МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

УО «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра технологии и важнейших отраслей промышленности

РЕФЕРАТ

по дисциплине: Технология и автоматизация делопроизводства

на тему:

**Обеспечение безопасности информации на наиболее уязвимых участках офисной деятельности**

Студент В.П. Герасименко

ФП, 2-й курс, ДПХ-3

Проверила: С.В. Некраха

ст. преподаватель

Минск 2009

Содержание

Введение

1. Защита информации при проведении переговоров

2. Защита информации в работе кадровой службы

Список использованных источников

# **Введение**

Словосочетание "информационная безопасность" в разных контекстах может иметь различный смысл. В Доктрине информационной безопасности Российской Федерации термин "информационная безопасность" используется в широком смысле. Имеется в виду состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

В Законе РФ "Об участии в международном информационном обмене" информационная безопасность определяется аналогичным образом – как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

В данном курсе наше внимание будет сосредоточено на хранении, обработке и передаче информации вне зависимости от того, на каком языке (русском или каком-либо ином) она закодирована, кто или что является ее источником и какое психологическое воздействие она оказывает на людей. Поэтому термин "информационная безопасность" будет использоваться в узком смысле, так, как это принято, например, в англоязычной литературе.

Под информационной безопасностью мы будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры. (Чуть дальше мы поясним, что следует понимать под поддерживающей инфраструктурой.).

Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Таким образом, правильный с методологической точки зрения подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем (ИС). Угрозы информационной безопасности – это оборотная сторона использования информационных технологий.

# **1. Защита информации при проведении переговоров**

Совещания и переговоры, в процессе которых могут обсуждаться сведения, составляющие тайну фирмы или ее партнеров, именуются обычно конфиденциальными. Порядок проведения подобных совещаний и переговоров регламентируется специальными требованиями, обеспечивающими безопасность ценной, в том числе конфиденциальной, информации (далее — ценной информации), которая в процессе этих мероприятий распространяется в санкционированном (разрешенном) режиме. Основной угрозой ценной информации является разглашение большего объема сведений о новой идее, продукции или технологии, чем это необходимо.

Причины, по которым информация может разглашаться на конфиденциальных совещаниях или переговорах, общеизвестны: слабое знание сотрудниками состава ценной информации и требований по ее защите, умышленное невыполнение этих требований, провоцированные и не провоцированные ошибки сотрудников, отсутствие контроля за изданием рекламной и рекламно-выставочной продукции и др. Оглашение ценной информации в санкционированном режиме должно быть оправдано деловой необходимостью и целесообразностью для конкретных условий и характера обсуждаемых вопросов.

Основные этапы проведения конфиденциальных совещаний и переговоров: подготовка к проведению, процесс их ведения и документирования, анализ итогов и выполнения достигнутых договоренностей.

Плановые и неплановые конфиденциальные совещания, проходящие без приглашения посторонних лиц, проводятся первым руководителем, его заместителями, ответственными исполнителями (руководителями, главными специалистами) по направлениям работы с обязательным предварительным информированием референта. По факту этого сообщения или проведения такого совещания референтом заводится учетная карточка описанной выше формы. Проведение конфиденциальных совещаний без информирования референта не допускается.

Доступ сотрудников фирмы на любые конфиденциальные совещания осуществляется на основе действующей в фирме разрешительной системы доступа персонала к конфиденциальной информации. Приглашение на конфиденциальные совещания лиц, не являющихся сотрудниками фирмы, санкционируется только в случае крайней необходимости их личного участия в обсуждении конкретного вопроса. Присутствие их при обсуждении других вопросов запрещается.

Ответственность за обеспечение защиты ценной информации и сохранение тайны фирмы в ходе совещания несет руководитель, организующий данное совещание. Референт оказывает помощь руководителям и совместно со службой безопасности осуществляет контроль за перекрытием возможных организационных и технических каналов утраты информации.

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

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

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

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

Перед началом конфиденциального совещания сотрудник службы безопасности обязан убедиться в отсутствии в помещении несанкционированно установленных аудио- и видеозаписывающих или передающих устройств и в качественной работе средств технической защиты на всех возможных каналах утечки информации. Помещение должно быть оборудовано кондиционером, так как открытие окон, дверей в ходе совещания не допускается. Окна закрываются светопроницаемыми шторами, входная дверь оборудуется сигналом, оповещающим о ее неплотном закрытии, В целях звукоизоляции целесообразно иметь двойную дверь (тамбур) или зашторивать двери звукопоглощающей тканью.

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

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

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

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

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

* вносить в помещение, в котором проводится совещание, фото-, кино- и видеоаппаратуру, компьютеры, магнитофоны, плееры, диктофоны, радиоприемники, радиотелефоны и другую аппаратуру, пользоваться ею;
* делать выписки из документов, используемых при решении вопросов на совещании и имеющих гриф ограничения доступа;
* обсуждать вопросы, вынесенные на совещание, в местах общего пользования;
* информировать о совещании (вопросах повестки дня, составе участников, времени и месте проведения, ходе обсуждения вопросов, содержании решений и т. п.) любых лиц, не связанных с проведением данного совещания, в том числе сотрудников фирмы.

Участники совещания, замеченные в несанкционированной аудио- или видеозаписи, использовании средств связи, фотографировании, лишаются права дальнейшего присутствия на совещании. По факту составляется акт, копия которого направляется фирме, представителем которой является данное лицо, или передается первому руководителю фирмы — организатора совещания, если это лицо является сотрудником последней. Одновременно носитель несанкционированно записанной информации передается референту для учета и хранения (или уничтожения). Устройство записи возвращается владельцу. Участники совещания не могут оглашать больший объем ценных сведений, чем это было установлено при подготовке совещания, или сообщать сведения, не относящиеся к обсуждаемому вопросу. Состав оглашаемых сведений регламентируется руководителем, организовавшим совещание.

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

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

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

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

При ведении переговоров не следует сразу же передавать партнеру всю запрашиваемую им информацию в полном объеме. Прежде всего следует выяснить, с какой целью ему необходимы эти сведения и как знание этих сведений отразится на ходе дальнейшего сотрудничества с ним. На этом этапе переговоров, при выяснении сути взаимных намерений, целесообразно строить дискуссию таким образом, чтобы ответы на вопросы были максимально лаконичными («да — нет», «можем — не можем»). Рекламно-выставочные материалы (проспекты, пресс-релизы, прайс-листы, брошюры и т. п.) следует рассматривать как контролируемый канал распространения ценных сведений. При этом следует помнить, что этот канал тщательно и глубоко анализируется конкурентом с целью выявления тех сведений, которые составляют тайну фирмы, издавшей рекламные материалы.

Защита информации в рекламно-выставочной деятельности предусматривает заблаговременный анализ, экспертизу предназначенной для широкого оглашения любой информации о деятельности фирмы и ее продукции в целях обнаружения в содержании или элементах отображения этой информации (таблицах, формулах, рисунках, фотографиях, схемах) конфиденциальных сведений или намека на наличие таких сведений. Подобная информация должна, как правило, анализироваться от противного — с точки зрения того интереса, который будет проявлен к ней конкурентами, и объема полезных сведений, извлекаемых конкурентом из ее содержания. Материалы, не прошедшие экспертизы, публикации не подлежат. Экспертиза включает также последующий контроль всех опубликованных о фирме материалов, сообщений средств массовой информации, рекламных изданий и рекламно-выставочных проспектов. Помимо этого, анализируются подобные материалы других фирм для определения возможной утраты ценных сведений. Рекламно-выставочные издания не должны сигнализировать недобросовестному конкуренту о том, что и где искать.

Чтобы предотвратить разглашение ценных сведений в рекламно-выставочных материалах, следует заблаговременно:

* проанализировать множество предполагаемых к изданию и изданных материалов с точки зрения возможности извлечения из них ценных конфиденциальных сведений;
* осуществить разбиение (дробление) информации на части и распределение их между разными рекламно-выставочными материалами, предназначенными для массового посетителя и посетителей-специалистов, издать серию дополнений к основному проспекту для специалистов разного профиля;
* осуществить разбиение информации по видам и средствам рекламы — традиционным бумажным изданиям, электронной рекламе, Web-странице, рекламе в средствах массовой информации и др.

Вместе с тем должен соблюдаться разумный баланс: рекламно-выставочные материалы не должны быть мало информативными для посетителей, все наиболее важные параметры новой продукции должны найти в них отражение.

Следовательно, подготовка и проведение совещаний и переговоров по конфиденциальным вопросам, оформление их результатов связаны с выполнением ряда обязательных процедур, необходимых для правильной организации работы устроителей и участников этих мероприятий. При несоблюдении изложенных требований возникает серьезная опасность разглашения или утечки ценных сведений и секретов фирмы, ее партнеров и клиентов. Контроль за выполнением этих требований возлагается на референта, который обеспечивает информационную безопасность деятельности фирмы, сохранение ее деловых и производственных секретов.

# 2. Защита информации в работе кадровой службы

Работа службы персонала, управления или отдела кадров, менеджера по персоналу, иногда, в некрупных фирмах, секретаря-референта (далее — отдела кадров) связана с накоплением, формированием, обработкой, хранением и использованием значительных объемов сведений о всех категориях сотрудников. Эти сведения относятся к так называемым персональным данным, которые по своей сути отражают личную или семейную тайну граждан, их частную жизнь и входят в круг информации, подлежащей защите от несанкционированного доступа.

Личная тайна гражданина охраняется Конституцией Российской Федерации. Разглашение этой тайны т. е. бесконтрольное распространение персональных данных во времени и пространстве, может нанести значительный ущерб физическому лицу. Понятие личной тайны близко примыкает к семейной тайне. Семейная тайна или тайна нескольких физических лиц, членов семьи не тождественна личной тайне по составу защищаемых сведений. Например, к семейной тайне относятся: тайна усыновления, тайна отцовства, тайна наследственного заболевания и др.

Под персональными данными (информацией о гражданах) понимается любая документированная информация, относящаяся к конкретному человеку. Персональные данные идентифицируют его личность. Субъектами персональных данных являются граждане Российской Федерации, иностранные граждане и лица без гражданства, находящиеся на территории России, к личности которых относятся соответствующие персональные данные. Держатели персональных данных — органы государственной власти и местного самоуправления, предприятия, учреждения, организации, юридические и физические лица, осуществляющие владение и пользование этими данными. Пользователями персональных данных могут быть органы государственной власти и местного самоуправления, предприятия, учреждения, организации, юридические и физические лица, обращающиеся к держателю данных за получением необходимых им персональных данных и пользования ими без права передачи.

Персональные данные всегда относятся к категории конфиденциальной информации. Не допускаются сбор, передача, уничтожение, хранение, использование и распространение информации о частной жизни, а равно информации, нарушающей личную тайну, семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений физического лица без его согласия, кроме как на основании судебного решения. Режим конфиденциальности персональных данных снимается в случаях обезличивания этих данных или по истечении 75лет срока их хранения, если иное не определено законом.

В целях выявления состава конфиденциальных сведений и определения основных направлений защиты персональных данных в отделе кадров выделим две большие группы документации: а) документация по организации работы отдела и б) документация, образующаяся в процессе основной деятельности отдела и содержащая персональные данные в единичном или сводном виде.

Первая группа документации содержит организационно-правовую документацию отдела кадров и включает: положение об отделе, должностные инструкции работников отдела, приказы, распоряжения, указания руководства фирмы, регламентирующие структуру отдела и распределение сфер ответственности между его работниками, рабочие инструкции по выполнению основных функций отдела, ведению документации и формированию персональных данных в комплексы (документы, базы данных и т. п.). Сюда относятся также дела с документацией по планированию, учету, анализу и отчетности в части основной деятельности отдела. Учитывая значительное своеобразие в формировании статуса отдела и организации основных процессов, сопровождающих его деятельность в различных фирмах, конфиденциальный характер этой группы документации определяется тем, что злоумышленник может извлечь из анализа этой документации в конкретной фирме следующие полезные для себя сведения:

* распределение функций между отделом кадров и планово-финансовым отделом, бухгалтерией, юридическим отделом, военно-учетным столом и другими подразделениями, т. е. сведения о том, где искать требуемую информацию;
* распределение функций внутри отдела кадров между структурными единицами отдела (группами, секторами) и между работниками, т. е. сведения о том, у кого искать требуемую информацию;
* регламентацию рабочего процесса по оформлению документации, пропусков, удостоверений, т. е. сведения о том, как можно воспользоваться этим в несанкционированном режиме для фальсификации документов, баз данных;
* регламентацию места хранения документов, дел, баз данных, т. е. сведения о том, где и как можно украсть или подменить тот или иной документ, получить требуемую информацию;
* регламентацию отчетной и справочной работы, т. е. сведения о том, когда и как можно перехватить требуемую информацию по организационным или техническим каналам.

Любые посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе кадров. Следует также учитывать, что работник отдела кадров не должен быть осведомлен о порядке работы других сотрудников этого отдела.

Вторая группа — документация, образующаяся в процессе основной деятельности отдела кадров и содержащая персональные данные, включает:

* комплекты документов, сопровождающие процесс оформления трудовых правоотношений гражданина (при решении вопросов о приеме на работу, переводе, увольнении и т. п.);
* комплекты материалов по анкетированию, тестированию, проведению собеседований с кандидатами на должность;
* подлинники и копии приказов по личному составу;
* личные дела и трудовые книжки сотрудников;
* дела, содержащие основания к приказам по личному составу;
* дела, содержащие материалы аттестации сотрудников, служебных расследований и т. п.;
* справочно-информационный банк данных по персоналу — учетно-справочный аппарат (картотеки, журналы, базы данных и др.);
* подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству предприятия, руководителям структурных подразделений и служб;
* копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения.

Главным моментом в защите персональных и иных конфиденциальных данных является четкая регламентация функций работников отдела кадров и в соответствии с этим — регламентация принадлежности работникам документов, дел, карточек, журналов персонального учета и баз данных.

Для реализации этого положения руководитель фирмы должен издать приказ или распоряжение о закреплении за работниками отдела определенных массивов документов, необходимых им для информационного обеспечения функций, указанных в должностных инструкциях этих работников, утвердить схему доступа работников отдела кадров и руководящего состава фирмы, структурных подразделений к документам отдела, ввести личную ответственность перечисленных должностных лиц и работников за сохранность и конфиденциальность персональных данных.

По каждой функции, выполняемой работником отдела кадров, должен быть регламентирован состав документов, дел и баз данных, с которыми этот работник имеет право работать. Не допускается, чтобы работник мог знакомиться с любыми документами и материалами отдела. Целесообразно, в целях разграничения доступа и разбиения знания персональных данных между работниками, закрепить за разными работниками:

а)документирование оформления трудовых правоотношений (приема, перевода, увольнения и др.);

б)ведение личных дел и трудовых книжек;

в)составление и хранение приказов по личному составу и контрактов;

г)ведение справочно-информационного банка данных.

Распределение сфер деятельности может варьироваться в зависимости от объема работы и штатной численности работников отдела, но разграничение обязанностей и массивов документации должно быть обязательно. Это позволит построить работу отдела в соответствии с указанными выше основополагающими принципами и обеспечить сохранность и конфиденциальность персональных данных. В случае необходимости перераспределения обязанностей среди работников отдела (например, при болезни одного из них, увольнении) должно быть издано соответствующее распоряжение начальника отдела кадров, в котором регламентируются характер изменений, их срок и дополнения в систему доступа к документам, делам и базам данных. Важно, что в этом распоряжении фиксируется изменение степени осведомленности работников в знании ими персональных данных и сферы личной ответственности за сохранность и конфиденциальность документации.

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

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

В часы приема посетителей работники отдела не должны выполнять функции, не связанные с приемом, вести служебные и личные переговоры по телефону. На столе работника, ведущего прием, не должно быть никаких документов, кроме тех, которые касаются данного посетителя. В помещении отдела кадров в часы приема посторонних лиц может находиться работник службы безопасности фирмы. Целесообразно также наличие сигнализации, оповещающей сотрудников этой службы о необходимости немедленно вмешаться в сложившуюся ситуацию. На столе работника отдела не должно быть тяжелых предметов.

Прием посетителей чаще всего связан с ведением справочной работы: ответов на вопросы посетителей и выдачей им справок.

Ответы на вопросы даются только лично тому лицу, которого они касаются. Не допускается передача персональной информации по телефону. Ответы на письменные запросы других учреждений, фирм и организаций даются в письменной форме, на бланке фирмы или отдела кадров и в том объеме, который позволяет не разглашать излишний объем персональных сведений.

При выдаче справки с места работы необходимо удостовериться в личности сотрудника, которому эта справка выдается. Не разрешается выдавать ее родственникам или сослуживцам лица, которому требуется справка. Справка выдается на основании учетной карточки Т-2, а не пропуска, так как сотрудник при увольнении мог не сдать пропуск или удостоверение. Справку подписывает начальник отдела кадров. На подпись справку передает работник отдела, а не посетитель. Одновременно начальник отдела ставит на справке печать. За получение справки сотрудник предприятия расписывается в журнале учета выдачи справок.

Чистые бланки справок подлежат обязательному учету. Они хранятся у начальника отдела кадров и выдаются в дневной норме работнику, выдающему справки. По окончании приемных часов этот работник отчитывается перед начальником отдела об израсходованных бланках справок и сдает ему оставшиеся чистые и испорченные бланки. Заранее ставить на чистых бланках справок подпись начальника отдела и печать не допускается.

В целях удобного доступа посетителей в отдел кадров помещения отдела должны располагаться на первом этаже здания, поблизости от входа. В часы приема лиц, не являющихся сотрудниками предприятия, вход в отдел должен быть свободным для всех желающих. Проход посторонних лиц в помещение отдела контролируется сотрудником службы безопасности: посетитель идентифицируется по паспорту или служебному удостоверению, при необходимости посетителя провожают. Не допускается бесконтрольное нахождение посторонних лиц в здании фирмы.

Отдел кадров должен иметь три смежных помещения: комнату для работников отдела, кабинет начальника отдела и помещение, в котором размешаются шкафы и сейфы для документов, дел и картотек. Вход в отдел кадров может быть только один. Для ожидающих приема посетителей целесообразно выделить дополнительное помещение за пределами основных помещений отдела. Помещение для размещения шкафов может не иметь окон и оборудуется эффективными техническими средствами пожаротушения. Все помещения оборудуются охранной сигнализацией.

Сдачу на охрану и снятие с охраны помещений отдела кадров осуществляет начальник отдела или его заместитель. Уборка помещений допускается только в присутствии этих лиц. Мусор, выносимый из помещений, должен сжигаться.

Подбор персонала для работы в отделе кадров ведется с учетом требований, которые разработаны для должностей, связанных с владением и обработкой конфиденциальных сведений и документов.

# Список использованных источников

1. Корнеев И.К., Степанов Е.А. Защита информации в офисе / И.К. Корнеев. – Москва: Изд-во Проспект, 2008. – 336 с.
2. Мельников В.В. Защита информации в компьютерных системах. — М.:

Финансы и статистика, <Электронинформ>, 1997. — 368с.

1. Энциклопедический словарь [Электронный ресурс]. – Режим доступа: www.wikipedia.ru. – Дата доступа: 25.09.2009.
2. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. М.: Изд–во Агентства "Яхтсмен", — 1996. — 192 с.