МИНИСТЕРСТВО ФИНАНСОВ МОСКОВСКОЙ ОБЛАСТИ

КОРОЛЁВСКИЙ ИНСТИТУТ УПРАВЛЕНИЯ, ЭКОНОМИКИ И СОЦИОЛОГИИ

Информационно-технологический факультет

Кафедра информационной безопасности

**Курсовая работа**

По дисциплине: «Организационная защита информации»

На тему**: «Особенности увольнения сотрудников, владеющих конфиденциальной информацией»**

г. Королёв

2011

**Введение**

В данной курсовой работе детально описывается особенности Увольнения сотрудников фирмы владеющих конфиденциальной информацией, а так же работы с ними особенности приёма и перевода на работу связанную с конфиденциальной тайной.

**1. Особенности увольнения сотрудников, владеющих конфиденциальной информацией**

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

Технологическая цепочка увольнения сотрудника включает в себя:

• написание сотрудником заявления об увольнении с подробным раскрытием причины увольнения и желательно указанием места предполагаемой работы;

• передача заявления руководителю структурного подразделения для оформления и передачи в отдел кадров или службу персонала;

• прием службой конфиденциальной документации от увольняющегося сотрудника всех числящихся за ним документов, баз данных, носителей информации, изделий, материалов, с которыми он работал, проверка их комплектности, полноты и оформление приема в описи исполнителя или актом;

• сдача сотрудником пропуска (идентификатора) для входа в рабочую зону, всех ключей и печатей, запрещение сотруднику входить в рабочее помещение с использованием знания шифра кодового замка (при необходимости - изменение кода);

• проведение сотрудником службы безопасности или службы персонала беседы с сотрудником с целью напоминания ему об обязательстве сохранения в тайне тех сведений, которые ему были доверены по службе в фирме, предупреждение сотрудника о запрещении использования этих сведений в интересах конкурента или в личных целях, выяснение причины увольнения и места новой работы;

• подписание сотрудником обязательства о неразглашенииим конфиденциальных сведений после увольнения;

• документальное оформление увольнения в соответствии с общими правилами;

• прием от сотрудника пропуска для входа в здание фирмы, выдача ему трудовой книжки и расчета по заработной плате, сопровождение его до выхода из здания сотрудником службы безопасности.

После сдачи всех документов и материалов сотруднику запрещается входить в режимную рабочую зону. При необходимости у него может быть изъят пропуск (идентификатор) сотрудника и выдан идентификатор посетителя с правом входа только в определенные административные помещения.

Беседа с увольняющимся сотрудником имеет целью предотвратить утрату информации или ее неправильное использование бывшим сотрудником в результате его природной или умышленной забывчивости. Следует напомнить увольняющемуся сотруднику, что он подписывал при поступлении на работу обязательство (подписку) о неразглашении фирменных секретов.

Ему напоминают, что и после увольнения из фирмы по крайней мере в течение года за его деятельностью будет осуществляться наблюдение. Предупреждение включается в обязательство, которое подписывает увольняющийся сотрудник.

В практике США аналогичный порядок рекомендуется применять в отношении консультантов, экспертов и временно работавших сотрудников. По крайней мере от них целесообразно в обязательном порядке потребовать письменное обязательство о неразглашении ставших известными им фактов и сведений, запрещении использования их в своей деятельности или работе конкурирующих фирм в течение определенного времени.

Эффективным средством против разглашения фирменных секретов в США считается заключение соглашения о предоставлении увольняющимся сотрудником консультационных услуг фирме в течение ряда лет. В течение этого времени, т.е. срока конфиденциальности известных ему сведений, ему выплачивается жалованье, близкое по размерам к зарплате. В результате бывший сотрудник противостоит соблазну использовать тайну фирмы в своих интересах.

Ущерб от увольнения сотрудника резко уменьшается, если тайна фирмы раздроблена и известна по частям достаточно большому числу служащих. В этом случае не приходится прибегать к указанным выше сложным и часто мало эффективным способам защиты тайны, известной уволенным сотрудникам.

В любом случае рекомендуется по истечении трех месяцев после увольнения направить бывшему сотруднику письмо-напоминание о необходимости сохранения тайны фирмы.

Если руководству фирмы стали известны случаи несанкционированного использования бывшим сотрудником конфиденциальных сведений или ноу-хау фирмы, следует начать активное судебное разбирательство выявленных фактов.

Рассмотренная технология оформления увольнения сотрудников, владеющих ценными и конфиденциальными сведениями, позволит не только повысить ответственность всего персонала за сохранность доверенных им сведений, но и предотвратить факты кражи увольняющимися сотрудниками ценной информации, ограничить возможность использования ее в других организациях и фирмах

**2. Особенности работы с персоналом владеющим конфиденциальной тайной. Персонал как основная опасность утраты конфиденциальной информации**

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

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

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

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

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

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

Работа с персоналом подразумевает целенаправленную деятельность руководства фирмы и трудового коллектива, направленную на наиболее полное использование трудовых и творческих способностей каждого члена коллектива, воспитание в нем фирменной гордости, препятствующей возникновению желания нанести вред организации, стать соучастником в недобросовестной конкуренции или криминальных действиях.

Человеческий фактор должен постоянно учитываться в долговременной стратегии фирмы и ее текущей деятельности, являться основным элементом построения действенной и эффективной системы защиты информационных ресурсов.

**3. Организационные мероприятия по работе с персоналом**

Организационные мероприятия по работе с персоналом, получающим доступ к конфиденциальной информации, можно разделить на несколько групп:

• проведение усложненных аналитических процедур при приеме и увольнении сотрудников;

• документирование добровольного согласия лица не разглашать конфиденциальные сведения и соблюдать правила обеспечения безопасности информации;

• Инструктирование и обучение сотрудников практическимдействиям по защите информации;

А контроль за выполнением персоналом требований по защите информации, стимулирование ответственного отношенияк сохранению конфиденциальных сведений. Сложности в работе с персоналом определяются:

• большой ценой решения о допуске лица к тайне предприятия;

• наличием в фирме, как правило, небольшого контингента сотрудников, служебные обязанности которых связаны с использованием конфиденциальных сведений (руководители, ответственные исполнители, сотрудники службы конфиденциальной документации);

• разбиением тайны на отдельные элементы, каждый из которых известен определенным сотрудникам в соответствии с направлением их деятельности.

Персонал является основным и самым трудно контролируемым источником ценной и конфиденциальной информации.

Источник, который мы именуем «Персонал и окружающие фирму люди», включает в себя:

• всех сотрудников данной фирмы, ее персонал;

• сотрудников других фирм - посредников, изготовителей комплектующих деталей, торговых фирм, рекламных агентств и т.п.);

• сотрудников государственных учреждений, к которым фирма обращается в соответствии с законом - налоговых и иных инспекций, муниципальных органов, правоохранительных органов и т.д.;

• журналистовсредств массовой информации, сотрудничающих с фирмой;

• посетителей фирмы, работников коммунальных служб, почтовых служащих, работников служб экстремальной помощи и т.д.;

• посторонних лиц, работающих или проживающих рядом со зданием или помещениями фирмы, уличных прохожих;

• родственников, знакомых и друзей всех указанных выше лиц. Перечисленные лица в той или иной мере являются или могут стать в силу обстоятельств источниками конфиденциальных сведений. Каждый из источников, особенно ставший им случайно, может стать опасным для фирмы в результате несанкционированного разглашения (оглашения) защищаемых сведений.

Наиболее осведомлены в секретах фирмы первый руководитель, его основной заместитель, их референты и секретари, работники службы конфиденциальной документации.

Следовательно, персонал фирмы, владеющий ценной и конфиденциальной информацией, работающий с конфиденциальными делами и базами данных, является наиболее осведомленным и часто достаточно доступным источником для злоумышленника, желающего получить необходимые ему сведения. Причем овладение требуемой информацией происходит в значительном числе случает в результате безответственности и необученности персонала, его недостаточно высоких личных и моральных качеств.

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

Процессу приема сотрудника на работу предшествует ряд подготовительных этапов, которые позволяют составить точное представление о том, какой специалист и какой квалификации действительно нужен для данной должности, какими деловыми, моральными и личными качествами он должен обладать. Особенно это касается должностей, связанных с владением конфиденциальной информацией. Можно выделить следующие этапы:

• предварительно сформулировать, какие функции должен выполнять сотрудник, каков круг его ответственности, какие качества, знания и уровень квалификации необходимо иметь претенденту;

• составить перечень ценных и конфиденциальных сведений, с которыми будет работать специалист;

• составить перечень форм поощрения и стимулирования,которые может получать сотрудник;

• составить другие перечни вопросов, которые необходимо будет решать специалисту, перечни его личных качеств, возрастных, профессиональных и иных характеристик;

• составить описание должности - документ аналогичный по структуре должностной инструкции, который определяет требования к кандидату на должность (но это документ - вспомогательный).

Выполнение указанных этапов облегчит процедуру подбора кандидатов и сделает отбор их более обоснованным и объективным. Кандидаты предварительно знакомятся с указанными выше документами, что делает собеседование с ними более целенаправленным и конкретным. Кроме того, ознакомившись с документами, кандидат может отказаться от предлагаемой работы. Описание вакантной должности имеет для работодателя примерно такое же значение, как и резюме для кандидата.

Поиск кандидата на вновь создаваемую или вакантную должность в фирме не должен носить бессистемный характер. Случайный человек, пришедший с улицы, в определенной степени таит опасность для фирмы как с точки зрения его профессиональной пригодности, так и личных, моральных качеств. Особую опасность подобный метод подбора представляет для должностей, связанных с владением конфиденциальной информацией или материальными ценностями. Случайные претенденты на должность обычно рассылают или разносят по предприятиям, учреждениям и фирмам свое резюме. Им не важно, где работать, их просто интересует работа по данной специальности.

С другой стороны, случайный человек не всегда плох и поэтому данный метод при подборе персонала является наиболее распространенным и объективно завоевал право на существование. Но дело в том, что он не Должен быть единственным.

Помимо пассивного ожидания прихода нужного человека, существует ряд эффективных направлений активного поиска кандидатов на вакантную должность или рабочее место. К числу основных направлений можно отнести следующие:

1. Поиск, кандидатов внутри фирмы, особенно если речь идет о руководителе или специалисте высокого уровня. Этот метод дает возможность продвигать перспективных работников по служебной лестнице и заинтересовывать их работой, воспитывать преданность делам фирмы. Можно приглашать на должность лицо, ранее работавшее в фирме и хорошо себя зарекомендовавшее.

Перераспределение персонала в соответствии с его склонностями и способностями всегда дает большой положительный эффект в улучшении работы фирмы и обеспечении ее информационной безопасности. Но надо учитывать, что поддерживается коллективом только такое продвижение по службе, которое определяется высокими деловыми качествами работника. Не может получить одобрения персонала выдвижение плохого работника, в частности по принципу личных связей или знакомства.

Большим преимуществом этого метода является то, что о кандидате достаточно много известно всему коллективу и судить о профессиональных, моральных и личных качествах, соответствии предлагаемой должности можно на основании достаточно обширного опыта.

Метод имеет недостаток, который состоит в том, что без притока новых людей коллектив теряет свои новаторские качества. Новые люди - это новые идеи, предложения и перспективы развития.Тем не менее этот метод является наилучшим и наиболее надежным при подборе кандидата на должность, связанную с владением ценной и конфиденциальной информацией.

2. Поиск кандидатов среди студентов и выпускников учебных заведений, установление связей с подразделениями вузов, занятыми трудоустройством выпускников. Можно иметь достаточно полную информацию о профессиональных и личных качествах студентов. Очень эффективно вести поиск (даже на средних курсах) наиболее способных студентов, привлекать их в процессе учебы к работе в организации, отплачивать их труд и, может быть, финансировать обучение в вузе, платить стипендию. Коллектив фирмы должен регулярно омолаживаться. Это лекарство от застоя идей, путь к успеху.

3. Обращение в государственные и частные бюро, агентства по найму рабочей силы, биржи труда, организации по трудоустройству лиц, уволенных по сокращению штатов, трудоустройству молодежи, бывших военнослужащих и т.п. Подобные агентства предлагают требуемый контингент работников на имеющиеся рабочие места, ведут целенаправленный поиск необходимого специалиста высокой квалификации, организуют переподготовку специалистов по индивидуальным заказам.

При обращении в агентство необходимо составить перечень служебных обязанностей и требований к нужному работнику, без указания конфиденциальных сведений, с которыми будет связана работа.

4. Рекомендации работающих в фирме сотрудников. Обычно такие рекомендации отличаются ответственным и взвешенным характером, так как с рекомендуемыми людьми сотрудникам придется работать вместе.

Указанные направления поиска кандидатов на должности, связанные с владением конфиденциальной информацией, как правило, позволяют выбрать необходимых работников из ряда лиц, изъявивших желание занять вакантную должность.

Технологическая цепочка приема сотрудников, работа которых связана с владением ценной и (или) конфиденциальной информацией, включает следующие процедуры:

• подбор предполагаемого кандидата (кандидатов) для приема на работу или перевода, получение резюме;

• изучение резюме (и личного дела, если кандидат работает на фирме) руководством фирмы, структурного подразделения и службой персонала, вызов для беседы подходящих кандидатов;

• информирование кандидатов, работающих в фирме, об их будущих должностных обязанностях, связанных с владением тайной фирмы;

• знакомство (предварительное собеседование) руководства фирмы, структурного подразделения и службы персонала с кандидатами, не работающими в фирме; беседа с ними, уточнение отдельных положений резюме; ответы на вопросы о будущей работе; изучение полученных от кандидата рекомендательных писем;

• заполнение кандидатами, не работающими в фирме, и представление в отдел кадров заявления о приеме, автобиографии, личного листка по учету кадров (с цветной фотокарточкой), копий документов об образовании, наличии ученых степей, ученых и почетных званий, передача в отдел кадров рекомендательных писем и при наличии характеристик;

• обновление материалов личного дела работающего в фирме сотрудника; получение представления о переводе на новую должность от руководителя структурного подразделения;

• собеседование кандидатов с работником отдела кадров по представленным документам, при необходимости подтверждение тех или иных сведений представлением дополнительных документов;

• опрос сотрудником отдела кадров авторитетных для фирмы лиц, лично знающих кандидата на должность, протоколирование опроса;

• собеседование экспертов с кандидатами с целью определения их личных и моральных качеств, а для неработающих в фирме сотрудников дополнительно - профессиональных способностей; рассмотрение медицинской справки;

• при необходимости - тестирование и анкетирование кандидатов;

• по совокупности собранных материалов и их анализа принятие решения руководством фирмы об отборе единственного претендента и возможности предложить ему работу, связанную с владением тайной фирмы;

• заключительное собеседование с претендентом на должность, получение от него принципиального согласия на работу с конфиденциальной информацией;

• в случае согласия - подписание претендентом обязательства о неразглашении тайны фирмы, в частности, сообщаемых ему конфиденциальных сведений; информирование претендента о характере конфиденциальной информации, с которой он будет работать, наличии системы защиты этой информации и тех ограничениях, которые придется учитывать работнику в служебной и неслужебной обстановке;

• беседа-инструктаж руководителя структурного подразделения, руководителя службы безопасности и сотрудника службы персонала с претендентом на должность; ознакомление претендента с должностной инструкцией, рабочими технологическими инструкциями, инструкцией по обеспечению информационной безопасности фирмы и другими аналогичными материалами;

• составление проекта контракта, содержащего пункт об обязанности работника не разглашать конфиденциальные сведения фирмы;

• подписание контракта о временной работе без права доступа к конфиденциальной информации;

• составление и подписание приказа о приеме на работу с испытательным сроком (или на временную работу);

• заведение личного дела на вновь принятого сотрудника;

• заполнение на сотрудника необходимых учетных форм, в том числе личной карточки формы Т-2;

• внесение фамилии сотрудника впервичные учетные бухгалтерские документы;

• внесение соответствующей записи в трудовую книжку сотрудника;

• изучение личных, моральных и профессиональных качеств сотрудника в течение испытательного срока;

• обучение сотрудника правилам работы с конфиденциальной информацией и документами, инструктажи, проверка знаний;

• анализ результатов работы сотрудника в течение испытательного срока, составление нового контракта о длительной работе и издание соответствующего приказа или отказ сотрудника в работе;

• оформление допуска сотрудника к конфиденциальной информации и документам.

Предоставленный комплект документов, из которых в дальнейшем будет сформировано личное дело сотрудника, является предметом тщательного изучения руководителями фирмы, структурного подразделения, коллегиального органа управления и службы персонала при решении вопроса о назначении данного лица на должность.

Изучение документов не должно носить формально-бюрократический характер и быть единственным критерием в решении вопроса о назначении данного лица на должность. Изучение документов следует сочетать с объективным анализом нескольких личностей, претендующих на должность, сопоставлением результатов собеседований, тестирования, опросов и т.п. Все это в совокупности позволит на конкурсной или неконкурсной основе правильно провести отбор именно того претендента на должность, который более всего отвечает составленным ранее требованиям.

Предоставленные кандидатом персональные документы тщательно проверяются на достоверность: соответствие фамилий, имен и отчеств, других персональных данных, наличие необходимых отметок и записей, идентичность фотокарточки и личности гражданина (на фотографии очки, парик - только при постоянной носке), соответствие формы бланка годам их использования, отсутствие незаверенных подчисток, исправлений, попыток замены листов, фотографий, соответствие и качество печатей и т.п. При каких-то сомнениях кандидата просят представить дубликаты испорченных документов, заверить исправления. Сведения, включенные в характеристики, рекомендательные письма, списки научных трудов и изобретений, выданные и заверенные другими учреждениями, могут быть проверены Путем обращения в эти учреждения. Документы, явно недостоверные, могут быть возвращены гражданину, и одновременно ему отказывается в рассмотрении вопроса о приеме на работу без объяснения причины отказа. Сведения, указываемые в резюме, не проверяются.

Заявление о назначении (переводе) на должность, личный листок по учету кадров, автобиография пишутся или заполняются гражданином собственноручно, без использования пишущей машинки или принтера.

Все записи, сделанные в личном листке по учету кадров, и текст автобиографии сравниваются сотрудником отдела кадров с персональными документами. Неподтвержденные записи, на которых настаивает гражданин, дополняются записью сотрудника отдела кадров «со слов гражданина». Исправления в указанных документах не допускаются.

Копии с аттестатов, дипломов, свидетельств, грамот и т.п., которые приобщаются к документам для решения вопроса о приеме на работу, снимаются с помощью копировальной техники в отделе кадров и заверяются сотрудником отдела. Копии, принесенные гражданином, внимательно сличаются с подлинником и также заверяются этим сотрудником. Нотариального заверения копий не требуется. Запрещается заверение копий с копии.

Паспорт, военный билет, дипломы, аттестаты и другие подобные персональные документы после работы с ними сотрудника отдела кадров возвращаются гражданину (кроме трудовой книжки).

При подборе персонала для работы с ценной или конфиденциальной информацией следует в первую очередь обращать внимание на личные и моральные качества кандидатов на должность, их порядочность и лишь затем - на их профессиональные знания, умения и навыки.

Важно уже на первых этапах отбора исключить те кандидатуры, которые по формальным признакам явно не соответствуют требованиям, предъявляемым к будущему сотруднику.

Собеседования с кандидатами на должность преследуют следующие цели:

• выявить реальную причину желания работать в даннойфирме;

• выявить возможных злоумышленников или попытаться увидеть слабости кандидата как человека, которые могут провоцировать преступные действия;

• убедиться, что кандидат не намерен использовать в работе секреты фирмы, в которой он раньше работал;

• убедиться в добровольном согласии кандидата соблюдать правила защиты информации и иметь определенные ограничения в профессиональной и личной жизни. Вопросники для собеседования составляются таким образом, чтобы выяснить:

• причины увольнения кандидата с прежнего места работы;

• источник информации о вакансии в данной фирме - кто подсказал, кто рекомендовал и т.п.;

• работал ли кандидат ранее с конфиденциальной информацией, подписывал ли обязательство о ее неразглашении;

• возникшие сомнения, появившиеся в связи с изучением документов кандидата;

• отношения в семье, уровень благосостояния кандидата, жилищные условия, культурный уровень и т.п.

Ответы кандидата фиксируются, и те из них, которые вызвали сомнения, уточняются путем опроса знающих кандидата лиц, путем тестирования и другими способами (если это необходимо).

При приеме на работу, связанную с информацией особой предпринимательской важности, для сбора полных сведений о кандидате могут привлекаться работники частных детективных агентств.

Одной из главных задач собеседования и тестирования является выявление несоответствия мотиваций в различных логических группах вопросов. Например: несоответствие - хочет получать большую зарплату, но раньше он получал столько же, работал близко oт дома, а хочет работать в фирме, находящейся на значительном расстоянии, и т.п.

С точки зрения безопасности психологический отбор преследует следующие цели:

• выявление имевших ранее местосудимостей, преступных связей, криминальных наклонностей;

• определение возможных преступных склонностей, предрасположенности кандидата к совершению противоправных действий, дерзких и необдуманных поступков в случае формирования в его окружении определенных обстоятельств;

• установление факторов, свидетельствующих о морально-психологической ненадежности, неустойчивости, уязвимости кандидата и т.д.

По мнению многих специалистов-психологов, основные личные качества, которыми должен обладать потенциальный сотрудник, включают:

• порядочность, честность, принципиальность и добросовестность;

• исполнительность, дисциплинированность;

• эмоциональная устойчивость (самообладание);

• стремление к успеху и порядку в работе;

• самоконтроль в поступках и действиях;

• правильная самооценка собственных возможностей и способностей;

• умеренная склонность к риску;

• умение хранить секреты;

• тренированное внимание;

• хорошая память, способности к сравнительной оценке фактов и т.д. Личные качества,не способствующие сохранению секретов:

• эмоциональная неуравновешенность;

• разочарование в себе и своих способностях;

• отчуждение от коллег по работе;

• недовольство своим служебнымположением;

• ущемленное самолюбие;

• крайне эгоистическое поведение;

• отсутствие достаточного благоразумия;

• нежелание и неспособность защищать информацию;

• нечестность;

• финансовая безответственность;

• употребление наркотиков;

• отрицательное воздействие алкоголя, приводящее к болтливости, необдуманным поступкам и т.д.

Не следует думать, что психологический отбор полностью заменяет прежние, достаточно надежные кадровые процедуры (анализ документов, собеседование, опросы сослуживцев и лиц, знающих кандидата, оперативная проверка в правоохранительных органах и т.д.). Только при умелом сочетании традиционных и психологических кадровых методов анализа можно с определенной степенью достоверности прогнозировать поведение сотрудников в различных, в том числе экстремальных, ситуациях.

Обычно отобранным для работы считается кандидат, у которого результаты анализа документов, собеседований, проверок, тестов и психологического изучения не противоречат друг другу, и не содержат данных, которые препятствовали бы приему на работу.

Материалы проверок и анализа кандидатов на должность (втомчисле вопросники и протоколы собеседований, заполненные тесты, а также используемые виды тестов и «ключи» к тестам, тестовые нормы, инструкции по проведению и интерпретации и другие подобные материалы) являются строго конфиденциальной информацией.

Обязательство о неразглашении конфиденциальной информации и сохранении тайны фирмы претендент подписывает до того, как ему будет сообщен состав ценных сведений, с которыми ему предстоит работать, и порядок защиты этих сведений.

Обязательство (подписка, соглашение) о неразглашении конфиденциальных сведений представляет собой правовой документ, которым претендент добровольно и письменно дает согласие на ограничение его прав в отношении использования конфиденциальной информации. Одновременно в обязательстве претендент предупреждается об ответственности за разглашение этой информации.

Например:

Договорноеобязательство.Обязуюсь:

1. В период оформления на работу и работы в \_\_\_\_\_\_ не разглашать сведения, составляющие ее коммерческую тайну, которые мне будут доверены или станут известны при исполнении обязанностей, собеседованиях, инструктировании и обучении.

2. Беспрекословно и аккуратно выполнять относящиеся ко мне требования приказов, инструкций и положений по защите коммерческой тайны, с которой я ознакомлен.

3. Не сообщать устно, письменно или иным способом кому бы то ни было сведений, составляющих тайну.

4. В случае отказа от работы, окончания работы или увольнения не разглашать и не использовать для себя и других лиц сведений, составляющих тайну \_\_\_\_\_\_.

Я предупрежден, что в случае нарушения данного обязательства должен возместить причиненный \_\_\_\_\_\_ ущерб или буду привлечен к дисциплинарной (вплоть до увольнения) или другой ответственности в соответствии с действующим законодательством.

Проинструктировал (подпись). Подпись лица, принимающего обязательство. Дата.

Текст обязательства может заканчиваться фразой об ознакомлении лица с его содержанием и добровольном согласии выполнять все пункты.

Многие американские фирмы включают в соглашение (обязательство) следующие пункты:

• детальное изложение принципов определения конкретных сведений, составляющих тайну фирмы;

• краткое изложение порядка охраны конфиденциальных сведений;

• изложение мер, которые должен принимать сам работник для обеспечения сохранности этих сведений;

• перечень административных наказаний, которым может быть подвергнут работник, разгласивший сведения, составляющие тайну фирмы (увольнение, понижение в должности, перевод на другую работу и т.п.).

Хорошо, если обязательство содержит пункт о том что сотрудник не будет использовать в своей деятельности информацию, принадлежащую на правах собственности фирме, в которой он ранее работал. Подобные обязательства подписывают не только претенденты на работу в данной фирме, но и все лица, тем или иным образом участвующие в работе фирмы и потенциально имеющие возможность узнать элементы тайны фирмы, например акционеры, поставщики, сотрудники работающих с фирмой рекламных и торговых структур, эксперты и т.п. Подписание обязательства о неразглашении тайны фирмы следует предусмотреть для служащих фирмы, которые не имеют непосредственного отношения к закрытым сведениям, однако имеют возможность ознакомиться с ними при исполнении служебных обязанностей (шоферы, дворники, уборщицы, сотрудники охраны и др.).

Считается, что обязательство о неразглашении тайны фирмы не дает полной гарантии сохраненияэтих сведений, однако, как показывает практика, существенно снижают риск разглашения персоналом или иными лицами этих сведений, риск незаконного их использования, а также число попыток конкурентов внедрить на фирму свою агентуру.

После подписания обязательства и проведения беседы-инструктажа с претендентом заключается трудовой договор (контракт). В контракте должен быть пункт об обязанности работника не разглашать сведения, составляющие тайну фирмы, а также конфиденциальные сведения партнеров и клиентов, об обязательстве соблюдать правила защиты конфиденциальных сведений. Может быть пункт о собственности фирмы на результаты работы сотрудника, на сделанные им изобретения и открытия и согласие сотрудника на публикацию этих достижений только с разрешения руководства фирмы. Часто содержится пункт об обязанности сотрудника сообщать в службу безопасности о всех попытках посторонних лиц получить у него конфиденциальную информацию. В обязательном порядке включается пункт об обязанности сотрудника немедленно сообщать непосредственному руководителю и службе безопасности об утере носителей конфиденциальной информации, документов, дел, конфиденциальных материалов, изделий и т.п.

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

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

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

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

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

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

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

персонал сотрудник конфиденциальный информация

**5. Доступ персонала к конфиденциальным сведениям, документам и базам данных**

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

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

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

**Принципы построения разрешительной системы доступа:**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Доступ - практическая реализация каждым сотрудником предоставленного ему допуском права на ознакомление и работу с определенным составом конфиденциальных сведений, документов и баз данных. Он санкционируется полномочным должностным лицом (первым руководителем, его заместителем, руководителем подразделения, службы или направления деятельности) в отношении конкретной информации и конкретного сотрудника. Право на выдачу такого разрешения строго регламентируется.

Разрешение (санкция) на доступ к конкретной информации может быть дано при соблюдении следующих условий:

• наличие подписанного приказа первого руководителя о приеме на работу (переводе, временном замещении, изменении должностных обязанностей и т.п.) или назначении на должность, в функциональную структуру которой входит работа

• с данной, конкретной информацией;

• наличие подписанного сторонами трудового договора (контракта)» имеющего пункт о сохранении тайны фирмы и подписанного обязательства о неразглашении ставших известными конфиденциальных сведений и соблюдении правил их защиты;

• соответствие функциональных обязанностей сотрудника передаваемым ему документам и информации;

• знание сотрудником требований нормативно-методических документов по защите информации и сохранении тайны фирмы;

• наличие необходимых условий в офисе для работы с конфиденциальными документами и базами данных;

• наличие систем контроля за работой сотрудника.

Особенность информационного обслуживания потребителей конфиденциальной информации заключается в том, что вопросы определения состава необходимой им информации решаются полномочным руководителем, а не самими потребителями. Существует общее, обязательное правило: исполнители, которым документ не адресован руководителем, не только не имеют права доступа к нему, но и не должны знать о существовании такого документа и исходных данных о нем.

Структура процедуры разграничения доступа должна быть многоуровневой, иерархической. Иерархическая последовательность доступа к информации реализуется по принципу «чем выше уровень доступа, тем уже круг допущенных лиц», «чем выше ценность сведений, тем меньшее число сотрудников может их знать». В фирме может составляться схема выдачи разрешений на доступ к массовой конфиденциальной информации. Такая схема разрабатывается с учетом двух аспектов: а) выдача разрешений в зависимости от категорий документов и б) выдача разрешений в зависимости от занимаемой должности. Графы схемы: категории документов, должностные лица, дающие разрешение, категории исполнителей, кому дается разрешение. В схеме отражаются также категории документов, с которыми знакомятся определенные категории исполнителей без специального разрешения.

Может составляться матрица полномочий, в которой по горизонтали - наименования категорий документов, по вертикали - фамилии или должности сотрудников.

Всю конфиденциальную информацию фирмы может знать только первый руководитель фирмы. Конфиденциальную информацию по конкретной работе в полном объеме вправе получать лишь соответствующий заместитель первого руководителя, руководители структурных подразделений или направлений деятельности по специальному перечню, утвержденному первым руководителем.

Необходимо добиваться минимизации для персонала привилегий по доступу к информации. При сбое в системе защиты информации или обнаружении факта утраты информации должно мгновенно вводиться ограничение на доступ или прекращение доступа к любой конфиденциальной информации до окончания служебного расследования.

Разграничение доступа основывается на однозначном расчленении информации по тематическим группам, уровням конфиденциальности этих групп и пользователям, которым эта информация необходима для работы. Задачей процедуры разграничения доступа является регламентация минимальных потребностей персонала в конфиденциальных сведениях.

Это дает возможность разделить знание элементов коммерческой тайны среди как можно большего числа сотрудников. Например, желательно, чтобы целиком идею, формулу, конструкцию не знал никто, каждый знал бы лишь свою незначительную часть. Дробление информации также не позволяет конкурентам использовать ее за счет прима на работу уволенного из фирмы сотрудника.

При составлении конфиденциального документа следует учитывать, что его содержание не только определяет функциональное назначение документа, но и лежит в основе разрешительной процедуры доступа персонала к данному документу. Поэтому документ необходимо посвящать только одной тематической группе вопросов, предназначенной, по возможности, одному конкретному исполнителю или структурному подразделению.

В соответствии с иерархической последовательностью доступа определяется структура рубежей защиты информации, которая предусматривает постепенное ужесточение защитных мер по иерархической вертикали возрастания уровня конфиденциальности сведений.

Этим обеспечивается недоступность этих сведений для случайных людей, злоумышленника и определяется необходимый уровень защищенности информации.

Разрешение на доступ к конфиденциальным сведениям строго персонифицировано, т.е. руководители несут персональную ответственность за правильность выдаваемых ими разрешений на доступ исполнителей к конфиденциальным сведениям, а лица, работающие с конфиденциальными документами, несут персональную ответственность за сохранение в тайне их содержания, сохранность носителя и соблюдение установленных правил работы с документами.

Руководитель фирмы имеет право давать разрешение на ознакомление со всеми видами конфиденциальных документов фирмы и всем категориям исполнителей и другим лицам. Однако целесообразно, чтобы первый руководитель оставлял за собой право распоряжаться только наиболее ценной информацией, делегируя право выдачи разрешений на доступ к другой информации нижестоящим руководителям. Следует иметь в виду, что чрезмерная централизация в выдаче разрешений на доступ к конфиденциальной информации неизбежно ведет к снижению оперативности в решении производственных вопросов. Излишняя децентрализация и либерализация создает условия для утраты ценных сведений.

Заместители первого руководителя по функциональным сферам (по науке, производственным вопросам, сбыту и др.) имеют право давать разрешение на ознакомление с конфиденциальными сведениями всем нижестоящим руководителям и исполнителям, но в пределах своей компетенции.

Руководителям структурных подразделений дается право разрешать доступ к конфиденциальным сведения всем работникам своих подразделений по тематике их работы. Руководитель подразделения может давать разрешение только непосредственно подчиненным ему сотрудникам. Для осуществления доступа к документам данного подразделения работника другого подразделения необходимо разрешение соответствующего заместителя руководителя фирмы.

Ответственные исполнители работ (направлений деятельности) имею право давать разрешение на доступ к конфиденциальной информации подчиненным им исполнителям и в пределах их компетенции. В небольших фирмах разрешение на доступ дает только первый руководитель.

Представителям государственных органов разрешение на доступ к конфиденциальным сведениям дает только первый руководитель фирмы. При необходимости доступа к конфиденциальным сведения представителей других фирм и предприятий руководствуются теми обязательствами, которые были закреплены в соответствующем договоре (контракте) на выполнение работ или услуг. Это касается как документированной информации, так и информации устной, визуальной и любой другой. В этом случае разрешение на доступ дает должностное лицо фирмы, включенное в специальный перечень, прилагаемый к договору и утвержденный первым руководителем.

Руководитель фирмы, вне зависимости от формы ее собственности, может устанавливать иные специальные или дополнительные правила доступа к конфиденциальным сведениям, документам, базам данных и носителям информации, конфиденциальным изделиям и продукции фирмы. Он несет за это единоличную ответственность.

Разрешение на доступ к конфиденциальной информации всегда дается полномочным руководителем только в письменном виде: резолюцией на документе, приказом, утверждающим схему именного или должностного доступа к конкретным группам информации, утвержденным руководителем списком-разрешением на обложке дела, списком ознакомления с документом и т.п.

Без дополнительного разрешения допускаются к документам: их исполнители (если они продолжают работать по той же тематике) и лица, визировавшие, подписавшие, утвердившие документ. Без специального разрешения могут допускаться также лица, указанные в тексте распорядительных документов. Если сотрудник допускается только к части документа, то в разрешении (резолюции) четко указываются конкретные пункты, разделы, страницы, приложения, с которыми он может ознакомиться. Сотрудник службы конфиденциальной документации (КД) обязан принять необходимые меры по исключению возможности ознакомления исполнителя с другими частями документа.

Разрешение на доступ к конфиденциальным сведениям представителя другой фирмы или предприятия оформляется резолюцией полномочного должностного лица на предписании (или письме, обязательстве), представленном заинтересованным лицом. В резолюции должны быть указаны конкретные документы или сведения, к которым разрешен доступ. Одновременно указывается фамилия сотрудника фирмы, который знакомит представителя другого предприятия с этими сведениями и несет ответственность за его работу - в помещении фирмы.

Следует соблюдать правило, по которому регистрируются все лица, имеющие доступ к определенным документам, коммерческим секретам. Это позволяет на высоком уровне осуществлять информационное обеспечение аналитической работы по выявлению возможных каналов утраты информации.

При организации доступа сотрудников фирмы к конфиденциальным массивам электронных документов, базам данных необходимо помнить о его многоступенчатом характере. Можно выделить следующие главные составные части:

• доступ к персональному компьютеру, серверу или рабочей станции;

• доступ к машинным носителям информации, хранящимся вне ЭВМ;

• непосредственный доступ к базам данных и файлам.

**Доступ к персональному компьютеру, серверу или рабочей станции,** которые используются для обработки конфиденциальной информации, предусматривает:

• определение и регламентацию первым руководителем фирмы состава сотрудников, имеющих право доступа (входа) в помещение, в котором находится соответствующая вычислительная техника, средства связи;

• регламентацию первым руководителем временного режима нахождения этих лиц в указанных помещениях; персональное и временное протоколирование (фиксирование) руководителем подразделения или направления деятельности фирмы наличия разрешения и периода работы этих лиц в иное время (например, в вечерние часы, выходные дни и др.);

• организацию охраны этих помещений в рабочее и нерабочее время, определение правил вскрытия помещений и отключения охранных технических средств информации и сигнализирования; определение правил постановки помещений на охрану; регламентацию работы указанных технических средств в рабочее время;

• организацию контролируемого (в необходимых случаях пропускного) режима входа в указанные помещения и выхода из них;

• организацию действий охраны и персонала в экстремальных ситуациях или при авариях техники и оборудования помещений;

• организацию выноса из указанных помещений материальных ценностей, машинных и бумажных носителей информации; контроль вносимых в помещение и выносимых персоналом личных вещей.

Несмотря на то, что по окончании рабочего дня конфиденциальные сведения должны быть перенесены на гибкие носители и стерты с жесткого диска компьютера, помещения, в которых находится вычислительная техника, подлежат охране. Объясняется это тем, что, во-первых, в неохраняемый компьютер легко установить какое-либо средство промышленного шпионажа, во-вторых, злоумышленник может с помощью специальных методов восстановить стертую конфиденциальную информацию на жестком диске (произвести «уборку мусора»).

**Доступ к машинным носителям конфиденциальной информации, хранящимся вне ЭВМ, предполагает:**

• организацию учета и выдачи сотрудникам чистых машинных носителей информации;

• организацию ежедневной фиксируемой выдачи сотрудникам и приема от сотрудников носителей с записанной информацией (основных и резервных);

• определение и регламентацию первым руководителем состава сотрудников, имеющих право оперировать конфиденциальной информацией с помощью компьютеров, установленных на их рабочих местах, и получать в службе КД учтенные машинные носители информации;

• организацию системы закрепления за сотрудниками машинных носителей информации и контроля за сохранностью и целостностью информации, учета динамикиизменениясостава записанной информации;

• организацию порядка уничтожения информации на носителе, порядка и условий физического уничтожения носителя;

• организацию хранения машинных носителей в службеКД в рабочее и нерабочее время, регламентацию порядка эвакуации носителей в экстремальных ситуациях;

• определение и регламентацию первым руководителем состава сотрудников не сдающих по объективным причинам технические носители информации на хранение в службу КД в конце рабочего дня, организацию особой охраны помещений и компьютеров этих сотрудников. Работа сотрудников службы КД и фирмы в целом с машинными носителями информации вне ЭВМ должна быть организована по аналогии с бумажными конфиденциальными документами.

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

Обычно доступ к базам данных и файлам подразумевает:

• определение и регламентацию первым руководителем состава сотрудников, допускаемых к работе с определенными базами данных и файлами; контроль системы доступа администратором базы данных;

• именование баз данных и файлов, фиксирование в машинной памяти имен пользователей и операторов, имеющих право доступа к ним;

• учет состава базы данных и файлов, регулярную проверку наличия, целостности и комплектности электронных документов;

• регистрацию входа в базу данных, автоматическую регистрацию имени пользователя и времени работы; сохранение первоначальной информации;

• регистрацию попытки несанкционированного входа в базу данных, регистрацию ошибочных действий пользователя, автоматическую передачу сигнала тревоги охране и автоматическое отключение компьютера;

• установление и нерегулярное по сроку изменение имен пользователей, массивов и файлов (паролей, кодов, классификаторов, ключевых слов и т.п.), особенно при частой смене персонала;

• отключение ЭВМ при нарушениях в системе регулирования доступа или сбое системы защиты информации;

• механическое (ключом или иным приспособлением) блокирование отключенной, но загруженной ЭВМ при недлительных перерывах в работе пользователя. Коды, пароли, ключевые слова, ключи, шифры, специальные программные продукты, аппаратные средства и т.п. атрибуты системы защиты информации в ЭВМ разрабатываются, меняются специализированной организацией и индивидуально доводятся до сведения каждого пользователя работником этой организации или системным администратором. Применение пользователем собственных кодов не допускается.

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

**Заключение**

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