило, не маркируются, потому что в полном объеме обладают строгим ограничением доступа к ним персонала.

Обязательному инвентарному учету и маркировки на всех уровнях исполнения управления подлежат магнитные носители информации, для которых любые угрозы представляют значительно большую безопасность, 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.

Рассматривая технологию подготовки к документированию и документирования конфиденциальной информации, мы ранее отметили две специфические особенности, необходимые для обеспечения заблаговременного сохранения в тайне содержания создаваемого документа: присвоение будущему документу определенного уровня грифа конфиденциальности и предварительный учет носителя, на котором этот документ будет составляться.

Третья специфическая особенность состоит в том, что ни один проект конфиденциального документа не может быть изготовлен на основе черновика и обрести статус правомерно документированной информации без санкции полномочного должностного лица организации.

Эта особенность обусловлена необходимостью документирования такого правового события, как зарождение персональной ответственности данного должностного лица за издание конкретного документа, т.е. распространение конфиденциальных сведений и соответствующие увеличение состава источников, владеющих данной информацией.

Четвертая (и, пожалую более существенная) особенность документирования конфиденциальной информации, касающаяся уже непосредственно технологических процедур изготовления самого документа, - централизированный учет черновика и проекта будущего документа (присвоение им единого учетного номера).

Одновременно на еще не изготовленный документ заполняется комплект учетных карточек. Учетный номер черновика документа будет сопровождать проект документа, а затем и сам документ в процессе его последующего «жизненного цикла».

Обязательно учитываются проекты подготовленных конфиденциальных электронных документов, факсов и телеграмм. Ответным документам присваивается новый учетный номер.

Приложения к новым конфиденциальным документам являются самостоятельными документами и имеют свои учетные номера по соответствующим видам учета, в том числе номер некофиденциального документа, если приложение не содержит защищаемых сведений.

В учетной карточке подготовленного документа отражается последовательно ход работы над проектом документа в процессе его изготовления, издания, последующего исполнения или отправки, хранения или уничтожения.

Цель этапа изготовления конфиденциального документа — перепечатывание черновика документа и создание его в соответствии с государственным стандартом оригинала проекта документа, предназначенного по окончании этапа издания стать подлинником документа.

Ценные текстовые и табличные конфиденциальные документы с грифом строгой конфиденциальности изготавливаются централизованно с использованием пишущих машин или ПК.

Основная масса проектов типовых по содержанию конфиденциальных документов может с разрешения первого руководителя фирмы изготавливаться децентрализовано самими исполнителями и руководителями непосредственно на рабочих местах.

Конфиденциальный документ находится в относительной безопасности до тех пор, пока он хранится в службе конфиденциальных документов (КД). При выходе документа за пределы рабочего помещения службы его уязвимость резко возрастает за счет санкционированного ознакомления с ним определенного числа сотрудников организации. Ответственность за сохранность конфиденциальных документов и предотвращение утраты ими конфиденциальности несут руководители подразделений организации.

Работники предприятия, допущенные к конфиденциальным сведениям и документам, прежде чем получить доступ к ним, должны пройти инструктаж и ознакомиться с памяткой о сохранении коммерческой тайны предприятия. Памятка составляется службой безопасности с учётом специфики конкретного предприятия, подписывается заместителем директора и утверждается директором предприятия. Ведение делопроизводства, обеспечивающего учёт и сохранность документов, содержащих коммерческую тайну, предусматривает выполнение ряда рекомендаций. Приказом руководителя предприятия назначается должностное лицо (лица), ответственное за учёт, хранение и использование документов, содержащих конфиденциальные сведения. Это может быть сотрудник, для которого работа с документами коммерческой тайны является основной служебной обязанностью, или секретарь – референт предприятия. Эти лица несут персональную ответственность за утерю или утечку информации из них. Все документы, содержащие коммерческую тайну или конфиденциальную информацию, подлежат учёту и специальному обозначению. На документе проставляют гриф ограничения доступа с указанием номера экземпляра, обладателя этой информации (для юридических лиц – полное наименование и место нахождения, для индивидуальных предпринимателей – фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

Такие грифы показывают, что право собственности на информацию, содержащуюся в документе, принадлежит предприятию и охраняется законодательно. При передаче документов, содержащих коммерческую тайну, в органы государственной власти и органы местного самоуправления гриф «Коммерческая тайна» или «Конфиденциально» проставляется в обязательном порядке. В тексте документа также может быть оговорена конфиденциальность сведений, права предприятия на них, порядок их использования и т.п. Например, если коммерческая тайна является результатом совместной деятельности с другим предприятием, то необходимость её сохранения должна быть отражена в договоре. В случае отсутствия грифа «Коммерческая тайна» и указаний на конфиденциальность в тексте предполагается, что автор и лица, подписавшие или утвердившие документ, предусмотрели все возможные последствия от свободной (без ограничения доступа) работы с документом. На документе с грифом «Коммерческая тайна» указывается количество экземпляров документа и место нахождения каждого из них (ниже реквизитов «подпись» и «отметка об исполнителе»).

Отметка о количестве составленных экземпляров проставляется на экземпляре, который подшивается в дело. На обороте листа документа, имеющего гриф, руководитель пишет фамилии тех должностных лиц, которым разрешено пользоваться этим документом (можно указать и в резолюции).

Печатание документов с грифом «Коммерческая тайна» производится централизованно, в специально отведённом помещении, исключающем доступ посторонних лиц. Отпечатанные и подписанные документы передаются для регистрации должностному лицу, ответственному за их учёт. Черновики, файлы, варианты документа уничтожаются этим должностным лицом с подтверждением факта уничтожения записью на копии документа: «Черновик (или файл) уничтожен. Подпись. Дата». Все документы, содержащие конфиденциальную информацию, должны регистрироваться отдельно от остальной документации в «Журнале регистрации документов с грифом «Коммерческая тайна». При значительном объёме документов могут быть заведены журналы отдельно для входящих, исходящих и внутренних документов предприятия, содержащих гриф «Коммерческая тайна». Все листы журналов, учитывающих такие документы, нумеруются, прошиваются и опечатываются. В конце журнала в заверительном листе указывается общее количество листов (цифрами и прописью). Все поступающие (входящие) документы с грифом «Коммерческая тайна» принимаются и вскрываются специально назначенным должностным лицом или секретарём – референтом, если ему предоставлено такое право. При поступлении обязательно проверяется целостность корреспонденции, количество листов и экземпляров основного документа и приложений к нему. В случае отсутствия или недостачи в конвертах (пакетах) документов с грифом «Коммерческая тайна» составляется акт в двух экземплярах, один из которых направляется отправителю. Документы, имеющие гриф «Коммерческая тайна», формируются в отдельное дело (или дела). На обложке в правом верхнем углу ставится гриф «Коммерческая тайна». На внутренней стороне обложки дела пишется список сотрудников, имеющих право пользования этим делом. Все листы дела нумеруются простым карандашом в правом верхнем углу. В начале дела подшивается внутренняя опись документов, содержащихся в нём, в конце дела подшивается заверительный лист. Хранятся такие дела в сейфе, который опечатывается должностным лицом, ответственным за сохранность документов с грифом «Коммерческая тайна». Другие работники предприятия не должны иметь доступа к этому сейфу. Движение (выдача и возврат) документов с грифом «Коммерческая тайна» должно своевременно отражаться в «Журнале учёта выдачи документов с грифом «Коммерческая тайна». При выдаче документа секретарём – референтом работник, получивший документ с грифом «Коммерческая тайна», должен сверить номер полученного документа с номером журнале, проверить количество листов и поставить в журнале свою подпись. Выданные документы с грифом «Коммерческая тайна» подлежат возврату секретарю – референту в тот же день. С разрешения руководства предприятия отдельные документы с грифом «Коммерческая тайна» могут находиться у исполнителя в течение срока, необходимого для выполнения работы с ним, при условии полного обеспечения сохранности документов на рабочем месте исполнителя (наличие сейфа, кодового замка и т.д.).

При возврате документа с грифом «Коммерческая тайна», секретарь – референт сверяет номер документа по журналу, проверяет количество листов документа и в присутствии работника ставит в графе «Отметка о возврате» свою подпись и дату возврата документа. Передача документов и дел между работниками предприятия, производится только через секретаря – референта с обязательной записью в журнале. Запрещается изъятие из дел или перемещение документов с грифом «Коммерческая тайна» из одного дела в другое без разрешения руководства и отметок в «Журнале регистраций документов с грифом «Коммерческая тайна». Документы с грифом «Коммерческая тайна» запрещается выносить из офиса. Лишь в исключительных случаях руководитель или его заместители могут разрешить сотрудникам вынос таких документов из здания для согласования, подписания и т.п. с принятием необходимых мер предосторожности. На предприятии должен быть принят строгий порядок размножения документов с грифом «Коммерческая тайна». Они должны копироваться с разрешения руководства предприятия в специально выделенном помещении. Все копии конфиденциальных документов берутся на учёт в специальном журнале или в «Журнале регистраций документов с грифом «Коммерческая тайна». Количество экземпляров документов с грифом «Коммерческая тайна» должно быть ограничено, причём каждый экземпляр готовится для заранее определённого адресата или исполнителя. Размножение документов следует производить в присутствии должностного лица, ответственного за документ. Все бракованные копии документа им забираются и подлежат немедленному уничтожению. При работе с конфиденциальными документами необходимо ввести ряд следующих ограничений для работников предприятия: - запрещается делать выписки из документов, имеющих гриф ограничения доступа, без письменного разрешения руководителя; - запрещается знакомиться с документами, делами, информацией, содержащейся в памяти компьютера, других работников предприятия; - запрещается использовать информацию из документов, имеющих гриф ограниченного доступа, в открытых докладах, сообщениях, переписке, рекламных изданиях; - запрещается предоставлять свой компьютер для работы другим сотрудникам предприятия и работать на их ПК; - запрещается бесконтрольно оставлять конфиденциальные документы на рабочем столе и работающий компьютер с конфиденциальной информацией. Все дела с грифом «Коммерческая тайна» и журналы их учёта вносятся в номенклатуру дел предприятия. В том случае, если заголовки дел несут элементы коммерческой тайны, могут применяться условные (кодовые) заголовки дел или составляться отдельная номенклатура только на эти дела. По окончании года специально созданная комиссия предприятия выполняет следующие работы: - проверяет наличие всех документов с грифом «Коммерческая тайна»; - отбирает документы с грифом «Коммерческая тайна» для архивного хранения; - отбирает документы с грифом «Коммерческая тайна» для уничтожения.3 Проверка наличия документов с грифом «Коммерческая тайна» по решению руководства предприятия может производиться с другой периодичностью, например, по окончании полугодия. В случае установления факта утраты документов с грифом «Коммерческая тайна» немедленно ставится в известность руководитель предприятия, служба безопасности и принимаются все меры к розыску документа. Руководителем предприятия в связи с фактом утраты назначается комиссия для служебного расследования. На утерянные документы после того, как розыск их не принёс положительных результатов, составляется акт. В «Журнал регистрации документов с грифом «Коммерческая тайна» вносятся соответствующие отметки об утрате. При увольнении сотрудника, ответственного за документы с грифом «Коммерческая тайна», производится проверка числящихся за ним документов и их передача вновь назначенному лицу. Акт приёма – передачи этих документов утверждается руководителем предприятия или его заместителем. При прекращении трудовых отношений с предприятием, на котором сотрудник был допущен к коммерческой тайне, обязательства о неразглашении конфиденциальных сведений действуют в течение двух лет, если иной срок не установлен трудовым договором. При передаче дел в архив на документы с грифом «Коммерческая тайна» составляется отдельная опись. Архивное хранение таких документов производится в опечатанных коробках, в помещениях, исключающих несанкционированный доступ. На документы с грифом «Коммерческая тайна», отобранные для уничтожения, составляется акт, утверждаемый руководителем предприятия. Уничтожаются документы в присутствии комиссии с помощью специальной машины или иным способом, исключающим возможность восстановления имеющейся в них информации. Руководитель предприятия по согласованию со службой безопасности может устанавливать дополнительные меры защиты документов по собственному усмотрению, например, ограничение круга должностных лиц, имеющих доступ к конфиденциальным сведениям, использование технических средств для обеспечения сохранности документов

Цель проверки наличия документов, и носителей конфиденциальной информации — установление их реального соответствия записям в учетных формах, сохранности, целостности и комплектности материалов и определение правильности выполнения процедур и операций по их учету, хранению и использованию.

Проверка стимулирует тщательное соблюдение всеми сотрудниками фирмы требований по работе с конфиденциальными документами, обеспечение их физической сохранности и, в конечном счете, - информационную безопасность организации.

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 организации.

Нерегламентированные проверки осуществляются при смене руководителей подразделений организации, увольнении сотрудника, после завершения экстремальной ситуации, выявления факта возможной утраты информации и в других случаях. Этот вид проверки обычно ограничивается конкретной частью конфиденциальных материалов.

Ежедневные проверки (самопроверки или проверки вторым работником) наличия конфиденциальных документов проводятся в конце рабочего дня всеми сотрудниками организации, работающими с конфиденциальным материалами. Квартальные и годовые проверки наличия проводят специально назначаемая комиссия; по результатам эти проверок составляется акт.

Отсутствие конфиденциального документа, дела или носителя информации у сотрудника, которому они были выданы, считается утратой этих материалов. В подобном случае комиссия составляет акт и немедленно докладывает об утрате первому руководителю организации для принятия решения.

Следовательно, процесс исполнения, дальнейшего движения и использования изданных конфиденциальных документов более сложен в технологическом отношении, чем аналогичный процесс обработки открытых документов, и требует четкого выполнения рассмотренных стадий, этапов и процедур в указанной последовательности, что дает возможность защитить ценную информацию и ее носителей от возможных потенциальных и реальных угроз. Этой же цели служат регулярные проверки наличия документов, и носителей информации.

1.3. Особенности архивной работы с документами

ограниченного доступа

В архиве составляется схема размещения документов и дел и план эвакуации на случай чрезвычайного происшествия. Оба этих документа согласовываются с руководителем режимного отдела (службы безопасности) и утверждаются руководителем архива.

Дальнейшее перемещение документов внутри архива производится только с разрешения руководителя архива.

Ознакомление с документами ограниченного доступа производится в режимном помещении только с разрешения руководителя организации или иного должностного лица.

В архиве организации должна проводиться проверка наличия документов и дел, но не реже 1 раза в 5 лет. Такая проверка должна проводиться не только в плановом порядке, но и в случае перемещения (перевода) архива в другое (другие) хранилища, после чрезвычайных происшествий (стихийное бедствие, несанкционированное проникновение в архивохранилище посторонних лиц и т.п.), при смене лица, ответственного за хранение документов, а также при ликвидации организации.

Остановимся более подробно на этом виде архивных работ.

Проверка наличия документов и дел осуществляется комиссионно. Состав комиссии (не менее 2 работников) поименно объявляется письменным приказом руководителя организации. Одновременно этим же приказом определяются задачи и сроки проведения проверки (сроки должны быть максимально сжатые и, по возможности, не превышать 1 календарного месяца).

Многолетняя практика большинства архивов подтверждает, что наиболее целесообразно осуществлять проверку "двойками": один проверяющий работает с учетными документами (описью), другой - визуально проверяет наличие и состояние хранения дел на месте, сличая архивный шифр и заголовок каждой единицы хранения с записью в описи и не прибегая, без особой необходимости, к полистному просмотру архивных документов. Все записи об отсутствующих единицах хранения, недостатках в их физическом состоянии и т.п. производятся в ходе проверки на отдельных листах (листах проверки наличия документов) вплоть до завершения проверки по одной конкретной описи.

Обнаруженные, так называемые "закладки", то есть нарушения в последовательном (по архивным номерам) расположении дел по данной описи, дела из другой описи или из другого фонда, устраняются немедленно, и обнаруженные "чужие" дела раскладываются по своим местам хранения. По окончании работы по одной описи выясняются причины и обоснованность отсутствия отмеченных единиц хранения (по записям в журнале выдачи (высылки) дел, контрольным карточкам, переписке и т.д.).

Итоговые документы по результатам проверки наличия архивных документов оформляются по завершении этой работы в масштабе всего архива, включая краткосрочный поиск выявленных необоснованно отсутствующих дел. Каждый акт проверки наличия утверждается руководителем архива (режимного отдела, собственной безопасности). Общие итоги докладываются руководителю организации с докладной запиской о необнаруженных делах и предлагаемых мерах по их розыску. Все документы по проверке приобщаются в дела фондов.

По завершении вышеизложенного комплекса мероприятий архив осуществляет меры по розыску, а также изыскивает возможности по устранению выявленных недостатков в физическом состоянии дел и отдельных документов.

При работе с документами ограниченного доступа очень важно организовать Соответствующий режим хранения этих документов, доступа к ним и их использования.

Помещения, в которых ведутся работы с документами ограниченного доступа и где данные сведения хранятся в нерабочее время, являются режимными.

Для контроля за входом могут устанавливаться шифрованные и электронные замки, автоматические турникеты, камеры видео наблюдения. Данные помещения должны быть оборудованы основном администрированном здании учреждения, предприятия, организации в зоне размещения кабинетов аппарата руководства.

Режимные помещения должны оборудоваться замками по средством пожарной и охранной сигнализации, выведенными на пульт дежурного, на пост охраны административного здания.

Доступ в эти помещения должен быть строго ограничен. В режимные помещения допускаются руководитель организации, его заместитель по режиму, начальник режимного отдела, а также лица, которые имеют прямое отношение к ведущимся в этих помещениях работам. Доступ других лиц в эти помещения может быть разрешен в случае служебной необходимости одним из перечисленных руководителей. С целью ограничения доступа посторонних лиц в режимное помещения оборудуются окном для выдачи и приема документов, выходящим в отдельный тамбур, либо часть помещения оборудуется барьером. Для хранения документов помещения снабжаются необходимым количеством сейфов и металлических шкафов. Большое количество документов ограниченного доступа может храниться в отдельном специально выделенном хранилище на открытых стеллажах при условии персональной ответственности одного работника за сохранность этих документов.

Если перед вскрытием данных помещений обнаружено нарушение целостности печатей и неисправность замков, то помещения не вскрываются, составляется акт о случившимся и немедленно докладывается руководителю организации, начальнику подразделения и службе безопасности. Принимаются меры по охране помещений до прибытия службы безопасности.

В организациях на случай чрезвычайного происшествия (пожар, авария, стихийное бедствие и т.п.) разрабатывается специальная инструкция, утверждаемая руководителем организации, в которой предусматривается порядок вызова должностных лиц, вскрытия режимных помещений, очередность и порядок спасения техники, документов ограниченного доступа и места дальнейшего их хранения. Инструкция должна находится у дежурного по организации, в службе безопасности и непосредственно в режимном помещении. Она не должна раскрывать состава вывозимых документов. С ней должны быть под расписку ознакомлены все заинтересованные и задействованные для этих целей работники и должностные лица. Для спасения документов каждое режимное помещение обеспечивается необходимым количеством специальной тары (мешками, чехлами, специальными контейнерами и т.д.).

В случае чрезвычайного происшествия в нерабочее время, при создании угрозы уничтожения документов дежурный по организации вместе с подразделением охраны имеет право вскрыть режимные помещения и принять меры к спасению техники и документов в соответствии с вышеуказанной инструкцией. О вскрытии помещений составляется соответствующий акт, который подписывается лицами, вскрывшими данные помещения.

1.4. Особенности изъятия и уничтожения документов, дел ограниченного доступа

в документационном обеспечение управления

Изъятие из дела документов или перемещение их из одного дела в другое производится в исключительных случаях, с оставлением в деле справки-заместителя, и только с разрешения начальника подразделения.

В случае безвозвратного изъятия из дела документов во внутренней описи дела и формах учета делаются соответствующие отметки. При изъятии из дел документов, зарегистрированных по журналам учета прошлых лет, они должны быть вновь зарегистрированы в журнале учета текущего года с отметкой об этом в справке-заместителе.

Отметки в деле об изменении количества листов при безвозвратном изъятии документов производятся на обложке дела, во внутренней описи и заверительном листе. При изъятии документов листы дела перенумерации не подлежат. В соответствии со статьей 183 Уголовно-процессуального кодекса РФ выемка документов, содержащих государственную или иную охраняемую федеральным законом тайну, производится следователем с санкции прокурора, а выемка документов, содержащих информацию о вкладах и счетах граждан в банках и иных кредитных организациях, производится на основании судебного решения, принимаемого в порядке, установленном статьей этого же Кодекса. До начала выемки следователь предлагает выдать документы, подлежащие изъятию, а в случае отказа производит выемку принудительно.

Первичные учетные документы бухгалтерского учета могут быть изъяты только органами дознания, предварительного следствия и прокуратуры, судами, налоговыми инспекциями и налоговой полицией на основании их постановлений в соответствии с законодательством Российской Федерации.

В организации должен быть установлен порядок, исключающий ознакомление посторонних лиц с уничтожаемыми документами (делами), неполное их уничтожение, позволяющее восстановить их содержание, а также случайное уничтожение не подлежащих уничтожению документов (дел).

Уничтожать документы и дела ограниченного доступа необходимо путем сжигания, расплавления, дробления, растворения или химического разложения, превращения в мягкую бесформенную массу и порошок. Допускается также уничтожение документов путем измельчения в кусочки в бумагоуничтожающей машине площадью не более 2,5 мм2.

Если перед уничтожением из дел изымаются отдельные документы, необходимые для дальнейшей работы, в акте указывается, какие документы и из каких дел изъяты (регистрационные номера и наименование документов, номера дел и листов), а также в какие дела и за какими номерами листов подшиты изъятые документы или зарегистрированы по журналам текущего года. В журналах учета делается отметка о новом местонахождении документов, а в акте на уничтожение указывается фактическое количество оставшихся листов дела, подлежащих уничтожению. Дела уничтожаются вместе с внутренними описями после обязательной полистной сверки с записями актов и внутренними описями дел.

Контроль за работой с документами ограниченного доступа осуществляют руководитель организации, его заместитель по режиму, руководитель режимного отдела (службы безопасности), а также руководители самостоятельных подразделений. В случае, если в организации циркулируют сведения, составляющие государственную тайну, то контрольные функции осуществляют также органы государственной безопасности.

За разглашение сведений, составляющих государственную тайну, утрату документов, содержащих такие сведения, а также за иные нарушения режима и порядка работы с этими документами виновные лица привлекаются к ответственности в соответствии с действующим законодательством:

а) за разглашение сведений, составляющих государственную тайну, утрату документов, содержащих такие сведения, виновные лица привлекаются к уголовной ответственности в соответствии с Уголовным кодексом РФ;

б) за разглашение сведений, составляющих служебную тайну, утрату документов, содержащих такие сведения, либо за иные нарушения режима виновные лица привлекаются к дисциплинарной ответственности и могут быть отстранены от выполнения таких работ с этими документами, а за передачу иностранным организациям или их представителям сведений, составляющих служебную тайну, - к уголовной ответственности.

В соответствии со статьей 139 Гражданского кодекса РФ лица, незаконными методами получившие информацию, которая составляет служебную или коммерческую тайну, обязаны возместить причиненные убытки. Такая же обязанность возлагается на работников, разгласивших служебную или коммерческую тайну вопреки трудовому договору.  
Согласно статье 857 Гражданского кодекса РФ в случае разглашения банком сведений, составляющих банковскую тайну, клиент, права которого нарушены, вправе потребовать от банка возмещения причиненных убытков.

2. ТЕХНОЛОГИЯ РАБОТЫ С ДОКУМЕНТАМИ ОГРАНИЧЕННОГО ДОСТУПА В ФГОУ СПО «ПРИМОРСКИЙ ПОЛИТЕХНИЧЕСКИЙ КОЛЛЕДЖ»

2.1. Краткая характеристика и структура ФГОУ СПО «Приморский политехнический колледж»

Приморский политехнический колледж был открыт 14 апреля 1988 года, но на самом деле его история началась 12 февраля 1953 года, - именно тогда был открыт во Владивостоке строительный техникум Министерства обороны СССР.

В 1954 году был сделан первый набор на три специальности: «Промышленное и гражданское строительство», «Санитарно-техническое устройство зданий», «технология изготовления железобетонных конструкций».

С 1959 по 1965 год проводился набор на вечернее и заочное отделение, а в 1965 году было принято решение о закрытии вечернего и заочного отделений и расширении дневного. С 1968 года в техникум набираются только учащиеся, имеющие полное среднее образование, ежегодный набор – 240 человек.

До 1960 года техникум располагался в двухэтажном здании казармы по ул. Флотской, 37, в котором было всего 8 аудиторий, лаборатория химии и строительных материалов, актовый зал на 140 чел. И библиотека. В 1960 году техникум получил новое просторное здание по ул. Геологов, 4, (ныне прапорщика Комарова, 4,), а в 1965 году было построено общежитие на 300 мест.

В 1970 году во Владивостоке на базе Главного управления по строительству «Главвладивостокстрой» открылся еще один строительный техникум. До 1988 года оба техникума подготовили около 9 тысяч специалистов. А в 1988 году на базе двух строительных техникумов был создан Приморский политехнический техникум, где и сегодня работаю многие преподаватели и сотрудники Владивостокских строительных техникумом.

Федеральное государственное образовательное учреждение среднего профессионального образования «Приморский политехнический колледж» реализует программы среднего профессионального образования, профессиональной подготовки, переподготовки и повышения квалификации и дополнительного образования на основании свидетельства о государственной аккредитации, в соответствии с выданной ему лицензией на право ведения образовательной деятельности и наделен правом выдавать выпускникам диплом государственного образца о среднем профессиональном образовании и свидетельство о профессиональной подготовке.

Основной целью деятельности Колледжа является оказание образовательных услуг наилучшего качества, открытие новых специальностей с учетом экономических и социальных условий жизни, востребованности специалистов на рынке труда, государственных и межгосударственных требований и стандартов.

Высшим управляющим звеном учреждения является директор. Директор несет ответственность за организацию бухгалтерского учета, соблюдения действующего законодательства при выполнении финансово-хозяйственных операций и хранение бухгалтерской документации.

Непосредственное руководство учебной, хозяйственной и финансовой деятельностью осуществляют заместители директора и главный бухгалтер, назначенные директором по согласованию с учредителем. На заместителей директора и главного бухгалтера возлагается планирование и организация учебно-методической; социально-экономической; административно-хозяйственной работы; руководство работой отделений, лабораторий, кабинетов, отделов и контроль в пределах своей компетенции.

Рис. 1

Организационная структура

ФГОУ СПО «Приморский политехнический колледж»

Социальный педагог, организатор, преподаватели

Хозяйственная служба, охранная служба

Бухгалтерский отдел

Зам. директора по воспитательной работе

Зам. директора по общим вопросам

Главный бухгалтер

Отдел кадров

Зам. директора по экономике

Зам. директора по производственному обучению

Мастера, преподаватели, зав. отделениями

Преподаватели, методисты,

Зав. отделениями

Зам. директора по учебной части

ДИРЕКТОР

Архив

2.2 Описание структурного подразделения – отделения экономики и сервиса,

и рабочего места

Отделение экономики и сервиса ФГОУ СПО «Приморский политехнический колледж», является структурным подразделением колледжа, реализует профессиональные образовательные программы среднего и дополнительного профессионального образования в соответствии с нормативными документами и правовыми актами, определяющими деятельность ФГОУ СПО «Приморский политехнический колледж».

В своей деятельности Отделение экономики и сервиса руководствуется Конституцией Российской Федерации, федеральными законами, нормативными и правовыми актами, регламентирующими деятельность ФГОУ СПО «Приморский политехнический колледж» в соответствии с его Уставом.

Отделение экономики и сервиса осуществляет подготовку специалистов при наличии учебно-материальной базы и преподавательского состава, необходимых для подготовки высококвалифицированных специалистов.

Количественный состав студентов определяется типовым положением об отделении и включает в себя не менее 200 человек по одной или нескольким родственным специальностям.

Отделение экономики и сервиса имеет печать «отделение экономики и сервиса» установленного образца, ведет делопроизводство в пределах предоставленных ему полномочий.

Основными задачами отделения экономики и сервиса являются:

* Удовлетворение потребностей в квалифицированных специалистах со средним профессиональным образованием;
* Осуществление подготовки специалистов по специальностям: 100105 «Гостиничный сервис», 230103 «Автоматизированные системы обработки информации и управление», 080110 «Экономика и бухгалтерский учет», 032202 «Документационное обеспечение управления и архивоведение»;
* Повышение образовательного уровня студентов, в том числе путем оказания дополнительных платных образовательных услуг.

Отделение экономики и сервиса несет ответственность за качество обучения, жизнь и здоровье обучающихся, соблюдение государственных требований к минимуму содержания и уровню подготовки выпускников в соответствии с Уставом ФГОУ СПО «Приморский политехнический колледж» и другими локальными актами.

Реорганизация или ликвидация отделения экономики и сервиса осуществляется на основании решения Совета колледжа в соответствии с уставом ФГОУ СПО «Приморский политехнический колледж».

Непосредственное управление отделением экономики и сервиса возлагается на заведующего отделением, назначаемого Директором колледжа из числа работников, имеющих высшее образование и опыт учебно-методической работы.

Заведующий отделением:

* Осуществляет управление отделением экономики и сервиса в соответствии с законодательством РФ, Уставом ФГОУ СПО «Приморский политехнический коллеж», Положением об отделении экономики и сервиса, Должностной инструкцией, регламентирующей его деятельность, приказами и распоряжениями Директора колледжа;
* Представляет интересы отделения экономики и сервиса в пределах, делегированных ему прав по поручению Директора колледжа или его заместителя по учебной работе;
* Издает распоряжения, касающиеся образовательного процесса на отделении экономики и сервиса, в пределах своей компетенции и прав, делегированных ему директором колледжа;
* Участвует в работе общего собрания, Совета колледжа, педагогического совета, информирует преподавательский состав отделения экономики и сервиса обо всех решениях, принимаемых органами самоуправления колледжа;

Организация рабочего места – это система мероприятий по оснащению рабочего места средствами и предметами труда. Основными факторами при разработке планировки являются технология и характер выполняемых работ, взаимосвязи секретаря в процессе труда.

Примерный перечень оргтехники и средств вычислительной техники, применяемых в работе секретаря:

* средства малой оргтехники (письменные принадлежности: ручки, бумага, карандаши, ластики и т. п.);
* средства составления и изготовления текстовых документов (пишущие машины, ПЭВМ, диктофон, принтер, сканер);
* средства обработки бумажных документов (склеивающие и скрепляющие машины, конвертовскрывающее и резательное оборудование, адресовальное и штемпевальное оборудование, машина для уничтожения документов);
* средства хранения и поиска документов (картотеки различного типа, шкафы и полки, сейфы);
* средства связи (телефон, радиотелефон, радио, телетайп, факс, локальные конторские сети, средства оперативной диспетчерской связи, электронная почта, модем);
* копировальные средства и аппараты; офисная мебель и оборудование.

Средства малой оргтехники необходимы при любом уровне автоматизации работы секретаря.

Из средств составления и изготовления текстовых документов все чаще используется компьютер, даже при очень небольшом документообороте. Созданные с его помощью документы имеют более привлекательный вид благодаря наличию различных шрифтов и цветового оформления, что не может не сказаться на отношении к документу и помогает создать благоприятное впечатление об авторе документа.

Диктофоны бывают, необходимы, когда имеет смысл бесшумное и точное отображение звуковой информации.

Сканер – устройство для считывания текстовой и графической информации – удобное средство при перепечатывании большого количества текстовой информации.

Перечисленные средства обработки документов требуются секретарю или экспедиционной службе, канцелярии при большом объеме документооборота.

Средства хранения и поиска документов необходимы для сохранности документов от внешних источников повреждения (пыли, влаги, солнечных лучей, механического воздействия), а также для ориентации и быстрого поиска нужной информации. Эти средства по возможности должны гармонировать с обстановкой рабочего места секретаря.

Средства связи могут быть объединены в единый комплекс (например, телефон – факс – модем), должны иметь компактный вид и спокойные, приятные для слуха средства оповещения о начале связи.

Копировальные аппараты подбираются в зависимости от объема работ, необходимого качества копий и других параметров.

Офисная мебель и оборудование должны соответствовать требованиям эргономики, антропометрии, дизайна.

При создании раздела «Рабочий день секретаря» необходимо учитывать, что рабочий день секретаря подвержен резким переменам. Но, тем не менее, как бы, ни влияли внешние факторы на работу, одними из ее главных правил остаются:

* постепенное вхождение в работу;
* ритмичность труда;
* обязательное чередование труда и отдыха;
* планирование работы.

Даже если не удается сделать что-то запланированное, то в любом случае это гораздо лучше, чем импровизация. Планирование, может быть, надень или неделю, месячное, квартальное или годовое.

Объективная основа четкого планирования – это наличие в работе секретаря достаточно большого количества стабильных, часто повторяющихся процедур и операций. Необходимым эффективным средством планирования рабочего дня секретаря и руководителя является еженедельник, в котором дела разносятся по датам.

Можно для этих целей использовать календарь типа Lotus Organizer, установленный на персональном компьютере, который называют личной информационной системой, предназначенной для эффективной организации рабочего времени. В ее состав помимо календаря входят телефонный справочник, адресная книга, блокнот и т.д. Но даже при наличии Lotus Organizer для дублирования информации необходимо иметь обычный ежедневник или периодически производить распечатку каких-то данных из Lotus Organizer. При планировании работ секретарь должен знать, что наиболее благоприятное время для выполнения творческих или трудных заданий – с 10 до 12 часов. Затем следует некоторый спад активности, во второй половине дня от 14 до 17 часов работоспособность наиболее высока, а потом она неуклонно падает, поэтому после 18 часов возможность ошибок в работе весьма высока. Повторяющиеся изо дня вдень работы рекомендуется планировать на одно и то же время рабочего дня, например, обработка полученной корреспонденции, приходится, как правило, наутро.

Необходимо организовать свой рабочий день таким образом, чтобы в течение всего рабочего времени помогать руководителю.

Примерная схема рабочего дня секретаря:

Первая половина рабочего дня:

* Прийти на работу за 10 мин до руководителя, для того чтобы проверить состояние рабочих мест (своего и руководителя), привести себя в порядок, составить или уточнить план на предстоящий день.
* Подобрать в соответствии с планом нужные документы и дела.
* Получить корреспонденцию, ознакомиться с содержанием и зарегистрировать. Отложить документы, требующие первоочередного решения руководителя.
* По остальным документам подготовить варианты возможных ответов или распределить их по исполнителям.
* Просмотреть поступившие обзоры, отчеты, приглашения и т. д. Даты и время проведения всех мероприятий записать в своем дневнике-календаре.
* Разложить поступившую корреспонденцию в зависимости от срочности исполнения. Телеграммы, срочные факсы и телефонограммы немедленно передать руководителю.
* Оставить у себя документы, необходимые для текущей информационно - справочной работы.
* Доложить руководителю о полученной корреспонденции.
* Уточнить вместе с руководителем содержание намечаемых мероприятий на текущий день.
* Передать по телефону и лично указания руководителя соответствующим исполнителям и напомнить об истекающих сроках исполнения документов.
* Работа с посетителями, телефонные переговоры.
* Подшивка исполненных документов вдела.
* Выполнение работ на компьютере.
* Организация копирования документов в соответствии с указанием руководителя.

Вторая половина дня:

* Продолжение работы с посетителями и телефонных переговоров.
* Сбор и подготовка для подписи исполненных документов.
* Доклад руководителю об исполненных документах, получение от него обработанных им документов.
* Обработка и отправка исходящих документов.
* Планирование мероприятий наследующий день.

Окончание рабочего дня:

* Просмотр своего дневника и информация соответствующих отделов о необходимости подготовки к проведению определенных мероприятий.
* Если руководитель остается работать после окончания рабочего дня – обеспечение его всей необходимой информацией, материалами.
* Приведение в порядок своего рабочего места (убрать документы, закрыть на ключ сейф и все шкафы с документами, выключить из сети электронное и техническое оборудование).

В табличной форме может быть представлен процесс обмена секретарем информацией со внешними и внутренними «корреспондентами» (подразделениями, ответственными исполнителями, вышестоящими организациями и др.):

Таблица 1

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Получаете | | | Передаете | | |
| Автор информации | Содержание | Сроки и периодичность получения | Автор информации | Содержание | Сроки и периодичность получения |
| 1 | 2 | 3 | 4 | 5 | 6 |

В отдельной таблице можно зафиксировать все информационные связи секретаря и руководителя.

Учитывая, что такие разделы обучающей инструкции, как «Взаимоотношения секретаря» и «Ответственность», принципиально не отличаются от должностной инструкции.

2.3. Составление, изготовление и издание

конфиденциального документа в

ФГОУ СПО «Приморский политехнический колледж»

Под исполнением конфиденциального документа понимается процесс документирования управленческих решений и действий, результатов выполнения руководителями и сотрудниками колледжа 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 попадают законодательные акты, организационно-правовые, нормативные, распорядительные, справочно-информационные документы, разнообразные рекламные издания и научно-техническая информация.

Процесс ознакомления с конфиденциальным документом – это информирование сотрудника колледжа или иного заинтересованного лица, осуществляемое в соответствии с резолюцией полномочного руководителя (директора колледжа либо его заместителей) на конфиденциальном документе, о принятом этим руководителем решении или решении другой организационной структуры.

В ходе исполнения конфиденциальных документов могут возникнуть следующие основные угрозы:

* Утрата (разглашение, утечка) ценной информации за счет ее документирования на случайном носителе;
* Подготовка к изданию документа, не обосновавшего деловой необходимостью или неразрешенного для издания, т.е. документирования определенной информации;
* Включение в документ избыточных конфиденциальных сведений, что равносильно разглашению тайны колледжа;
* Случайное или умышленное занижение грифа конфиденциальности сведений, включенных в документ;
* Изготовление документа в условиях, которые не гарантируют сохранность носителя, конфиденциальность информации;
* Утеря оригинала, черновика, варианта или редакции документа, его части, приложения к документу;

Важно, что в отличие от исполнения открытых документов исполнение конфиденциальных документов представляет собой стадию, насыщенную различными технологическими этапами и процедурами, основными из которых являются:

* Установление уровня грифа конфиденциальности сведений, подлежащих включению в будущий документ;
* Оформление и учет носителя для документирования выделенного комплекса конфиденциальной информации;
* Составление и изготовление конфиденциального документа, и его издание;

Общеизвестно, что в наибольшей безопасности находится конфиденциальная информация, не зафиксированная на каком-либо носителе; ценная информация немедленно подвергается угрозе при возникновении необходимости ее документирования.

В связи с этим система защиты конфиденциальной информации в ФГОУ СПО «Приморский политехнический колледж» начинает функционировать не после издания (подписания) конфиденциального документа, а заблаговременно, т.е. до создания будущего документа.

Прежде чем издать документ, следует установить, является ли данная информация конфиденциальной и какой уровень грифа конфиденциальности ей должен быть присвоен в случае положительного ответа.

Своевременное установление грифа конфиденциальности сведений, подлежащих включению в будущий документ, - первый и основной элемент защиты документированной информации, позволяющий обеспечить относительно надежную безопасность тайны колледжа.

Основу присвоения документу грифа конфиденциальности должны составлять: перечень конфиденциальных сведений колледжа, требования партнеров, а также перечень конфиденциальных документов колледжа.

Система грифования (маркирования) документов не гарантирует сохранность информации, однако, позволяет четко организовать работу с документами, 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.

Гриф располагается, в соответствии с ГОСТ Р. 6.30-2003, 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.

Документы и информация, конфиденциальные в целом, в своей массе (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.

Изменение или снятие грифа конфиденциальности документа производится при изменении степени конфиденциальности и ценности содержащихся в нем сведений.

Основными задачами учета носителей конфиденциальной информации (или, как часто их называют в научной литературе, документов предварительного учета) являются:

* закрепление факта присвоения носителю (например, обычным листам бумаги, дискете и др.) 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.

Все типы носителей конфиденциальной документированной информации должны быть учтены до начала составления проектов черновика, вариантов и беловика будущего документа.

При этом в колледже соблюдаются следующие условия защиты информации ограниченного доступа:

* 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.

Информация всегда передается в письменном виде за подписью директора колледжа фирмы с соблюдением порядка обращения с отправляемыми конфиденциальными документами. Передача конфиденциальных сведений в устной форме не разрешается.

Обязательно учитываются проекты подготовленных конфиденциальных электронных документов, 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 неконфиденциального документа, если приложение не содержит защищаемых сведений.

Цель этапа изготовления конфиденциального документа- 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 в ФГОУ СПО «Приморский политехнический колледж» решаются следующие задачи:

* предотвращение несанкционированного изготовления конфиденциального документа кем-либо из сотрудников колледжа, 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 изготовляется черновик, проект документа и его варианты, контроля за сохранностью и порядком уничтожения испорченных носителей за счет установления информационной связи различных форм учета, например учета носителя, учета черновика и изготовленного проекта документа, инвентарного учета и др.;
* обеспечение оперативных и результативных проверок наличия, комплектности и подлинности документов за счет нанесения на проект документа учетных и защитных отметок.

Сотрудники ФГОУ СПО «Приморский политехнический колледж», 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;
* ежедневно по окончании рабочего дня проверять наличие документов и сдавать их на хранение;
* немедленно сообщать первому директору колледжа или другому его непосредственному руководителю об утрате или недостаче документов, обнаружении лишних или неучтенных документов, отдельных листов;

Работа с конфиденциальными документами разрешается сотрудникам колледжа на рабочих местах, но только при наличии условий, исключающих возможность утраты документа или хищения информации. При отсутствии этих условий сотрудники колледжа работают с конфиденциальными традиционными и электронными документами, делами и базами данных в специально предназначенном для этого помещении.

Сотрудникам не разрешается хранить конфиденциальные документы, дела, дискеты в ящиках рабочего стола, неприспособленных шкафах. Дела, закрепленные за конкретным исполнителем, могут иметь индивидуальные цветовые отличия, позволяющие выявлять факты несанкционированного обращения к этим делам другого сотрудника.

Всем сотрудникам колледжа, 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);
* знакомиться с документами, делами и базами данных других сотрудников, работать с их компьютерами без письменного разрешения директора колледжа или его непосредственного заместителя;
* переписывать сведения из документов в личные дневники, карточки учета работы, календари, еженедельники и т. п;
* выносить из здания колледжа любые документы без письменного разрешения директора колледжа;
* составлять документы на рабочем столе или работающий компьютер при любом по длительности выходе из помещения;
* 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 об известных ему элементах обеспечения безопасности фирмы и персонала.

Любое санкционированное или несанкционированное обращение к электронной конфиденциальной информации должно регистрироваться (протоколироваться). Применение персоналом собственных защитных мер при работе с компьютером не допускается.

Рациональная организация работы с конфиденциальными сведениями, соблюдение сотрудниками фирмы установленных правил обращения с конфиденциальными документами, делами и базами данных, к которым они допущены, сами по себе в значительной степени защищают тайну колледжа от посягательств злоумышленника.

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 ими установленного порядка работы с конфиденциальными материалами, их хранения, правильности ведения внутренней описи документов, находящихся у исполнителя, своевременности и полноты ежедневной сдачи всех материалов.

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 акт и немедленно докладывает об утрате первому руководителю фирмы для принятия решения.

2.4. Учет, хранение и использование носителей

конфиденциальной информации в

ФГОУ СПО «Приморский политехнический колледж»

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 задачами, решаемыми при выполнении процедур и операций формирования и ведения дел с конфиденциальными документами (конфиденциальных дел), являются не только эффективное использование этих документов в управленческой и производственной деятельности колледжа, но и обеспечение сохранности документов, дел, массивов информации и их носителей, а также других конфиденциальных материалов в процессе хранения и использования.

В период текущего (оперативного) архивного хранения ценные и конфиденциальные материалы колледжа подвергаются таким же угрозам, как и во время, их рассмотрения, исполнения, обработки и движения.

Комплекты документов на магнитных носителя (дискетах и др.), а также архивные массивы (подмассивы) электронных документов, находящихся в компьютере, вносятся в номенклатуру дел на общих основаниях. Закрепление дел за конкретными исполнителя Рациональная организация работы с конфиденциальными сведениями, соблюдение сотрудниками фирмы установленных правил обращения с конфиденциальными документами, делами и базами данных, к которым они допущены, сами по себе в значительной степени защищают тайну колледжа от посягательств злоумышленника.

ми 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-, видеодокументы, особо ценные документы выделенного хранения и др.

Перечень заголовков дел составляется таким образом, чтобы состав, содержание и уровень конфиденциальности документов каждого дела соответствовали функциональным обязанностям тех сотрудников колледжа, которые допущены к делу и будут с ним работать. Каждое дело должно содержать документы, имеющие приблизительно одинаковый период конфиденциальности. Под одним заголовком обычно заводится конфиденциальное и неконфиденциальное (открытое) дело.

Конфиденциальные документы комплектуются в дела с учетом того, что сведения, составляющие предпринимательскую тайну, не должны попадать в государственный архив до истечения срока их конфиденциальности.

После снятия грифа конфиденциальности документ передается в службу открытого делопроизводства и помещается в аналогичное по заголовку дело открытого доступа временного, длительного или постоянного срока хранения.

3. АНАЛИЗ ТЕХНОЛОГИИ РАБОТЫ С ДОКУМЕНТАМИ ОГРАНИЧЕННОГО ДОСТУПА В ФГОУ СПО «ПРИМОРСКИЙ ПОЛИТЕХНИЧЕСКИЙ КОЛЛЕДЖ»

В ходе анализа теоретической и практической части дипломной работы можно сделать вывод, что технология работы с документами ограниченного доступа в Приморском политехническом колледже ведется в соответствии с нормативно-правовыми актами Российской Федерации.

На основании нормативно-правовых актов РФ в Приморском политехническом колледже разработана и утверждена номенклатура дел. По номенклатуре дел документы ограниченного доступа находятся в отделе кадров, бухгалтерии, учебной части и архиве.

Документы ограниченного доступа по номенклатуре дел в Приморском политехническом колледже формируются в номенклатурные дела, на обложке которых указываются списки сотрудников, имеющих доступ или разрешение на ознакомление с этими делами.

В соответствии с Федеральным законом об информации, информатизации и защите информации», в Приморском политехническом колледже проводятся ежегодные проверки документов, дел ограниченного доступа.

Проверка проводится специальной комиссией, назначаемой директором колледжа, в составе не менее трех сотрудников из числа лиц, имеющих прямое отношение к проверяемым документам и соответствующий допуск к данным работам, с обязательным включением в ее состав работников режимного отдела (службы безопасности).

По результатам проверки составляется акт, утвержденный руководителем подразделения, о результатах проверки сообщают директору Приморского политехнического колледжа.

3.1. Учет документов ограниченного доступа в

Приморском политехническом колледже

Учет документов ограниченного доступа в Приморском политехническом колледже производится в соответствии с основными нормативно-право РФ.

Каждый документ ограниченного доступа, поступивший в Приморский политехнический колледж, будь то пакет с документами, отдельный бумажный или машинописный документ, поступивший путем электронной или факсимильной почты, регистрируются в журналах учета входящей документации. Аналогичным образом регистрируются сведения куда-либо направляемые, в журнале регистрации исходящей документации.

Следовательно, учет документов ограниченного доступа делится на ряд видов регистрации этих документов: инвентарный, номенклатурный, пакетный.

Также как в любой другой организации, в Приморском политехническом колледже при любом виде учета конфиденциальных документов выполняются следующие процедуры:

* индексирование документов;
* первичная регистрация сведений, находящихся в документе;
* последующая запись рабочих сведений л документе;
* сохранность документов и учетных форм.

3.2. Архивная работа с документами ограниченного доступа в Приморском политехническом колледже

В Приморском политехническом колледже есть специальное помещение отведенное под архив для хранения документов. Составлена схема размещения документов и дел в архиве и план эвакуации на случай чрезвычайного происшествия.

Хранение документов ограниченного доступа производится в специальных сейфах, которые находятся в отделе кадров, учебной части, в кабинете директора, в бухгалтерии. За каждым сейфом закреплено ответственное лицо, которое отвечает за наличие и сохранность документов в этом сейфе. Сейфы закрепляются и опечатываются. Помещения в котором находятся сейфы оборудованы сигнализацией. если перед вскрытием данных помещений обнаружена неисправность замков или какие-либо другие нарушения, то помещения не вскрываются, случившиеся происшествие активизируется, и незамедлительно сообщается в службу безопасности и директору Приморского политехнического колледжа. Принимаются строгие меры по охране этого помещения до прибытия службы безопасности. В Приморском политехническом колледже разработана специальная инструкция на случай ЧП, в которой предусмотрен порядок вызова ответственных лиц за вскрытие режимного помещения, т.е. помещения находятся под сигнализацией, Также в этой инструкции определяется очередность и порядок эвакуации, документов ограниченного доступа и места дальнейшего их хранения. Каждое режимное помещение обеспечено необходимым количеством специальной тары для эвакуации.

В соответствии со всем выше сказанным, можно сделать вывод, что технология работы с документами ограниченного доступа в ФГОУ СПО «Приморский политехнический колледж», производится в соответствии со всеми нормативно-правовымит актами.

ЗАКЛЮЧЕНИЕ

Проанализировав все вышесказанное можно сделать вывод, что в ФГОУ СПО «Приморский политехнический колледж», технология работы с документами ограниченного доступа ведется в соответствии со всеми нормативно-правровыми актами, методиками и законами Российской Федерации.

В заключение следует сказать, что для обеспечения сохранности и неразглашения конфиденциальных сведений предприятия необходимо выполнение самых простых требований безопасности, профессиональное обучение персонала требованиям работы с конфиденциальными документами, материальное стимулирование руководством организации сотрудников, имеющих доступ к документам с грифом «Коммерческая тайна», правильная организация секретного делопроизводства и документооборота на предприятии. Строгое привлечение к ответственности сотрудников предприятия за нарушение норм и инструкций по секретному делопроизводству. Сведения к минимуму несанкционированного доступа к конфиденциальной документации можно достичь путём увеличения различных административных, технологических и других барьеров. Это делается для того, чтобы организация хищения (разглашения) конфиденциальных сведений предприятия влекло за собой значительные финансовые, материальные и иные траты, которые неоправдывали бы риск и затраченные на это усилия.

На взгляд автора дипломной работы, данное условие сильно бы сократило несанкционированные утечки конфиденциальных сведений организации, что, конечно, и дорогостояще, но в наше время бы сильно помогло предприятиям конкурировать, в конце концов, на рынке.

БИБЛИОГРАФИЯ

1. Федеральный закон «Об информации, информатизации и защите информации» № 24-ФЗ от 20 февраля 1995 г. (в ред. От 10 января 2003 г.) // СЗ РФ. 1995 № 8. СТ. 609; СЗ РФ. 2003. № 2. Ст. 167.
2. Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне» (в ред. От 06.10.1997 № 131-ФЗ, от 30.06.2003 № 86-ФЗ, от 11.11.2003 № 153-ФЗ, от 29.06.2004 № 58-ФЗ, от 22.08.2004 № 122-Фз, с изм. от 27.03.1996 № 8-П, от 10.11.2002 № 293-О, от 10.11.2002 № 314-О).
3. Указы Президента РСФСР «Об архивах Комитета государственной безопасности СССР», «О партийных архивах» от 21.08.1991 // Сов. Архивы. 1992. № 1.
4. Приказ Роскомархива от 18.08.1992 № 176 «О примерном положении, об архиве государственного учреждения, организации, предприятия».
5. Примерный договор между учреждением государственной архивной службы РСФСР организацией, предприятием о взаимоотношениях и сотрудничестве в области архивного дела и делопроизводства.
6. ГОСТ Р 51141-98. Делопроизводство и архивное дело. Термины и определения. - М., 1998.
7. Государственная система документационного обеспечения управления. Общие требования к документам и службам документационного обеспечения управления. М., 1991.
8. Типовая инструкция по делопроизводству в федеральных органах исполнительной власти. М., 2001
9. Примерное положение о центральной экспертной комиссии (ЦЭК) министерства, ведомства Российской Федерации (утв. Приказом Росархива № 19 от 17.03.1998). М.: Росархиф, 2000.
10. Типовая инструкция по делопроизводству в федеральных органах исполнительной власти (утв. Приказом Росархива от 27.11.2000 № 68).
11. Басаков М.И., Замыцкова О.И., Делопроизводство. 3-е издание, переработано и дополнено – Ростов Н/Д: Феникс, 2005.
12. Бергено Я.Я., Кирсанова М.В., Основы технологии делопроизводства – М.: ИНФРА-М; Новосибирск: Сибирское соглашение, 2005.
13. Белов А.Н., Белов А.А., Делопроизводство и документооборот. – М.: издательство Эксмо, 2005.
14. Волкова К.А., Казакова Ф.К., Предприятие: Положения об отделах и службах, должностные инструкции. - М.: Экономика, 2001.
15. Дёмин Ю.М., Делопроизводство. Подготовка служебных документов. 2-е издание, дополнено и переработано – СПб.: Питер, 2005.
16. Квалификационный справочник должностей руководителей, специалистов и других служащих / Минтруд России. - М.: Экономические новости, 1998.
17. Кирсанов М.В., Современное делопроизводство. 4-е издание. – М.: ИНФРА-М; Новосибирск: Сибирское соглашение, 2006.
18. Кирсанова М.В., Аксенов Ю.М., Курс делопроизводства: Документационное обеспечение управления. 6-е издание, исправлено и дополнено – М.: ИНФРА-М; Новосибирск: Сибирское соглашении, 2006.
19. Космотаров  М. Н. - Секретарское дело №4/2001- С.28-32.
20. Кудряев В.А., Организация работы с документами: Учебник– М.: ИНФРА-М, 1998.
21. Кузнецова Т.В., Делопроизводство (Документационное обеспечение управления). 4-е издание, исправленное и дополненное – М.: ООО «Журнал «Управление персоналом», 2003.
22. Кузнецова Т.В. Делопроизводство. – М.: ЮНИТИ-ДАНА, 2001.
23. Мингалев В.С. Общие закономерности и тенденции документообразования в социально-экономических системах управления (Проблемы изучения): Учеб. пособие. М., 1993.
24. Охотников А.В., Булавина Е.А. Документоведение и делопроизводство. 2-е издание, переработано и дополнено – М.: ИКЦ «МарТ»; Ростов н/Д: издательский центр «МарТ», 2005.
25. Павлюк Л. В., Киселева Т. И., Воробьев Н. И. Справочник по делопроизводству, архивному делу и основам работы на компьютере. Санкт Петербург Издательский торговый дом «Герда», 1998.
26. Печникова Т.В., Печникова А.В., Практика работы с документами в организации. – М.: Ассоциация авторов и издателей «Тандем». Издательство ЭКМОС, 2000.
27. Рогожин М.Ю. Документационное обеспечение управления (Практическое пособие). – М.: издательство РДЛ, 2003.
28. Рогожин М.Ю. Документационное обеспечение управления. 2-е издание, переработано и дополнено – М.: издательство РДЛ, 2006.
29. Румынина Л.А. Документационное обеспечение управления. 3-е издание, исправленное – М.: Издательский центр «Академия», 2005.
30. Труханович А.В., Щур Д.Л., Справочник по кадровому делопроизводству. – 3-е изд., перераб. и доп. – М.: Издательство «Днло и Сервис», 2005. – 640 с.