Дипломная работа:

**Законодательство о защите персональных данных работника**

**Содержание**

Введение

1.История развития правового регулирования персональных данных работников в России

2. Понятие персональных данных

2.1 Законодательное регулирование

2.2 Отграничение персональных данных от другой информации

3. Порядок работы с конфиденциальными сведениями о работнике

3.1 Работа кадровой службы с персональными данными

3.2 Общие требования при обработке персональных данных работника и гарантии их защиты

3.3 Передача персональных данных работников

3.4 Защита информации при работе с ЭВМ

3.5 Контроль защиты информации

3.6 Правовые аспекты применения полиграфа

4. Ответственность за нарушение правил работы с персональными данными

4.1 Уголовная и гражданско-правовая ответственность

4.2 Административная ответственность

4.3 Дисциплинарная ответственность

Заключение

Библиография

Приложение

**Введение**

В XXI веке у человечества появляется все больше новых объектов, нуждающихся в защите путем закрепления соответствующих норм в законе. Основной объект на сегодняшний день – это информация. В наше время общество всецело зависит от получаемых, обрабатываемых и передаваемых данных. По этой причине данные сами по себе приобретают высокую ценность. И тем больше цена полезной информации, чем выше ее сохранность.

В виду вышесказанного, законодательными актами как в России, так и зарубежных стран предусматривают немалое количество норм, направленных на регулирование создания, пользования, передачи и защиты информации во всех ее формах.

Особой ценностью обладает информация, несущая в себе данные о личной, индивидуальной или семейной жизни человека. Ст.2 Конституции Российской Федерации закрепляет основной принцип современного демократического общества: «Человек, его права и свободы являются высшей ценностью». Соответственно и информация, непосредственно затрагивающая частные интересы человека должны уважаться и защищаться государством. В повседневной жизни человека сохранность информации о его жизни зависит от него самого. Но совсем другая ситуация, когда мы обязаны предоставить данные о себе в соответствии с законом третьему лицу, а конкретно – работодателю. Работник в данной ситуации передает конфиденциальную информацию о себе на ответственное хранение. Далее за сохранность данных отвечает уже работодатель. Он обязан оберегать сведения о работнике от посягательств третьих лиц и нести ответственность за распространение указанных данных.

Эффективное управление поведением работника в процессе труда возможно лишь при наличии достоверных сведений о его личности, представленных в достаточном объеме. В Трудовом кодексе РФ это обстоятельство нашло четкое закрепление. В специальной главе кодифицированного закона о труде работодателю разрешено получать, хранить, комбинировать, использовать персональные данные нанятого им работника. Законодатель установил общие требования к обработке персональных данных работника и определил гарантии их защиты. В современных социально-экономических условиях в связи с формированием в стране рыночной экономики и обострением социальных проблем роль защиты персональных данных работника значительно возрастает. В литературе по трудовому праву вопросы охраны персональных данных работника уже подвергались научному анализу, однако в настоящее время все еще остается потребность в системном изучении этого института отечественного трудового права, что и предопределило выбор темы дипломной работы и обусловило ее актуальность.

Цель дипломной работы заключается в исследовании трудовых отношений в сфере защиты персональных данных работника.

Поставленная цель достигается путем решения ряда взаимосвязанных задач, наиболее существенными из которых являются:

1. Изучение истории развития правового регулирования персональных данных работников в России.

2. Рассмотрение понятия персональных данных.

2. Исследование порядка работы с конфиденциальными сведениями о работнике кадровой службы.

3. Анализ видов ответственности за нарушение правил работы с персональными данными.

4. Подведение итогов по теме дипломного исследования.

Данная проблема рассматривалась в трудах Степанова Е., Французовой Л., Кузьмина И., Ситниковой Е. и других.

Информационной базой дипломной работы являются Трудовой кодекс РФ, Федеральный закон «Об информации, информационных технологиях и о защите информации», Федеральный закон «О персональных данных» и другие нормативные правовые акты.

Все вышеизложенное определило структуру дипломной работы, которая состоит из введения, трех глав, заключения и библиографии.

**1. История развития правового регулирования персональных данных работников в России**

Трудовые отношения в Российской Федерации и государствах–участниках СНГ, которые входили в состав СССР в качестве союзных республик, в 70–90-х годах регулировались Основами законодательства о труде СССР 1970 годов.

Вместе с тем в каждой союзной республике действовал свой Кодекс законов о труде, который соответствовал Основам законодательства СССР.

КЗоТ РСФСР был принят 09.12.1971 г. и введен в действие с 01.04.1972 г. В КЗоТ РСФСР, как и в кодексах других союзных республик, отсутствовала специальная глава, посвященная персональным данным работника. Однако во всех кодексах содержалась специальная статья, запрещавшая требовать при приеме на работу документы, помимо предусмотренных законодательством.

Перечень документов, которые работник обязан представить при приеме на работу, был закреплен в Типовых правилах внутреннего трудового распорядка (постановление Госкомтруда СССР от 20.07.1984 г.). Во всех случаях в целях заключения трудового договора работник должен был предъявить:

- трудовую книжку, а при поступлении на работу впервые – справку о последнем занятии, выданную по месту жительства;

- уволенные из Вооруженных Сил – военный билет;

- паспорт или другой документ, удостоверяющий личность (лица в возрасте от 14 до 16 лет – свидетельство о рождении).

Прием на работу без предъявления указанных документов не допускался.

В случаях, когда были необходимы специальные знания, требовалось предъявление документов об образовании, профессиональной подготовке, уровне квалификации. Некоторые категории лиц при приеме на работу должны были представить и ряд других документов, если это прямо устанавливалось законодательством. Например, инвалиды должны были иметь трудовую рекомендацию органов врачебно-трудовой экспертизы, лица, принимаемые на работу с детьми и на предприятия общественного питания, – справку медицинского учреждения о состоянии здоровья. При приеме на работу по конкурсу требовалась письменная характеристика с последнего места работы и т. п.

Основным документом о трудовой деятельности в России и государствах – участниках СНГ до настоящего времени остается трудовая книжка. Ранее действовала Инструкция о порядке ведения трудовых книжек на предприятиях, в учреждениях и организациях, утвержденная постановлением Госкомтруда СССР от 20.06.1974 г. В настоящее время Постановлением Министерства труда и социального развития РФ утверждена новая Инструкция по заполнению трудовых книжек.

Трудовые книжки ведутся на всех работников, проработавших свыше пяти дней. Вопросы, связанные с порядком ведения трудовых книжек, их хранения, изготовления, снабжения и учета, регулировались Постановлением Совета Министров СССР и ВЦСПС от 06.09.1973 г. «О трудовых книжках рабочих и служащих» и Инструкцией от 20.09.1974 г.

Заполнение трудовых книжек и вкладышей к ним производилось на языке союзной, автономной республики, автономной области, автономного округа, на территории которых располагалось предприятие, учреждение, организация, и на официальном языке СССР.

Заполнение трудовой книжки производилось администрацией предприятия в присутствии работника не позднее недельного срока со дня приема на работу.

В трудовую книжку вносилось:

– сведения о работнике: фамилия, имя, отчество, дата рождения, образование, профессия, специальность;

– сведения о работе: прием на работу, перевод на другую постоянную работу, увольнение;

– сведения о награждениях и поощрениях: награждения орденами и медалями, присвоение почетных званий; поощрения за успехи в работе, применяемые трудовым коллективом, а также награждения и поощрения, предусмотренные правилами внутреннего трудового распорядка и уставами о дисциплине;

- другие поощрения в соответствии с действующим законодательством;

– сведения об открытиях, на которые выданы дипломы, об использованных изобретениях и рационализаторских предложениях и о выплаченных в связи с этим вознаграждениях.

Взыскания в трудовую книжку не записывались (что соответствует нормам, действующим и в настоящее время).

Все записи в трудовой книжке вносились администрацией предприятия только после издания приказа (распоряжения), но не позднее недельного срока, а при увольнении – в день увольнения и должны были точно соответствовать тексту приказа (распоряжения).

После указания даты заполнения трудовой книжки работник своей подписью заверял правильность внесенных сведений.

При увольнении все записи заверялись подписью руководителя предприятия или специально уполномоченным им лицом и печатью предприятия или печатью отдела кадров.

Если трудовая книжка заполнялась одновременно на языке союзной, автономной республики, автономной области, автономного округа и на официальном языке СССР, то заверялись оба текста.

Помимо трудовой книжки, на каждого работника работодателем велось личное дело, в котором хранились о нем наиболее полные сведения. Личное дело включало в себя:

– анкетно-биографические и характеризующие документы;

- дополнительные документы (анкета; автобиография; копии (ксерокопии);

- документы об образовании;

- личные заявления о приеме на работу или об увольнении и копии приказов об этом;

- заявления работника о перемещениях и переводах и копии приказов;

- представления к поощрению;

- аттестационные листы и др.;

– дополнительные документы (характеристики с прежнего места работы;

- справки о состоянии здоровья; фотографии и др.

Все документы личного дела подшивались в обложку (папку) установленного образца.

Личное дело оформлялось после издания приказа о приеме на работу.

После увольнения работника его личное дело оформлялось для передачи на хранение.

Личные дела выдавались для ознакомления только работникам, занимающим определенные должности. Круг таких лиц, допускаемых к работе с документом личного дела, определялось законодательством и работодателем.

При работе с личным делом, выданным для ознакомления, запрещалось производить какие-либо исправления в ранее сделанных записях, вносить в него новые записи, извлекать из личного дела имеющиеся там документы или помещать в него новые и разглашать содержащиеся в нем конфиденциальные сведения.

При извлечении каких-либо документов из личного дела лицо, ответственное за ведение личных дел, обязано было сделать во внутренней описи соответствующую запись.

В кадровом подразделении хранились только личные дела работников. Для хранения должны были использоваться сейфы или конторские шкафы, в которых личные дела располагаются по порядку номеров. Шкафы или металлические сейфы должны были запираться на замок и опечатываться.

Ст. 24 Конституции РФ запрещает сбор, хранение, использование и распространение информации о частной жизни лица без его согласия.

Органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

В соответствии со ст. 41 Конституции РФ 1993 года, а также Конституциями государств–участников СНГ граждане этих стран обладают неотъемлемым правом на охрану здоровья.

Государство обеспечивает гражданам охрану здоровья независимо от пола, расы, национальности, языка, социального происхождения, должностного положения, места жительства, отношения к религии, убеждений, принадлежности к общественным объединениям, а также других обстоятельств.

Каждый имеет право знакомиться в органах государственной власти, органах местного самоуправления, учреждениях и организациях со сведениями о себе, не являющимися государственной или иной защищенной законом тайной.

Каждому гарантируется судебная защита права опровергать недостоверную информацию о себе и членах своей семьи и права требовать изъятия любой информации, а также право на возмещение материального и морального ущерба, причиненного сбором, хранением, использованием и распространением такой недостоверной информации».

В трудовых кодексах стран–участников СНГ, принятых в период с 1997 года по 2001 года, содержатся статьи, устанавливающие перечень документов, необходимых для заключения трудового договора. К ним относятся:

– трудовая книжка;

– документ, удостоверяющий личность;

– документ о профессиональной подготовке или образовании, если это необходимо для выполнения трудовой функции;

– справка о состоянии здоровья для определенных работ, профессий и должностей, а также трудовая рекомендация для инвалидов;

– документы воинского учета.

Запрещается требовать при приеме на работу документы, не предусмотренные трудовыми кодексами или действующим законодательством.

30 марта 1995 года в России был принят Федеральный закон «О предупреждении распространения в Российской Федерации заболевания, вызываемого вирусом иммунодефицита человека (ВИЧ-инфекции)».

Государством гарантируются:

– регулярное информирование населения, в том числе через средства массовой информации, о доступных мерах профилактики ВИЧ-инфекции;

– эпидемиологический надзор за распространением ВИЧ-инфекции на территории Российской Федерации;

– производство средств профилактики, диагностики и лечения ВИЧ-инфекции, а также контроль за безопасностью медицинских препаратов, биологических жидкостей и тканей, используемых в диагностических, лечебных и научных целях;

– доступность медицинского освидетельствования для выявления ВИЧ-инфекции, в том числе и анонимного, с предварительным и последующим консультированием и обеспечение безопасности такого медицинского освидетельствования как для освидетельствуемого, так и для лица, проводящего освидетельствование;

– бесплатное предоставление всех видов квалифицированной и специализированной медицинской помощи ВИЧ–инфицированным гражданам Российской Федерации, бесплатное получение ими медикаментов при лечении в амбулаторных или стационарных условиях, а также их бесплатный проезд к месту лечения и обратно в пределах Российской Федерации;

– развитие научных исследований по проблемам ВИЧ-инфекции;

– включение в учебные программы образовательных учреждений тематических вопросов по нравственному и половому воспитанию;

– социально-бытовая помощь ВИЧ-инфицированным гражданам Российской Федерации, получение ими образования, их переквалификация и трудоустройство;

– подготовка специалистов для реализации мер по предупреждению распространения ВИЧ-инфекции;

– развитие международного сотрудничества и регулярный обмен информацией в рамках международных программ предупреждения распространения ВИЧ-инфекции.

ВИЧ-инфицированные граждане РФ обладают на ее территории всеми правами и свободами и несут обязанности в соответствии с Конституцией Российской Федерации, законодательством РФ и законодательством субъектов РФ.

Работники отдельных профессий, производств, предприятий, учреждений и организаций, перечень которых утверждается Правительством РФ, проходят обязательное медицинское освидетельствование для выявления ВИЧ-инфекции при проведении обязательных предварительных при поступлении на работу и периодических медицинских осмотров.

Правила, в соответствии с которыми осуществляется обязательное медицинское освидетельствование лиц в целях охраны здоровья населения и предупреждения распространения ВИЧ-инфекции, а также в местах лишения свободы, устанавливаются Правительством РФ и пересматриваются им не реже одного раза в пять лет.

В случае выявления ВИЧ-инфекции у несовершеннолетних в возрасте до 18 лет, а также у лиц, признанных в установленном законом порядке недееспособными, работники медицинских учреждений уведомляют об этом родителей или иных законных представителей указанных лиц.

Не допускаются увольнение с работы, отказ в приеме на работу, отказ в приеме в образовательные учреждения и учреждения, оказывающие медицинскую помощь, а также ограничение иных прав и законных интересов ВИЧ-инфицированных на основании наличия у них ВИЧ-инфекции, равно как и ограничение жилищных и иных прав и законных интересов членов семей ВИЧ-инфицированных (ст. 17).

Медицинские работники и другие лица, которым в связи с выполнением служебных или профессиональных обязанностей стали известны сведения о результатах проведения медицинского освидетельствования на выявление ВИЧ-инфекции, обязаны сохранять эти сведения в тайне.

За разглашение сведений, составляющих врачебную тайну, лица, которым эти сведения стали известны в связи с выполнением ими своих служебных или профессиональных обязанностей, несут ответственность в соответствии с законодательством Российской Федерации.

В случае выявления ВИЧ-инфекции у работников отдельных профессий, производств, предприятий, учреждений и организаций, перечень которых утверждается Правительством РФ, эти работники подлежат переводу на другую работу, исключающую условия распространения ВИЧ-инфекции.

При отказе от прохождения обязательного медицинского освидетельствования на выявление ВИЧ-инфекции без уважительных причин работник подлежит дисциплинарной ответственности в установленном порядке.

Свод практических правил МОТ по защите персональных данных работника был принят на совещании экспертов в 1996 года. Он не имеет обязательной силы, но мог быть использован при разработке национального законодательства.

В нем изложены основные принципы сбора, обработки, использования и хранения личной информации о работниках, а также о лицах, обращающихся к работодателю в целях трудоустройства.

Специальные разделы Свода посвящены личным правам работника, возникающим в связи со сбором персональных данных, в частности, праву на уведомление о сборе персональных данных, на ознакомление в рабочее время со сведениями о себе, которые имеются у работодателя, на получение копий документов, право на доступ к медицинским документам через своего врача-представителя и др.

Свод практических правил МОТ по защите персональных данных работника явился практическим руководством для разработчиков проекта Трудового кодекса Российской Федерации, которые включили в него главу 13 «Защита персональных данных работника». Нормы этой главы полностью соответствуют положениям Свода.

В Трудовых кодексах других государств–участников СНГ подобные главы отсутствуют.

**2. Понятие персональных данных**

**2.1 Законодательное регулирование**

В современном мире к защите конфиденциальных сведений предъявляют все большие требования. Поскольку персональные данные работников содержат данные личного характера, к обеспечению гарантий по их сохранности и неразглашению относятся очень серьезно. В связи с этим нормативные акты, регулирующие обеспечение сохранности персональных данных вообще и работников в частности предусмотрены не только национальным законодательством, но и международными актами.

Статья 12 Всеобщей декларации прав человека 1948 года гласит «Никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств». Право на уважение к личной и семейной жизни содержится так же и в Конвенции о защите прав человека и основных свобод. Эти международные правовые акты заложили основу создания национальных правовых систем. Необходимо отметить, что принимались они спустя несколько лет после разрушительной Мировой войны, в то время, когда права человека были чем-то очень далеким от реальности. И, тем не менее, право неприкосновенности частной жизни (в том числе конфиденциальных сведений) было вписано в Декларацию как одно из основных.

В дальнейшем, когда в мировом сообществе происходила серьезная борьба за закрепление политических прав человека, право неприкосновенности личной жизни было подтверждено Международным пактом о гражданских и политических правах.

В 1995 году Содружеством Независимых Государств (в состав которого входит Россия) была принята Конвенция о правах и основных свободах человека, закрепившая основные права на территории распавшегося Союза СССР.

Что касается Российской Федерации, то на сегодняшний день сохранность конфиденциальных сведений на ее территории обеспечивается следующими нормативными актами.

Во-первых, это Конституция Российской Федерации. В ее положениях признается не только само право на неприкосновенность личной жизни, личную и семейную тайну (ч.1 ст.23), но и обеспечивающие это право дополнительные гарантии. В соответствии со ст. 2 Конституции «человек, его права и свободы являются высшей ценностью. Признание, соблюдение и защита прав и свобод человека и гражданина - обязанность государства». Таким образом, Российская Федерация не только устанавливает право, но и обязуется защищать его; ставит интересы человека и гражданина на ступень выше, чем интересы государства, общества, либо общественных или коммерческих организаций. Согласно ч.1 ст. 15 Конституция РФ является документом прямого действия, т.е. ее нормы не требуют дополнительного признания и исполняются «как есть». Ч.4 ст. 15 признает Международные договоры (в т.ч. указанные Конвенции) источником права и отводит им главенствующую роль. Ч.1 ст. 24 запрещает сбор, хранение, использование и распространение информации о частной жизни лица без его согласия. И, наконец, согласно ст. 46 каждому гарантируется судебная защита его прав, в том числе в межгосударственных органах.

Кроме того, данную сферу регулирует Федеральный Закон "Об информации, информационных технологиях и о защите информации" и Федеральный Закон «О персональных данных». В частности ч.1 ст. 11 Закона определяет, что персональные данные являются конфиденциальной информацией, а ч.3 этой же статьи предупреждает о наступлении ответственности юридических и физических лиц за нарушение режима защиты, обработки и порядка использования этой информации.

Персональные данные отнесены к категории конфиденциальных сведений (в соответствии с ФЗ «Об информации…») и соответствующим Перечнем, который дает им следующее определение: «сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность».

Сфера отношений, касающаяся персональных данных работника регулируется гл.14 Трудового кодекса Российской Федерации. Где установлено понятие персональных данных работника, установлен порядок работы с ними и закрепляется ответственность работодателя за нарушение соответствующих норм.

* 1. **Отграничение персональных данных от другой информации**

В Трудовом кодексе впервые появилась специальная глава, посвященная защите персональных данных работника (ст. 85-90). Работодатель всегда собирал данные о личности работника. Для этой цели использовались "Личный листок" и различные анкеты, а также письменные характеристики и т.д. Однако официальная правовая регламентация обработки этих данных, доступная работнику, отсутствовала.

В ст. 85 ТК и последующих статьях настоящей главы применительно к трудовым отношениям получили конкретизацию конституционные положения о праве каждого на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени (ст. 23 Конституции РФ).

В Трудовом кодексе под персональными данными работника понимается информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника (ч.1 ст.85 ТК РФ).

Легко заметить, что под это определение можно подвести любую информацию о работнике. И работодатели нередко собирают о сотруднике всю информацию, мотивируя это тем, что хотят иметь максимально полное представление о нем.

Довольно часто от работника требуют сообщить исчерпывающую информацию о его семейном положении и ближайших родственниках, о жилищных условиях, состоянии здоровья, о фактах привлечения к уголовной ответственности, о наличии постоянной регистрации по месту жительства и многое другое. Но такого рода информация никаким образом не относится к трудовой деятельности работника. Наоборот, тем самым работодатель переходит тонкую грань, отделяющую персональные данные от сведений, составляющих тайну частной жизни, личную или семейную тайну гражданина.

Среди документов и материалов, содержащих информацию, необходимую работодателю в связи с трудовыми отношениями, основное место занимают:

1) документы, предъявляемые при заключении трудового договора (см. ст. 65 ТК);

2) документы о составе семьи работника, необходимые для предоставления ему гарантий, связанных с выполнением семейных обязанностей;

3) документы о состоянии здоровья работника, если в соответствии с законодательством он должен пройти предварительный и периодические медицинские осмотры;

4) документы, подтверждающие право на дополнительные гарантии и компенсации по определенным основаниям, предусмотренным законодательством (об инвалидности, донорстве, нахождении в зоне воздействия радиации в связи с аварией на Чернобыльской АЭС и др.);

5) документ о беременности работницы и возрасте детей для предоставления матери установленных законом условий труда, гарантий и компенсаций. Вышесказанное можно представить в виде следующей таблицы:

Таб. 1 Основной критерий оценки - характер собираемой работодателем информации

|  |  |  |  |
| --- | --- | --- | --- |
| Характер информации | Персональные данные (информация о работнике, необходимая работодателю в связи с трудовыми отношениями – ст. 85 ТК РФ) | | Информация о частной жизни работника, не касающаяся трудовых отношений |
| Информация о выполнении служебных обязанностей | Сведения о фактах, событиях и обстоятельствах частной жизни (конфиденциальные данные) |
| В каком случае работодатель вправе получать информацию | Всегда | При соблюдении установленных законом условий | Никогда |

Среди персональных данных работника должны быть трудовой договор, приказ (распоряжение) о приеме на работу, приказы (распоряжения) об изменении условий трудового договора, его прекращении, а также приказы (распоряжения) о поощрениях и дисциплинарных взысканиях, примененных к работнику. В период действия трудового договора среди персональных данных работника должна находиться его трудовая книжка.

Для того чтобы установить, в каком объеме работодатель вправе получать от работника информацию о его персональных данных, необходимо обратить внимание на очень важное ограничение - это целевой характер использования персональных данных. Обработка этого вида информации может производиться исключительно в целях, указанных в пункте 1 статьи 86 ТК РФ.

**3. Порядок работы с конфиденциальными сведениями о работнике**

**3.1 Работа кадровой службы с персональными данными**

В силу специфики своей деятельности обработкой персональных данных в организации занимается отдел кадров. Именно здесь "оседает" весь объем сведений о работниках. Вот почему процессы обработки, передачи и защиты конфиденциальной информации о работниках должны быть упорядочены, прежде всего, в этой службе.

Правила ведения конфиденциального делопроизводства должны применяться в первую очередь в отношении личных дел сотрудников, в которых содержатся персональные данные. Комплектация личных дел является наиболее сложной и ответственной работой, требует особой тщательности и аккуратности при оформлении. Каждое предприятие вправе самостоятельно решать вопрос о том, какие документы включать в состав личных дел.

Работники отдела кадров должны помнить, что личные дела сотрудников должны храниться строго отдельно от всех других документов в закрывающихся шкафах или ящиках. Необходимо иметь в виду также то обстоятельство, что документы, включенные в состав личных дел, имеют разные сроки хранения. Для некоторых из них (приказов, личных карточек) установлены продолжительные сроки хранения и обязательное требование по их передаче в государственные архивы.

Отделу кадров целесообразно вести журнал учета, в который будут заноситься все факты ознакомления с персональными данными работников, а также информация о движении документов, включенных в личные дела, и самих личных дел. В таком журнале должны быть предусмотрены графы о дате выдачи и возврата документов (личных дел), сроке пользования, цели выдачи, наименовании выдаваемых документов (личных дел). В присутствии лица, возвращающего личное дело, обязательно сверяется по описи наличие всех документов. Лица, получающие документы (личные дела) во временное пользование, не имеют права делать в них пометки, исправления, вносить новые записи, извлекать документы из личного дела или помещать в него новые.

Принципиальным требованием правил работы с персональными данными является установление личной ответственности сотрудников за неразглашение доверенной им конфиденциальной информации, за сохранность сведений, а также их носителей. В этой связи лицо, получившее право работать с персональными данными, должно принять на себя ряд обязательств: не разглашать доверенные им сведения, неукоснительно выполнять правила работы с персональными данными, обеспечивать надежное хранение носителей конфиденциальной информации.

Также следует незамедлительно сообщать уполномоченным лицам об утрате ключей, печатей и штампов, давать устные и письменные объяснения по фактам нарушения правил. В число ограничений входят также запреты на совершение определенных действий, могущих повлечь утрату носителей информации или разглашение конфиденциальных сведений, в частности, на передачу персональных данных лицам, не имеющим к ним доступа; на вынос документов из рабочего помещения без служебной необходимости и пр. Перечень указанных обязательств целесообразно отразить в Положении либо должностной инструкции специалиста.

Более того, в соответствии с частью 3 статьи 57 Трудового кодекса условие о неразглашении работником сведений, составляющих охраняемую законом тайну, ставшую ему известной в связи с исполнением своих должностных обязанностей, может быть включено в трудовой договор с таким специалистом. В этом случае на работодателе лежит обязанность ознакомить работника с локальными нормативными актами предприятия, содержащими правила обработки и защиты персональных данных. Именно такая процедура доступа может быть использована в отношении специалистов кадровых служб.

Система защиты конфиденциальных сведений должна предусматривать проведение регулярных проверок наличия документов и других носителей информации, содержащих персональные данные работников, а также соблюдение правил работы с ними.

Как показывает опыт, применение только административных мер не гарантирует полноценную охрану конфиденциальных сведений. Надежность защиты зависит во многом от расстановки и внутрифирменного развития сотрудников. Кроме того, персонал - один из главных каналов утечки информации. Деятельность кадровой службы должна быть направлена на воспитание работников, допущенных к работе с персональными данными, выработку навыков работы с носителями конфиденциальной информации, закрытие бытовых каналов утечки данных. Здесь могут быть полезны индивидуальная беседа, предупреждение об ответственности, разъяснение юридических последствий разглашения информации.

**3.2 Общие требования при обработке персональных данных работника и гарантии их защиты**

Конфиденциальность, сохранность и защита персональных данных в отделе кадров обеспечивается отнесением их к служебной тайне. Работа с персональными данными должна быть организована в строгом соответствии с требованиями к обработке и хранению информации ограниченного доступа. Режим конфиденциальности персональных данных снимается в случаях обезличивания их или по истечении 75 – лет срока хранения, если иное не определено законом.

В ст. 86 Трудового кодекса РФ содержатся общие требования при обработке персональных данных работника и гарантии их защиты.

В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника обязаны соблюдать следующие общие требования:

1) обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и про движении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

2) при определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом и иными федеральными законами;

3) все персональные данные работника следует получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и по следствиях отказа работника дать письменное согласие на их получение;

4) работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия;

5) работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных Трудовым кодексом или иными федеральными законами;

6) при принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения;

7) защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном Трудовым кодексом и иными федеральными законами;

8) работники и их представители должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области;

9) работники не должны отказываться от своих прав на сохранение и защиту тайны;

10)работодатели, работники и их представители должны совместно вырабатывать меры защиты персональных данных работников.

Персональные данные содержатся в документации отдела кадров. Это:

* документы, связанные с подбором персонала;
* документы, сопровождающие процесс оформления трудовых правоотношений гражданина (при решении вопросов о приеме на работу, переводе, увольнении и т.п.);
* материалы анкетирования, тестирования, проведения собеседований с кандидатами на должность;
* трудовые договоры, соглашения, устанавливающие взаимоотношения сторон;
* подлинники и копии приказов по личному составу;
* личные дела и трудовые книжки сотрудников;
* дела, содержащие основания к приказам по личному составу;
* дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным рас следованиям 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, муниципальные и другие учреждения.

При работе с персональными данными сотрудниками отделов кадров должны соблюдаться следующие основополагающие принципы по их защите:

- личная ответственность руководства предприятия и работников отдела кадров за сохранность и конфиденциальность сведений о работе отдела и персональных данных, а также о носителях этой информации;

- разбиение (дробление) персональных данных между разными руководителями предприятия и работниками отдела кадров;

- наличия четкой разрешительной системы доступа руководства предприятия и работников отдела кадров к документам, содержащим персональные данные;

- проведения регулярных проверок наличия традиционных и электронных документов, дел и баз данных у работников отдела и кадровых документов в подразделениях предприятия.

Главным здесь является четкая регламентация функций работников отдела кадров по разным видам документов, дел, карточек, журналов персонального учета и баз данных. Посторонние лица не должны знать распределение этих функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе кадров. Под посторонними лицами понимаются не только злоумышленники или их сообщники, но и сотрудники предприятия, функциональные обязанности которых не связаны с работой отдела кадров. Следует также учитывать, что работник отдела кадров не должен быть осведомлен о порядке работы других сотрудников отдела.

Для этого первый руководитель предприятия должен издать приказ о закреплении за работниками отдела кадров определенных массивов документов, необходимого для информационного обеспечения функций, указанных в должностных инструкциях. Должна также быть схема доступа работников отдела кадров и руководящего состава предприятия, структурных подразделений к документам отдела, введена личная ответственность указанных должностных лиц и работников за сохранность и конфиденциальность персональных данных.

Не допускается, чтобы работник отдела кадров мог знакомиться с любыми документами и материалами отдела. Целесообразно, чтобы каждый из них был закреплен за определенной группой персонала предприятия и выполнял весь объем функций от подбора кандидата на вакантную должность до хранения документации.

В случае необходимости перераспределения обязанностей среди работников отдела (например, при болезни одного из них) издается соответствующее распоряжение начальника отдела кадров, в котором регламентируется характер изменений, их срок и дополнения к документам, делам и базам данных.

Следует соблюдать следующие особенности обработки и хранения документов.

Приказы по личному составу составляются, оформляются и хранятся в отделе кадров, а не в делопроизводственной службе.

Операции по оформлению, формированию, ведению и хранению личных дел выполняются одним работником отдела кадров, который несет личную ответственность за сохранность документов в делах и доступ к делам других работников.

Материалы, связанные с анкетированием, тестированием, проведением собеседований с кандидатами на должность, помещаются не в личное дело сотрудника, а в специальное дело с грифом «Строго конфиденциально». Объясняется это тем, что подобные материалы раскрывают личные и моральные качества сотрудника и могут при разглашении содержащихся в них сведений стать полезными злоумышленнику.

Материалы тестирования работающих сотрудников, их аттестации формируются в отдельное дело также с грифом строгой конфиденциальности. В случае изъятия из личного дела документа в описи дела производится запись с указанием основания для его изъятия и нового местонахождения. С документа, подлежащего изъятию, снимается копия, которая подшивается на место изъятого документа. Отметка в описи и копия заверяются начальником и работником отдела кадров. Замена документов в личном деле кем бы то ни было запрещена. Новые исправленные документы помещаются с ранее подшитыми.

Приказом первого руководителя предприятия должен быть установлен порядок выдачи и ознакомления руководящего состава с личными делами сотрудников. Личные дела могут выдаваться только на рабочие места первого руководителя предприятия, его заместителя по кадрам и начальника отдела (управления) кадров. Дела выдаются (в том числе начальнику отдела кадров или при наличии письменного разрешения – работнику отдела) под роспись в контрольной карточке. При возврате дела тщательно проверяется сохранность документов, отсутствие повреждений и включений в дело других документов или их подмены. Просмотр дела производится в присутствии руководителя. Передача личных дел руководителям через их секретарей или референтов не допускается.

Другие руководители предприятия могут знакомиться с личными делами (или при отсутствии личных дел – карточками формы Т-2) только непосредственно подчиненных им сотрудников; к справочно-информационному банку данных и другой документации отдела кадров они не допускаются. Ознакомление с делами осуществляется в помещении отдела кадров под наблюдением работника, ответственного за сохранность и ведение личных дел. Факт ознакомления фиксируется контрольной карточке личного дела. Работник предприятия вправе ознакомиться только со своим личным делом и трудовой книжкой, учетными карточками, отражающими его персональные данные. Факт ознакомления с личным делом также фиксируется в контрольной карточке.

Не менее строгого контроля требует работа со справочно-информационным банком данных по персоналу предприятия (карточками, журналами и книгами персонального учета сотрудников).

Отчетная и справочная работа отдела формирует каналы несанкционированного получения и незаконного использования персональных данных. В связи с этим первым руководителем устанавливается: кто, когда, какие сведения и с какой целью может запрашивать в отделе кадров. И, что особенно важно – определяется порядок дальнейшего хранения сведений, работа с которыми закончена: где эти сведения будут находиться, кто несет ответственность за их сохранность и конфиденциальность.

На документах, выходящих за пределы отдела кадров, может ставиться гриф «конфиденциально» или «для служебного пользования». В отделе кадров обязательно остаются копии всех отчетных и справочных документов. Целесообразно, чтобы подлинники этих документов после минования в них надобности возвращались в от дел кадров для включения в дело вместо хранящейся там копии.

В структурных подразделениях предприятия могут быть следующие документы, содержащие персональные данные:

- журнал табельного учета с указанием должностей, фамилий и инициалов сотрудников (находится у работника, ведущего табельный учет, - табельщика),

- штатное расписание (штатный формуляр) подразделения, в котором может дополнительно указываться, кто из сотрудников занимает ту или иную должность, вакантные должности (находится у руководителя подразделения),

- дело с выписками из приказов по личному составу, касающимися персонала под разделения (находится у табельщика).

Руководитель подразделения может иметь список сотрудников с указанием основных биографических данных каждого из них (год рождения, образование, местожительство, домашний телефон и др.). Все перечисленные документы следует хранить в соответствующих делах, включенных в номенклатуру дел и имеющих гриф ограничения доступа. Не реже одного раза в год работники отдела кадров проверяют наличие этих дел в подразделениях, их комплектность, правильность ведения и уничтожения.

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

Помимо операций с документами работники отдела кадров значительную часть времени тратят на прием посетителей. Этот вид работы также должен быть строго регламентирован, т.к. посетители могут представлять определенную угрозу информационной безопасности отдела кадров и физической безопасности работников отдела. Приемные часы должны быть разными для сотрудников предприятия и лиц, не входящих в эту категорию. 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. Ответы на вопросы даются только лично тому лицу, которого они касаются. Не допускается отвечать на вопросы, связанные с передачей персональной информации, по телефону или факсу. Ответы на правомерные письменные запросы других учреждений и организаций даются в письменной форме и в том объеме, который позволяет не разглашать излишний объем персональных сведений.

Подбор персонала для работы в отделе кадров ведется с учетом требований, которые разработаны для должностей, связанных с владением и обработкой конфиденциальных сведений и документов. Здесь: анализ личностных и моральных качеств претендентов на должность; подписание обязательства о неразглашении защищаемых сведений; оформление приказом первого руководителя предприятия допуска к конфиденциальной информации; обучение правилам защиты конфиденциальной информации и регулярное инструктирование по отдельным вопросам защиты; контроль соблюдения действующих инструкций по работе с конфиденциальными документами.

Иными словами, порядок функционирования отдела кадров должен быть подчинен решению задач обеспечения безопасности персональных сведений, их защиты от разного рода злоумышленников.

**3.3 Передача персональных данных работников**

Информация, относящаяся к персональным данным работника, может быть предоставлена государственным органам в порядке, установленном федеральным законом.

Работодатель не вправе предоставлять персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом.

В случае если лицо, обратившееся с запросом, не уполномочено федеральным законом на получение персональных данных работника либо отсутствует письменное согласие работника на предоставление его персональных сведений, работодатель обязан отказать в предоставлении персональных данных. Лицу, обратившемуся с запросом, выдается письменное уведомление об отказе в предоставлении персональных данных.

Персональные данные работника могут быть переданы представителям работников в порядке, установленном Трудовым кодексом, в том объеме, в каком это необходимо для выполнения указанными представителями их функций.

Работодатель обеспечивает ведение журнала учета выданных персональных данных работников, в котором регистрируются запросы, фиксируются сведения о лице, направившем запрос, дата передачи персональных данных или дата уведомления об отказе в предоставлении персональных данных, а также отмечается, какая именно информация была передана.

В случае если лицо, обратившееся с запросом, не уполномочено федеральным законом или настоящим Положением на получение информации, относящейся к персональным данным работника, работодатель обязан отказать лицу в выдаче информации. Лицу, обратившемуся с запросом, выдается уведомление об отказе в выдаче информации, копия уведомления подшивается в личное дело работника.

**3.4 Защита информации при работе с ЭВМ**

Утечка конфиденциальной информации от персональных ЭВМ может происходить по следующим каналам:

- организационному каналу через персонал, злоумышленника, его сообщника, силовым криминальным путем,

- побочных электромагнитных излучений от ЭВМ и линий связи,

- наводок злоумышленником опасного сиг нала на линии связи, цепи заземления и электропитания,

- акустических сигналов,

- через вмонтированные радиозакладки, съема информации с плохо стертых дискет, ленты принтера.

Основным источником высокочастотного электромагнитного излучения является дисплей. Картинку дисплея можно уловить и воспроизвести на экране другого дисплея на расстоянии 200 - 300 м. Печатающие устройства всех видов излучают информацию через соединительные провода. Однако основным виновником утраты электронной информации всегда является человек.

Защита данных должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ. Программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики ЭВМ (надежность, быстродействие).

Организация системы защиты информации включает:

- защиту границ охраняемой территории,

- защиту линий связи между ЭВМ в одном помещении,

- защиту линий связи в различных помещениях, защиту линий связи, выходящих за пределы охраняемой зоны (территории).

Защита информации включает ряд определенных групп мер:

- меры организационно-правового характера: режим и охрана помещений, эффективное делопроизводство по электронным документам – внемашинная защита информации, под бор персонала,

- меры инженерно-технического характера: место расположения ЭВМ, экранирование помещений, линий связи, создание помех и др.,

- меры, решаемые путем программирования: регламентация права на доступ, ограждение от вирусов, стирание информации при несанкционированном доступе, кодирование информации, вводимой в ЭВМ,

- меры аппаратной защиты: отключение ЭВМ при ошибочных действиях пользователя или попытке несанкционированного доступа.

Помещения, в которых происходит обработка информации на ЭВМ, должны иметь аппаратуру противодействия техническим средствам промышленного шпионажа. Иметь сейфы для хранения носителей информации, иметь бесперебойное электропитание и кондиционеры, оборудованные средствами технической защиты.

Комплекс программно-технических средств и организационных (процедурных) решений по защите информации от несанкционированного доступа состоит из четырех элементов:

- управления доступом;

- регистрации и учета;

- криптографической;

- обеспечения целостности.

Правильная организация доступа - управление доступом к конфиденциальной информации является важнейшей составной частью системы защиты электронной информации. Реализация системы доступа как к традиционным, так и электронным документам основывается на анализе их содержания, которое является главным критерием однозначного определения: кто из руководителей, кому из исполнителей (сотрудников), как, когда и с какими категориями документов разрешает знакомиться или работать. Любое обращение к конфиденциальному документу, ознакомление с ним в любой форме (в том числе случайное, несанкционированное) обязательно фиксируется в учетной карточке документа и на самом документе в виде соответствующей отметки и подписи лиц, которые обращались к документу. Этот факт указывается также в карточке учета осведомленности сотрудника в тайне фирмы.

Организуя доступ сотрудников фирмы к конфиденциальным массивам электронных документов и базам данных, необходимо по мнить о его многоступенчатом характере. Можно выделить следующие главные составные части доступа этого вида:

- доступ к персональному компьютеру, сер веру или рабочей станции;

- доступ к машинным носителя информации, хранящимся вне ЭВМ;

- непосредственный доступ к базам данных и файлам.

Доступ к персональному компьютеру, сер веру или рабочей станции, которые используются для обработки конфиденциальной ин формации, 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 (на пример, 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 информирования и сиг нализирования; 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.

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

Перед началом обработки информации на ЭВМ сотрудник обязан убедиться в отсутствии в помещении посторонних лиц. При подходе такого лица к сотруднику экран дисплея дол жен быть немедленно погашен.

В конце рабочего дня исполнители обязаны перенести всю конфиденциальную информацию из компьютера на гибкие носители информации, стереть информацию с жестких дисков, проверить наличие всех конфиденциальных документов (на бумажных, магнитных и иных носителях), убедиться в их комплектности и сдать в службу КД. Оставлять конфиденциальные документы на рабочем месте не разрешается. Не допускается также хранение на рабочем месте исполнителя копий конфиденциальных документов.

Лицам, имеющим доступ к работе на ЭВМ, запрещается:

- разглашать сведения о характере автоматизированной обработки конфиденциальной информации и содержании используемой для этого документации,

- знакомиться с изображениями дисплея рядом работающих сотрудников или пользоваться их магнитными носителями без разрешения руководителя подразделения,

- разглашать сведения о личных паролях, используемых при идентификации и защите массивов информации,

- оставлять магнитные носители конфиденциальной информации без контроля, принимать или передавать их без росписи в учет ной форме, оставлять ЭВМ с загруженной памятью бесконтрольно,

- пользоваться неучтенными магнитными носителями, создавать неучтенные копии документов.

После изготовления бумажного варианта документа его электронная копия стирается, если она не прилагается к документу или не сохраняется в справочных целях. Отметки об уничтожении электронной копии вносятся в учетные карточки документа и носителя и заверяются двумя росписями.

Хранение магнитных носителей и электронных документов должно осуществляться в условиях, исключающих возможность иххищения, приведения в негодность или уничтожения содержащейся в них информации, а также в соответствии с техническими условиями завода-изготовителя. Носители хранятся в вертикальном положении в специальных ячейках металлического шкафа или сейфа. Номера на ячейках должны соответствовать учетным номерам носителей. Недопустимо воздействие на носители теплового, ультрафиолетового и магнитного излучений.

Магнитные носители, содержащие конфиденциальную информацию, утратившую свое практическое значение, уничтожаются по акту с последующей отметкой в учетных фор мах.

С целью контроля и поддержания режима при обработке информации на ЭВМ необходимо:

- периодически проводить проверки наличия электронных документов и состава баз данных,

- проверять порядок ведения учета, хранения и обращения с магнитными носителями и электронными документами,

- систематически проводить воспитательную работу с персоналом, осуществляющим обработку конфиденциальной информации на ЭВМ,

- реально поддерживать персональную ответственность руководителей и сотрудников за соблюдение требований работы с конфиденциальной информацией на ЭВМ,

- осуществлять действия по максимальному ограничению круга сотрудников, допускаемых к обрабатываемой на ЭВМ конфиденциальной информации и праву входа в помещения, в которых располагаются компьютеры, для обработки этой информации.

**3.5 Контроль защиты информации**

Взаимопонимание между руководством фирмы и работниками не означает полной свободы в организации рабочих процессов и желании выполнять или не выполнять требования по защите конфиденциальной информации. С этой целью руководителям всех рангов и службе безопасности следует организовать регулярное наблюдение за работой персонала в части соблюдения ими требований по защите информации.

Основными формами контроля могут быть:

- аттестация работников;

- отчеты руководителей подразделений о работе подразделений и состоянии системы защиты информации;

- регулярные проверки руководством фирмы и службой безопасности соблюдения работниками требований по защите информации;

- самоконтроль.

Аттестация работников представляется одной из наиболее действенных форм контроля их деятельности как в профессиональной сфере (исполнительность, ответственность, качество и эффективность выполняемой работы, профессиональный кругозор, организаторские способности, преданность делу организации и т. д.), так и в сфере соблюдения информационной безопасности фирмы.

В части соблюдения требований по защите информации проверяется знание работником соответствующих нормативных и инструктивных документов, умение применять требования этих документов в практической деятельности, отсутствие нарушений в работе с конфиденциальными документами, умение общаться с посторонними лицами, не раскрывая секретов фирмы и т.д.

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

Другой формой контроля является заслушивание руководителей структурных подразделений и руководителя службы безопасности на совещании у первого руководителя фирмы о состоянии системы защиты информации и вы полнении ее требований работниками подразделений. Одновременно на совещании принимаются решения по фактам нарушения работниками установленных правил защиты секретов фирмы.

Формой контроля являются также регулярные проверки выполнения сотрудниками (в том числе хорошо работающими) правил работы с конфиденциальной информацией, документами и базами данных.

Проверки проводятся руководителями структурных подразделений и направлений, заместителями первого руководите ля и работниками службы безопасности.

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

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

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

Кроме того, необходимо помнить, что работники, владеющие конфиденциальной информацией, вынуждены действовать в рамках требований, регламентированных инструкцией по обеспечению режима конфиденциальности. Ограничение свободы человека в использовании информации может приводить к стрессам, нервным срывам. Сохранение чего-то в тайне противоречит потребности чело века в общении путем обмена информацией. В связи с этим особенно важно, что бы психологический настрой коллектива и отдельных работников всегда находился в центре внимания руководства фирмы и службы безопасности.

В случае установления фактов невыполнения любым из руководителей или работников требований по защите ин формации к ним в обязательном порядке должны применяться меры порицания и наказания в соответствии с правилами внутреннего трудового распорядка. Важно, чтобы наказание было неотвратимым и своевременным, невзирая на должностной уровень работника и его взаимоотношения с руководством фирмы.

Одновременно с виновным лицом ответственность за разглашение сведений, составляющих секреты фирмы, несут руководители фирмы и ее структурных под разделений, направлений деятельности, филиалов, т.к. они полностью отвечают за разработку и реализацию мер, обеспечивающих информационную безопасность всех видов деятельности фирмы.

Информационная база для контроля работы персонала, владеющего конфиденциальной информацией, формируется на основе анализа степени осведомленности работников в секретах фирмы. Эта работа входит в состав комплексного аналитического исследования по поиску и обнаружению каналов утраты персона лом конфиденциальной информации.

Объектами комплексного аналитического исследования являются: выявление, классификация и постоянное изучение источников и объективных каналов распространения конфиденциальной информации, а также обнаружение и анализ степени опасности источников угрозы информации. Важен превентивный контроль безопасности ценной информации.

Одновременно подлежат специальному (экстремальному) учету все замеченные несанкционированные или ошибочные действия персонала с документами и информацией, нарушения системы доступа к информации и правил работы с конфиденциальными документами и базами электронных данных. Подобные факты подлежат оперативному, тщательному сравнительному анализу, а результаты анализа должны докладываться непосредственно первому руководителю фирмы.

В целях превентивного контроля рекомендуются следующие учетные и аналитические действия по отношению к персоналу, который обладает или может обладать конфиденциальной информацией:

- анализ реального состава известной персоналу конфиденциальной информации и динамики ее распределения по структурным подразделениям фирмы;

- анализ степени владения конфиденциальной информацией руководством фирмы, руководителями структурных под разделений, направлений деятельности и каждым работником, т.е. учет уровня и динамики их реальной осведомленности в секретах фирмы;

- анализ выявленных потенциальных и реальных источников угрозы персоналу в целом и каждому отдельному работнику с целью завладеть ценной информацией фирмы (конкурентов, соперников, криминальных структур и отдельных преступных элементов);

- анализ эффективности защитных мер, предпринятых по отношению к персоналу, их действенности в обычных условиях и при активных действиях злоумышленника.

Своевременный учет состава конфиденциальной информации, известной каждому из работников фирмы, является наиболее информативной частью аналитической работы в целом. Учитываются любые контакты любого работника фирмы с конфиденциальными сведениями, как санкционированные, так и случайные (ошибочные). Подлежит также учету вы явленное несанкционированное ознакомление с информацией, к которой работник не имел разрешения на доступ, в том числе несанкционированное ознакомление с информацией работника, во обще не имеющего допуска для работы с конфиденциальной информацией.

Для учета и последующего анализа степени осведомленности работников в секретах фирмы ведется специальная учетная форма.

Традиционная (карточная) или электронная учетная форма должна содержать ряд предметных зон, позволяющих сопоставлять функциональные обязанности сотрудника и состав конфиденциальной информации, полученной сотрудником, и который должен соответствовать выполняемым видам работы.Целесообразно включить в учетную форму следующие зоны:

- зона штатных функциональных обязанностей работника, при реализации которых используется конфиденциальная информация (по утвержденной должностной инструкции);

- зона изменений и дополнений, внесенных в функциональные обязанности работника, с указанием документа-основания, его даты и фамилии руководителя, подписавшего документ;

- зона стандартного состава конфиденциальные сведений или их индексов, по перечню конфиденциальной информации фирмы, к которым допущен работник в соответствии с должностной инструкцией (с указанием наименования документа о допуске, его даты, номера и фамилии руководителя, подписавшего документ);

- зона изменений и дополнений в составе конфиденциальных сведений, к которым допускается работник в связи с пересмотром его должностных обязанностей (с указанием наименований и дат документов о допуске, фамилий руководителей, подписавших документы);

- зона документированной информации (документов), с которой знакомится или работает сотрудник, с указанием наименований документов, их дат и номеров, краткого содержания, целевого использования содержащихся в документах конфиденциальных сведений или их индексов по перечню, фамилий руководителей, разрешивших работу с документами;

- зона недокументированной конфиденциальной информации, которая стала известна работнику, с указанием даты и цели ознакомления, фамилии руководи теля, разрешившего ознакомление, со става конфиденциальных сведений или их индексов по перечню;

- зона обнаруженного несанкционированного ознакомления работника с конфиденциальной информацией с указанием даты ознакомления, условий или причин ознакомления, фамилии виновного работника, места ознакомления, со става конфиденциальных сведений или их индексов по перечню.

Анализ осуществляется сравнением содержания записей в зонах и индексов известной сотруднику конфиденциальной информации, т.е. ведется поиск не соответствия.

По фактам разглашения или утечки конфиденциальной информации, утраты документов и изделий, другим грубым нарушениям правил защиты информации организуется служебное расследование.

Служебное расследование проводит специальная комиссия, формируемая приказом первого руководителя фирмы. Расследование предназначено для выяснения причин, всех обстоятельств и их последствий, связанных с конкретным фактом, установления круга виновных лиц, размера причиненного фирме ущерба. По результатам расследования даются рекомендации по устранению причин случившегося.

План проведения служебного рас следования:

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

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

- назначение ответственных лиц за проведение каждого мероприятия;

- указание сроков проведения каждого мероприятия;

- определение порядка документирования;

- обобщение и анализ выполненных действий по всем мероприятиям;

- установление причин утраты информации, виновных лиц, вида и объема ущерба;

- передача материалов служебного рас следования с заключительными вывода ми первому руководителю фирмы для принятия решения.

При проведении служебного расследования все мероприятия обязательно документируются в целях последующего комплексного анализа выявленного факта. Обычно анализируются следующие виды документов:

- письменные объяснения опрашиваемых лиц, составляемые в произвольной форме;

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

- другие документы, относящиеся к расследованию (справки, заявления, планы, анонимные письма и т. д.).

Служебное расследование проводится в кратчайшие сроки. По результатам анализа составляется заключение о результатах проведенного служебного рас следования, в котором подробно описывается проведенная работа, указываются причины и условия случившегося и полный анализ происшедшего.

**3.6** Правовые аспекты применения полиграфа

В настоящее время в России использование полиграфа законом не запрещено. Получение лицензии на его приобретение и использование не требуется.

Имеются различные ведомственные корпоративные акты, регламенты, инструкции, касающиеся применения полиграфа. При этом прямое законодательное регулирование использования полиграфа в деятельности государственных и коммерческих структур отсутствует. Однако анализ российского законодательства дает повод утверждать о наличии серьезных и правомочных оснований использования полиграфа в частном секторе. Можно уверенно констатировать, что сегодня не существует каких-либо правовых барьеров для широкого применения проверок на полиграфе в интересах кадрового отбора.

Согласно ныне действующему Трудовому кодексу РФ, работодатель имеет право вводить ограничения или делать предпочтение при приеме на работу, исходя из требований, свойственных определенному виду труда или служебной деятельности.

Кроме этого Трудовой кодекс РФ предоставляет право работодателю собирать персональные данные работника - информацию, касающуюся конкретного работника и необходимую работодателю в связи с трудовыми отношениями (Глава 14, ст. 85-90). В этой же главе впервые вводится понятие персональных данных работника, дается определение процедурам обработки данных (ст. 85 ТК РФ): «Персональные данные работника - информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника. Обработка персональных данных работника - получение, хранение, комбинирование, передача или любое другое использование персональных данных работника». Сюда же можно отнести и данные, полученные с помощью тестирования на полиграфе.

В ст. 86 ТК РФ (п.п.1, 3, 4, 5, 8) установлены ограничения в постановке вопросов, касающихся политических, религиозных убеждений, частной жизни, ответы на которые работодатель получает с помощью обработки персональных данных. Трудовой кодекс РФ предусматривает добровольность предоставления работником таких данных, ознакомление с ними, письменное согласие на передачу таких данных работодателю, запрещение получать такие данные через третьих лиц без письменного согласия работника.

Получение персональных данных работника, как это явствует из статей Трудового кодекса РФ, осуществляется от него самого, и необходимо работодателю для решения вопросов о «трудоустройстве, продвижении по службе, обеспечения личной безопасности работников, обеспечения сохранности имущества».

Согласно комментарию к новому Трудовому кодексу РФ, метод тестирования (которым, по сути, и является проверка на полиграфе), признается одним из современных методов организации подбора и расстановки кадров (глава 11 ТК РФ «Заключение трудового договора»). Поэтому, в должном соответствии с Трудовым кодексом является включение в Трудовой договор положения о том, что работник «обязан активно содействовать проводимым работодателем служебным разбирательствам и, в случае необходимости, проходить опрос с использованием полиграфа». Итак, внесение указанных выше положений в трудовые договоры и локальные правовые нормативные акты делают применение полиграфа государственными и негосударственными пользователями вполне легитимным в рамках действующего отечественного законодательства. В связи с этим вопрос - «Применять или не применять полиграф при работе с кадрами?» - носит уже не столько правовой, сколько эмоциональный характер.

Полиграф является, согласно действующему Трудовому кодексу РФ, законным при соблюдении определенных норм. Согласно этим нормам, проведение опроса на полиграфе - акт сугубо добровольный, и никто не вправе насильно заставить человека проходить его. Перед началом проверки на полиграфе тестируемый должен дать свое письменное согласие на это. К тому же следует использовать только те приборы, которые имеют соответствующий сертификат и не наносят ущерба здоровью и психологическому состоянию обследуемых, кроме этого важно привлекать к работе на полиграфе только обученных специалистов. И еще раз надо подчеркнуть: опрашиваемые обязательно должны быть ознакомлены со своими правами перед началом обследования.

Основная идея, положенная в основу работы полиграфа, заключается в том, что наше сознание изначально запрограммировано на правду, только правду и ничего, кроме правды. Именно поэтому когда мы лжем, возникает эмоциональный дискомфорт (стресс), который выражается в определенных физиологических реакциях, которые можно фиксировать и объективно измерять в связи с тем, что сознательный контроль вегетативных функций, связанных с переживанием тех или иных эмоций большей частью невозможен.

Любая жизненно важная для человека информация - «убил - не убил», «украл - не украл», «принимал наркотики - не принимал» и так далее - всегда откладывается в его памяти. Поэтому «мишенью» для полиграфа является память опрашиваемого лица.

Задача полиграфа сводится к тому, что бы определить владеет ли обследуемой определенной информацией или нет. При этом, чем важнее для человека какая-либо информация, тем больше его стресс при попытке эту информацию скрыть.

Понятно, что полиграф эффективен только в том случае, если испытуемый осознает возможность разоблачения - это как раз и создает тот самый стресс, контролировать который человек не может и на который реагирует прибор.

Подводя итог данной главе, хотелось бы отметить, что нормы главы 14 ТК РФ, обязывающие работодателя создать и ввести в действие положение о защите персональных данных работника, действуют уже более четырех лет, но, несмотря на это, многие работодатели сталкиваются с трудностями при создании данного локального нормативного акта. Данный локальный акт должен содержать:

* Положение о защите персональных данных работников.
* Расписку об ознакомлении работника с Положением о защите персональных данных.
* Обязательство о неразглашении персональных данных работников.
* Письменное согласие работника на получение его персональных данных у третьих лиц.
* Уведомление.
* Согласие работника на обработку его персональных данных.
* Запрос о доступе работника к своим персональным данным.
* Уведомление об уничтожении, (изменении, прекращении обработки, устранении нарушений персональных данных).

**4. Ответственность за нарушение правил работы с персональными данными**

Статья 90 ТК РФ предусматривает ответственность за нарушение норм, регулирующих получение, обработку и защиту персональных данных работника. Нарушитель может нести дисциплинарную, административную, гражданско-правовую и уголовную ответственность.

Таблица.2.Типичные нарушения, влекущие уголовную и административную ответственность

|  |  |  |
| --- | --- | --- |
| Характер нарушения | Типичные примеры | Нормы ответственности |
| Сбор информации без согласия работника | Применение негласного видеонаблюдения и прослушивания  Просмотр электронной и бумажной корреспонденции без предупреждения | Ст.ст. 137, 138 УК РФ  Ст. 138 УК РФ |
| Сбор информации, не касающейся трудовых отношений | Установление средств наблюдения в доме работника, ведение слежки в публичных местах и т.д. | Ст.ст. 137, 139 УК РФ |
| Нарушение установленного порядка сбора информации | Превышение частным детективным агентством своих полномочий  Превышение охранно-сыскным подразделением предприятия своих полномочий | Отзыв лицензии  Ст.ст. 137, 138 УК РФ |
| Нарушение установленного порядка использования информации | Отказ работнику в доступе к его персональным данным  Умышленное распространение информации о частной жизни работника  Небрежное обращение с персональными данными, непринятие мер к обеспечению их конфиденциальности | Ст. 140 УК РФ  Ст. 137 УК РФ или ст. 13.14 КоАП РФ (если сведения не составляют семейную и личную тайну)  Ст. 13.11 КоАП РФ |

**4.1 Уголовная ответственность**

Самая строгая, конечно, уголовная ответственность. Статья 137 УК РФ предусматривает наказание за незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную и семейную тайну. Уголовная ответственность грозит в том случае, если эти действия совершены намеренно, из корыстной или иной личной заинтересованности и повлекли за собой нарушение законных прав и свобод граждан. Причем наказание ужесточается, если виновный использовал свое служебное положение.

Личную или семейную тайну составляют сведения, не подлежащие, по мнению лица, которого они касаются, оглашению. Личную и семейную тайну не могут составлять сведения, которые были ранее опубликованы либо оглашены иным способом.

Нарушение неприкосновенности частной жизни (ст. 137 УК) может выражаться в:

а) незаконном собирании сведений о частной жизни;

б) незаконном их распространении;

в) незаконном их распространении в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации.

Закон не связывает ответственность за незаконное распространение сведений о частной жизни лица с конкретным способом распространения. Под распространением имеется в виду любая незаконная передача указанных сведений третьим лицам. Незаконным распространением является разглашение личной или семейной тайны лицом, обязанным ее хранить в силу своей профессии. В некоторых случаях разглашение сведений о частной жизни по УК образует одновременно состав другого преступления например, разглашение тайны усыновления (ст. 155), В таких случаях содеянное квалифицируется по совокупности со ст. 137 УК.

Обязательным элементом объективной стороны преступления, предусмотренного ст. 137 УК, является причинение вреда правам и законным интересам граждан. Характер вреда закон не ограничивает. Он может быть:

а) материальным (имущественным), например потеря хорошо оплачиваемой работы, срыв выгодной сделки, иные убытки в предпринимательской деятельности;

б) физическим (телесным), например заболевание от пережитого;

в) моральным, например распад семьи, подрыв репутации.

Установление наличия вреда правам и законным интересам потерпевшего производится в каждом конкретном случае с учетом индивидуальных особенностей личности и ситуации.

Нарушение неприкосновенности частной жизни считается оконченным преступлением только с момента причинения соответствующего вреда (материальный состав).

Субъективная сторона данного преступления характеризуется прямым умыслом. Обязательным элементом субъективной стороны является мотив: корыстная или иная личная заинтересованность. Корыстная заинтересованность выражается в стремлении приобрести материальную (имущественную) выгоду за счет потерпевшего или в виде вознаграждения от третьей стороны. Иная личная заинтересованность может заключаться в стремлении дискредитировать конкурента, сделать карьеру, отомстить за что-либо, продемонстрировать свое превосходство либо привлечь внимание к себе.

Ответственность по ч. 1 ст. 137 УК несет любое физическое вменяемое лицо, достигшее 16 лет (общий субъект), а по ч. 2 ст. 137 УК - должностное лицо либо служащий государственного или муниципального учреждения, использующий для совершения преступления свое служебное положение (специальный субъект).

А если кадровик или руководитель допустили ситуацию, когда информация о работнике стала известна другим, ненамеренно? Или даже существует пока только угроза "утечки" такой информации? Тогда в ход могут пойти меры административной и дисциплинарной ответственности, которые применяются к должностным лицам предприятия.

Гражданско-правовая ответственность за ограничения приватности возможна, как правило, в порядке возмещения морального вреда (ст.ст.151, 1099-1101 ГК РФ). В силу сложившихся в судебной практике подходов работнику будет нетрудно доказать, что любые действия по негласному наблюдению и сбору информации без его согласия причиняют ему моральный вред. В случае же, если разглашение конфиденциальной информации о гражданине повлекло ущерб его деловой репутации и имущественным интересам, он вправе потребовать и возмещения имущественных потерь.

**4.2 Административная ответственность**

Административные штрафы. Нарушение правил работы с персональными данными может повлечь административную ответственность работодателя или его представителей. Кодекс РФ об административных правонарушениях содержит на этот счет две статьи.

Статья 13.11 предусматривает ответственность в виде предупреждения или наложения штрафа на работодателя в размере от 5 до 10 МРОТ за нарушение установленного порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных). Этот порядок установлен главой 14 Трудового кодекса РФ и локальными нормативными актами предприятия.

Объективная сторона данного правонарушения состоит в действии или бездействии, нарушающем установленный законом порядок сбора, хранения, использования или распространения информации о гражданах (персональных данных). Вина в совершении данного правонарушения может быть как умышленной, так и неосторожной.

Ввиду того, что персональные данные - один из видов охраняемой законом тайны, защита ее конфиденциальности предусмотрена также статьей 13.14 КоАП РФ. Если лицо, получившее доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, разгласило сведения, составляющие персональные данные, то административный штраф для него будет составлять от 40 до 50 МРОТ.

Объектом правонарушения, предусмотренного данной статьей, является порядок получения информации с ограниченным доступом.

Объективная сторона данного правонарушения состоит в действии, представляющем собой разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей.

Отнесение информации к конфиденциальной осуществляется в порядке, установленном отраслевым законодательством Российской Федерации (гражданским, административным и т.д.).

Вина в совершении данного правонарушения может быть как умышленной, так и неосторожной.

К административной ответственности работодателя или его представителей может привлечь Рострудинспекция или суд.

**4.3 Дисциплинарная ответственность**

Дисциплинарная ответственность кадровика. В отношении сотрудника-кадровика работодатель вправе применить одно из дисциплинарных взысканий, предусмотренных статьей 192 Трудового кодекса РФ: замечание, выговор, увольнение. Более того, кодекс предусматривает специальное основание для расторжения трудового договора по инициативе работодателя в случае разглашения охраняемой законом тайны, ставшей известной работнику в связи с исполнением им трудовых обязанностей (п.п. "в" п.6 ст.81).

Дисциплинарная ответственность работников является самостоятельным видом юридической ответственности. К дисциплинарной ответственности могут привлекаться работники, совершившие дисциплинарный проступок.

Как и любое другое правонарушение, дисциплинарный проступок обладает совокупностью признаков: субъект, субъективная сторона, объект, объективная сторона.

Субъектом дисциплинарного проступка может быть гражданин, состоящий в трудовых правоотношениях с конкретной организацией и нарушающий трудовую дисциплину.

Субъективной стороной дисциплинарного проступка выступает вина со стороны работника. Она может быть в форме умысла или по неосторожности.

Объект дисциплинарного проступка - внутренний трудовой распорядок конкретной организации. Объективной стороной здесь выступают вредные последствия и прямая связь между ними и действием (бездействием) правонарушителя.

В соответствии с заключенным трудовым договором работодатель вправе требовать от работника выполнения трудовых обязанностей. Согласно ст. 192 Кодекса работодатель имеет право, но не обязан привлекать к дисциплинарной ответственности работника, совершившего дисциплинарный проступок. Однако следует знать, что настоящим Кодексом, другими федеральными законами, уставами и положением о дисциплине могут быть определены и иные правила при совершении дисциплинарного проступка.

Разглашение может быть совершено среди коллег, знакомых, родственников и других лиц, не имеющих законного доступа к ним. Кроме разглашения основными видами нарушений правил работы с персональными данными являются незаконное получение или использование сведений, составляющих персональные данные, и утрата материальных носителей, содержащих данную информацию. Следует подчеркнуть, что увольнение работника может быть осуществлено только за разглашение персональных данных. В иных случаях работодатель вправе наложить на виновное лицо другое дисциплинарное взыскание.

К дисциплинарной ответственности могут быть привлечены лишь те работники кадровой службы, которые приняли на себя обязательство соблюдать правила работы с персональными данными. То есть условие о неразглашении сведений, составляющих персональные данные, было включено в их трудовой договор, они были ознакомлены с локальными нормативными актами по вопросу защиты этой конфиденциальной информации, а работодатель создал для работы все необходимые условия. Если такая подготовительная работа не была проведена, то специалист, кому доверена работа с персональными данными, нести ответственности не будет.

Факт нарушения правил работы с персональными данными может быть установлен представителем работодателя (например, начальником отдела кадров), самим работником или специалистом Рострудинспекции.

Работники и их представители имеют право осуществлять контроль над выполнением требований по защите конфиденциальности этой категории информации, запрещать или приостанавливать обработку персональных данных в случае их невыполнения. Любые неправомерные действия (бездействие) работодателя при обработке и защите персональных данных работник вправе обжаловать в судебном порядке.

**Заключение**

Сегодня многие предприятия, стремясь обеспечить информационную безопасность своей коммерческой деятельности, подкрепляют формальные меры (такие как подписание договоров о неразглашении информации) практическими мероприятиями охранного характера, в рамках которых тем или иным образом нарушается неприкосновенность частной жизни работников. И здесь интересы бизнеса могут вступать в конфликт с принципом недопустимости вмешательства в частную жизнь.

Конституция РФ закрепила свободу поиска, получения, передачи, производства и распространения информации (ч. 4 ст. 29), гарантировала право на неприкосновенность частной жизни, личную, семейную тайну, тайну сообщений и запретила распространение информации о частной жизни лица без его согласия (ст.ст. 23, 24). Жизнедеятельность человека предполагает предоставление информации о себе другим членам общества. Отношения по предоставлению и охране информации регулируются нормами российского права.

Таким образом, проанализировав ситуацию по поводу охраны персональных данных работника, можно сделать следующие выводы.

1. Личная тайна работника охраняется законом на самом высоком уровне. Законодатель предусмотрел практически все необходимые нормы для защиты этой категории правоотношений. Однако следует заметить, что основным источником правонарушений в области охраны персональных данных персонала служит неграмотность работников кадровых служб в указанных вопросах, вызванная, тем, что нормативно не отрегулирован порядок организации деятельности по сохранности персональных данных в организациях и на предприятиях.

2. Не существует обязательных правил хранения персональных данных. Конечно, нельзя не сказать, что Рострудинспекция при проведении проверок требует очень веские доказательства сохранности указанных сведений.

3. Нормы главы 14 Трудового кодекса «Защита персональных данных работника» носят скорее инструктивный характер, регламентируют сбор и хранение информации о работнике.

Думается, что Правительству РФ следовало бы разработать и утвердить правила, регулирующие порядок хранения и использования персональных данных на предприятии и в организациях.

4. Лица, виновные в нарушении установленных норм, регулирующих получение, обработку и защиту персональных данных работников, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность.

Надо отметить, что санкции, предусмотренные за нарушение законодательства по охране персональных данных работника достаточно адекватны и соответствуют мере правонарушения. Но санкции скорее восстанавливают справедливость, нежели снижают количество правонарушений.

5. Все механизмы сбора информации о работниках должны применяться только на основании принятых в надлежащем порядке внутриорганизационных норм. Использование видеонаблюдения, прослушивания, контроля за перепиской, контроля за перемещениями работников по предприятию и других мер должно быть урегулированы правилами внутреннего распорядка или специальным регламентом. Этот документ должен быть доступен всем работникам предприятия. Все меры наблюдения и контроля, не урегулированные таким документом, могут рассматриваться работниками как незаконное вторжение в их частную жизнь. Если на предприятии действует служба безопасности (как обособленное подразделение), ее права следует четко указать в уставе этого подразделения, который должен быть согласован с органами внутренних дел (ст.14 Закона РФ «О частной детективной и охранной деятельности в РФ»).

6. Необходимо получать согласие работников на ограничения их приватности. Это можно зафиксировать непосредственно в трудовом договоре. Однако работник, приступающий к работе, в любом случае должен подписать документ о согласии на применение мер наблюдения или контроля; его следует под расписку ознакомить с действующими правилами сбора и обработки персональных данных. Следует учесть также, что такие нематериальные блага, как честь и достоинство, личная и семейная тайна, являются неотчуждаемыми (ст. 150 ГК РФ, п. 9 ст. 86 ТК РФ); следовательно, согласие на применение мер, ущемляющих честь и достоинство работника и ограничивающих его право на тайну, будет в случае конфликта признано недействительным.

7. Собираемая информация должна касаться исключительно служебной деятельности работника и не затрагивать его частную жизнь. Помимо обеспечения интересов работника, целью сбора персональных данных может быть лишь контроль за количеством и качеством работы, а также за сохранностью имущества. Поэтому, например, контроль за электронной перепиской со служебного электронного адреса, хотя и допустим, но все же должен ограничиваться регистрацией адресатов и не касаться содержания пересылаемых сообщений. Это же касается телефонных линий и других средств сообщения. Использование служебного имущества и служебных средств связи в личных целях может повлечь дисциплинарное взыскание, но работодатель не вправе на этом основании вмешиваться в личную жизнь работника.

8. Любую информацию о работнике необходимо получать из законных источников. Законным источником, согласно п. 3 ст. 86 ТК РФ, является или сам работник, или такой источник, на обращение к которому он дал согласие. Следовательно, информация о работнике, полученная работодателем случайно из сторонних источников, не может быть включена в состав персональных данных; она не может обрабатываться, храниться на предприятии и тем более не может передаваться третьим лицам.

Большое значение имеет то, как работодатель относится к конституционным правам своих работников. Ведь только администрация предприятия или организации в состоянии вести непрерывный контроль за соблюдением установленного порядка осуществления защиты персональных данных работников.

**Библиография**

**Нормативная литература**

1. Всеобщая декларация прав человека (принята на третьей сессии Генеральной Ассамблеи ООН резолюцией 217 А (III) от 10 декабря 1948 г.). - М.: Права человека, 2000.

2. Конвенция о защите прав человека и основных свобод (Рим, 4 ноября 1950 г.) (с изменениями от 21 сентября 1970 г., 20 декабря 1971 г., 1 января, 6 ноября 1990 г., 11 мая 1994 г.). – М.: Права человека, 2000.

3. Международный пакт о гражданских и политических правах (Нью-Йорк, 19 декабря 1966 г.). – М.: Права человека, 2000.

4. Конвенция о правах и основных свободах человека, 1995 год. – М.: Права человека, 2000.

1. Конституция Российской Федерации от 12 декабря 1993 года. – М.: Норма, 2009.
2. Уголовный кодекс РФ от 13 июня 1996 г. – М.: Кодекс, 2009.
3. Кодекс РФ об административных правонарушениях от 30 декабря 2001 г. – М.: Кодекс, 2009.

Трудовой кодекс РФ от 30 декабря 2001 г. – М.: Гросс медиа, 2009.

9. Гражданский кодекс РФ. – М.: Норма, 2009.

1. Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 г. // СПС Консультант Плюс.
2. Федеральный закон № 152-ФЗ «О персональных данных» от 27.07.2006 г. (в ред. от 27.12.2009 г.) // СПС Консультант Плюс.
3. Перечень сведений конфиденциального характера, утв. Указом Президента РФ от 6.03.1997 г. № 188 (в ред. Указа Президента от 23.09.2005 г.). // СПС Консультант Плюс.
4. Положение об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации, утв. Постановлением Правительства РФ от 15.09.2008 г. № 687. // СПС Консультант Плюс.
5. Постановление Министерства труда и социального развития РФ № 69 от «Об утверждении инструкции по заполнению трудовых книжек» 10.10.2003 г.. // СПС Консультант Плюс.

**Специальная литература**

1. Айман Т.О. Трудовое право. – М.: РИОР, 2007.
2. Басаков М.И. Трудовое право: Конспект лекций. – М.: Феникс, 2007.
3. Комментарий к Трудовому кодексу Российской Федерации. / Под ред. К.Н. Гусова - ООО «ТК Велби», ООО «Издательство Проспект», 2006.
4. Демин Ю.М. Делопроизводство, подготовка служебных документов. - С-П, 2004.
5. Демократия на производстве. Практика передовых стран Запада. – М., Наука, 2003.
6. Исаев А.К. Трудовое право Российской Федерации. – М.: Омега-Л, 2007.
7. Казанцев В.И., Васин В.Н. Трудовое право. – М.: Академия, 2006.
8. Комментарии официальных органов к Трудовому кодексу РФ. - М.: Инфра-М, 2006.
9. Кашанина Т.В. Корпоративное (внутрифирменное) право. – М.: Норма, 2007.
10. Коршунов Ю.Н., Коршунова Т.Ю., Кучма М.И., Шеломов Б.А. Комментарий к Трудовому Кодексу РФ. – М.: Спарк, 2005.
11. Комментарий к Кодексу Российской Федерации об административных правонарушениях. / Под ред. Ю.М. Козлова – М.: Юристъ, 2006.
12. Кузьмин И. Внимание! Сведения конфиденциальные. // Российская юстиция, № 4. 2007.
13. Куракин П. Контроль защиты информации. // Кадровое дело, № 9. 2005.
14. Комментарий к Уголовному кодексу Российской Федерации. / Под ред. В.М. Лебедева. – М.: Юристъ, 2005.
15. Лебедева Е.С. Трудовое законодательство. – М.: Центр ЮрИнфоР, 2007.
16. Мачульская Е.Е. Правовое регулирование персональных данных работника в Российской Федерации и государствах– участниках СНГ. – М.: МГУ им. Ломоносова, 2005.
17. Мышко Ф.Г., Михайлов Ф.Н., Курочкина В.В. Трудовое право. – М.: ЮНИТИ, 2006.
18. Постатейный Комментарий к Уголовному кодексу РФ 1996 г. / Под ред. А.В. Наумова.– М.: Проспект, 2004.
19. Основные права человека в сфере труда и их защита. Основополагающие международные правовые документы-стандарты. // Библиотека «Российской газеты». Вып. № 22-23. 1999.
20. Николаев С.Н. Трудовые отношения: правовые основы регулирования, судебная практика. – М.: Налоговый вестник, 2006.
21. Орловский Ю.П., Нуртдинова А.Ф. Трудовое право. – М.: МЦФЭР, 2005.
22. Смирнов О.В. Трудовое право. – М.: Проспект, 2007.
23. Смоленский М.Б. Трудовое право для студентов вузов. – М.: Феникс, 2008.
24. Снежко О.А. Трудовое право РФ: Учебный комплекс курса. – М.: ПРИОР, 2004.
25. Степанов Е. Учетная карточка – как личное дело. // Кадровое дело, №3. 2004.
26. Степанов Е. Персональные данные и их защита. // Кадровое дело, №9. 2007.
27. Степанов Е. Защита информации при работе с ЭВМ. // Кадровое дело, № 2. 2006.
28. Ситникова Е. Дисциплинарная ответственность работника. // Кадровое дело, № 1. 2006.

### 29. Трудовое право России: учебник для вузов. / Под ред. С.Ю. Головиной, М.В. Молодцова. – М.: Норма, 2008.

### 30. Трудовое право России. /Под ред. С.П. Маврина, Е.Б. Хохлова. – М.: Норма, 2008.

### 31. Трудовое право России. / Под общ. ред. Е.Б. Хохлова, В.А. Сафонова. – М.: Юрайт, 2008.

32. Французова Л. Личные данные работников. // Кадровое дело, № 4. 2004.

33. Шириков А. Безопасность против приватности? // Экономика и жизнь, 2005. №3.

**Приложение 1. Положение о защите персональных данных работников**

«УТВЕРЖДАЮ»

Директор ООО "ОООО"

Иванов В.И.

«\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_ 2010 г.

**Положение о защите персональных данных работников ООО "ОООО"**

**1. Общие положения**

1.1. Персональные данные Работника – информация, необходимая Работодателю в связи с трудовыми отношениями и касающаяся конкретного Работника.

1.2. Обработка персональных данных – получение, хранение, комбинирование, передача или другое любое использование персональных данных Работника.

Обработка персональных данных Работников осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия Работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности Работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

1.3. Объем, содержание и обработка персональных данных регламентируется Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом «Об информации, информатизации и защите информации» и другими нормативными правовыми актами.

1.4. Запрещается получать и обрабатывать персональные данные Работника о его политических, религиозных и иных убеждениях, частной жизни, членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами (в соответствии со статьей 24 Конституции Российской Федерации данные о частной жизни Работника разрешается получать и обрабатывать с его письменного согласия).

**2. Порядок сбора, обработки и хранения персональных данных**

2.1. Все персональные данные Работника Работодатель получает у него самого через заместителя по кадрам и общим вопросам или юрисконсульта.

2.2. Если персональные данные Работника возможно получить только у третьей стороны то Работодатель имеет на это право только если эти данные необходимы в целях предотвращения угрозы жизни и здоровья Работника, других лиц, предотвращения террористических актов или других противоправных действий а также для обеспечения сохранности охраняемых материальных средств.

2.3. Персональные данные Работников обрабатываются и хранятся у заместителя по кадрам и общим вопросам, бухгалтерии.

- в электронном виде на персональных ЭВМ без права хранения на внешних носителях информации (дискеты, компакт-диски).

- на бумажных носителях в специально оборудованных шкафах и сейфах (трудовые книжки, личные дела, личные карточки Работников по форме Т-2).

2.4. При передаче персональных данных Работника Работодатель должен соблюдать следующие требования:

2.4.1.Не сообщать персональные данные Работника третьей стороне без письменного согласия Работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровья Работника, других лиц или сохранности охраняемого имущества.

2.4.2.Не сообщать персональные данные Работника в коммерческих целях без его письменного согласия.

2.4.3.Разрешать доступ к персональным данным Работников только:

- генеральному директору – в полном объеме;

- заместителю по кадрам и общим вопросам, юрисконсульту – в полном объеме;

- начальнику участка, главному инженеру, бухгалтерии – по направлениям деятельности.

2.4.4. В другие организации персональные данные представляются Работодателем по почте установленным порядком только по письменному запросу организации с письменного согласия самого Работника.

**3. Права Работников в целях обеспечения защиты персональных данных, хранящихся у Работодателя**

3.1. Работники имеют право на:

3.1.1. Свободный, бесплатный доступ к своим персональным данным, включая право на получение копий любой записи (по письменному заявлению), за исключением случаев, предусмотренных федеральным законом.

3.1.2. Требование об исключении или исправлении неверных или неполных персональных данных.

3.1.3. Требование об извещении всех лиц, которым ранее были сообщены неверные или неполные персональные данные Работника.

3.1.4. Определение своих представителей для защиты персональных данных.

3.1.5. Обжалование в суд любых неправомерных действий или бездействий при обработке и защите его персональных данных.

**4. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных Работника**

4.1. Лица, виновные в нарушении норм, регулирующих обработку и защиту персональных данных Работника, несут ответственность в соответствии с действующим законодательством Российской Федерации.

Исполнитель:

Заместитель по кадрам и общим вопросам

Юрисконсульт: