**Содержание:**

**Введение** 3

**Глава I** 4

Персональные данные

Правовое регулирование 4

Понятие персональных данных их отграничение от другой информации 6

Работа кадровой службы с персональными данными 7

Общие требования при обработке персональных данных работника и

гарантии их защиты 9

Передача персональных данных работников 14

Защита информации при работе с ЭВМ 15

Контроль защиты информации 20

**Глава II** 26

Ответственность за нарушение правил работы с персональными данными

Уголовная ответственность 26

Административная ответственность 28

Дисциплинарная ответственность 29

**Заключение** 32

**Список литературы** 33

**Приложение** 34

Личная карточка работника 34

Приказ о приеме работника на работу 40

Приказ о переводе работника на другую работу 41

Приказ о прекращении действия трудового договора 42

Приказ о поощрении работника 43

**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.

Цель этой работы заключается в исследовании трудовых отношений в сфере защиты персональных данных работника. Рассматривается порядок работы с конфиденциальными сведениями о работнике, способы их защиты, а также ответственность работодателя за невыполнение обязательств по обеспечению сохранности персональных данных.

**Глава I**

**Персональные данные**

**Правовое 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»[[1]](#footnote-1). Право на уважение к личной и семейной жизни содержится так же и в Конвенции о защите прав человека и основных свобод[[2]](#footnote-2). 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[[3]](#footnote-3).

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. [[4]](#footnote-4)

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

Во-первых, это Конституция РФ[[5]](#footnote-5). 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». Т.о. 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, информатизации и защите информации"[[6]](#footnote-6). 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»[[7]](#footnote-7).

Сфера отношений, касающаяся персональных данных работника регулируется гл.14 Трудового кодекса Российской Федерации[[8]](#footnote-8). Где установлено понятие персональных данных работника, установлен порядок работы с ними и закрепляется ответственность работодателя за нарушение соответствующих норм.

**Понятие персональных данных, их отграничение 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)[[9]](#footnote-9).

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.

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[[10]](#footnote-10).

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.[[11]](#footnote-11)

**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[[12]](#footnote-12).

**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.

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 рас­следованиям 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 (Приложение 1)) 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 Тим 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 от­дел кадров для включения в дело вместо хранящейся там копии.

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

* журнал табельного учета с указанием должностей, фамилий и инициалов сотруд­ников (находится у работника, ведущего табельный учет, - табельщика),
* штатное расписание (штатный форму­ляр) подразделения, в котором 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 под­разделения (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 не­рабочее 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[[13]](#footnote-13).

**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.

**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 сиг­нала 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, под­бор 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 по­мнить о его многоступенчатом характере. Можно выделить следующие главные состав­ные части доступа этого вида:

* доступ к персональному компьютеру, сер­веру или рабочей станции;
* доступ к машинным носителя информации, хранящимся вне ЭВМ;
* непосредственный доступ к базам данных и файлам.

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

* определение и регламентацию первым ру­ководителем фирмы состава сотрудников, имеющих право доступа (входа) в помещение, в котором находится соответствующая вычис­лительная техника, средства связи;
* регламентацию первым руководителем временного режима нахождения этих лиц в указанных помещениях; персональное и вре­менное протоколирование (фиксирование) руководителем подразделения или направле­ния деятельности фирмы наличия разрешения и периода работы этих лиц в иное время (на­пример, в вечерние часы, выходные дни и др.);
* организацию охраны этих помещений в ра­бочее и нерабочее время, определение правил вскрытия помещений и отключения охранных технических средств информирования и сиг­нализирования; определение правил поста­новки помещений на охрану; регламентацию работы указанных технических средств в ра­бочее время;
* организацию контролируемого (в необхо­димых случаях пропускного) режима входа в указанные помещения и выхода из них;
* организацию действий охраны и персона­ла в экстремальных ситуациях или при ава­риях техники и оборудования помещений;
* организацию выноса из указанных поме­щений материальных ценностей, машинных и бумажных носителей информации; конт­роль вносимых в помещение и выносимых персоналом личных вещей.

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 машиночитаемо­го документа. Подобная проблема несуще­ственна для носителей, содержащих откры­тую информацию. В основе обеспечения сохранности носителей электронных конфи­денциальных документов, находящихся вне машины, в настоящее время эффективно ис­пользуются зарекомендовавшие себя принци­пы и методы обеспечения безопасности доку­ментов в традиционной технологической системе.

Перед началом обработки информации на ЭВМ сотрудник обязан убедиться в отсутствии в помещении посторонних лиц. При подходе такого лица к сотруднику экран дисплея дол­жен 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 учет­ной 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 фор­мах.

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.

**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 вы­полнении 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 руководите­ля 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 чело­века в общении путем обмена информа­цией. В связи с этим особенно важно, что­бы 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 ин­формации 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, не взирая 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 под­разделений, 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 персона­лом 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 под­разделений, 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 вы­явленное несанкционированное озна­комление с информацией, к которой ра­ботник не имел разрешения на доступ, в том числе несанкционированное озна­комление с информацией работника, во­обще 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 руководи­теля, разрешившего ознакомление, со­става 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, со­става конфиденциальных сведений или их индексов по перечню.

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

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 рас­следования:

* определение возможных версий слу­чившегося (утрата, хищение, уничтожение по неосторожности, умышленная пе­редача сведений, неосторожное разгла­шение и т.д.);
* определение (планирование) конкрет­ных мероприятий по проверке версий (осмотр помещений, полистная провер­ка документации, опрос сотрудников, взятие письменного объяснения у подо­зреваемого лица и т. д.);
* назначение ответственных лиц за про­ведение каждого мероприятия;
* указание сроков проведения каждого мероприятия;
* определение порядка документирова­ния;
* обобщение и анализ выполненных действий по всем мероприятиям;
* установление причин утраты инфор­мации, виновных лиц, вида и объема ущерба;
* передача материалов служебного рас­следования с заключительными вывода­ми 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 рас­следования, в котором подробно описы­вается проведенная работа, указываются причины и условия случившегося и полный анализ происшедшего.[[14]](#footnote-14)

**Глава II**

**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.

**Уголовная ответственность**

Самая строгая, конечно, уголовная. 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).[[15]](#footnote-15)

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. Остановимся на них подробнее.

**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.[[16]](#footnote-16)

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[[17]](#footnote-17).

**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.[[18]](#footnote-18)

**Заключение**

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

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, на мой взгляд, тем, что нормативно не отрегулирован порядок организации деятельности по сохранности персональных данных в организациях и на предприятиях.

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

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

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.

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.

**Список использованной литературы:**

**Книги и комментарии:**

1. Ю.М. Демин. Делопроизводство, подготовка служебных документов, С-П, 2003.
2. Комментарии официальных органов к Трудовому кодексу РФ, М., 2003.
3. Комментарий к Трудовому кодексу Российской Федерации (под ред. К.Н.Гусова) - ООО "ТК Велби", ООО "Издательство Проспект", 2003.
4. Комментарий к Трудовому Кодексу РФ (Коршунов Ю.Н., Коршунова Т.Ю., Кучма М.И., Шеломов Б.А.) - Спарк, 2002 г.
5. Комментарий к Кодексу Российской Федерации об административных правонарушениях (под ред. Ю.М.Козлова) - Юристъ, 2002.
6. Комментарий к Уголовному кодексу Российской Федерации (под ред. Лебедева В.М.).
7. Постатейный Комментарий к Уголовному кодексу РФ 1996 г. (под ред. Наумова А.В.).

**Публикации:**

1. И. Кузьмин. Внимание! Сведения конфиденциальные. // Российская юстиция. №4, 2002.
2. Е. Степанов. Учетная карточка – как личное дело. // Кадровое дело. №3, 2003.
3. Е. Степанов. Персональные данные и их защита. // Кадровое дело. №9, 2003.
4. Е. Степанов. Защита информации при работе с ЭВМ. // Кадровое дело. №2, 2001
5. П. Куракин. Контроль защиты информации. // Кадровое дело. №9, 2003.
6. Е. Ситникова. Дисциплинарная ответственность работника. // Кадровое дело. № 1, 2003.
7. Л. Французова. Личные данные работников. // Кадровое дело. №4, 2003.

**Нормативные акты:**

1. Всеобщая декларация прав человека (принята на третьей сессии Генеральной Ассамблеи ООН резолюцией 217 А (III) от 10 декабря 1948 г.).
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.).
3. Международный пакт о гражданских и политических правах (Нью-Йорк, 19 декабря 1966 г.).
4. Конвенция о правах и основных свободах человека, 1995 год.
5. Конституция Российской Федерации от 12 декабря 1993 года.
6. Уголовный кодекс РФ от 13 июня 1996 г. № 63-ФЗ.
7. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. N 195-ФЗ
8. Трудовой кодекс Российской Федерации от 30 декабря 2001 г. N 197-ФЗ (с изменениями от 24, 25 июля 2002 г., 30 июня 2003 г.).
9. Федеральный закон N 24-ФЗ "Об информации, информатизации и защите информации" от 20.02.1995 г. (СЗ РФ. 1995. №8.).
10. Перечень сведений конфиденциального характера (утв. Указом Президента РФ от 6 марта 1997 г. N 188).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Унифицированная форма № Т- 2  Утверждена постановлением Государственного комитета РФ по статистике  от 06.04.01 № 26 | | | | |
|  | | | | Код |
|  | | Форма по ОКУД | | 0301002 |
|  | | | по ОКПО |  |

наименование организации

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Дата  составления | Табельный номер | Идентификационный номер  налогоплательщика | Номер страхового свидетельства государственного пенсионного страхования | Алфавит | Характер работы | Вид работы  (основная,  по совместительству) | Пол  (мужской, женский) |
|  |  |  |  |  |  |  |  |

Личная карточка

работника

**I. ОБЩИЕ СВЕДЕНИЯ**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | |  | | Трудовой договор (контракт) | | | | | номер |  |
|  | |  | |  | | |  | | дата |  |
| 1. Фамилия |  | | Имя | |  | Отчество | |  | |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | |  | | | |  | | |  | | | |  | Код |
| 2. Дата рождения | |  | | | | | | | | | | |  |  |
| 3. Место рождения | | | день, месяц, год | | | | | | | | | по ОКАТО | |  |
| 4. Гражданство | |  | | | | | | | | | | по ОКИН | |  |
| 5. Знание иностранного языка | | | |  | | | | | | | | по ОКИН | |  |
|  | | | | наименование | | |  | степень знания | | | | по ОКИН | |  |
| 6. Образование | | | | наименование | | |  | степень знания | | | | по ОКИН | |  |
|  | среднее (полное, общее), начальное профессиональное, среднее профессиональное, высшее профессиональное | | | | | | | | | | |  | |  |
| наименование образовательного учреждения | | | | | Диплом, серия, номер | | | | | Год окончания | | | |  |
|  | | | | |  | | | | |  | | | |  |
|  | | | | |
| Квалификация по диплому | | | | | Направление или специальность по диплому | | | | | | | | |  |
|  | | | | |  | | | | | | Код по ОКСО | | |  |
|  | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| наименование образовательного учреждения | Диплом,  серия, номер | Год окончания | |  |
|  |  |  | |  |
|  |
| Квалификация по диплому | Направление или специальность по диплому | | |  |
|  |  |  | Код по ОКСО |  |
|  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 4. Послевузовское профессиональное образование |  | | | Код по ОКИН |  |
| аспирантура, адъюнктура, докторантура | | | |  |
| Наименование образовательного,  научного учреждения | Удостоверение, номер,  дата выдачи | | Год окончания | |  |
|  |  | |  | |  |
|  |  | |  | |  |
|  | Специальность |  |  | |  |
|  |  |  |  | |  |
|  |  |  | Код по ОКСО | |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | |  |  |  | |  | Код | |
| 7. Профессия |  | | | | по ОКПДТР | | |  | |
|  | основная | | | | по ОКПДТР | | |  | |
|  | другая | | | |  | | |  | |

2-я страница формы № Т-2

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8. Стаж работы (по состоянию на “ ” \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20 года): | | | | | |  | |  | | |
| Общий |  | дней |  | месяцев | |  | | лет |
| Непрерывный |  | дней |  | месяцев | |  | | лет |
| Дающий право на надбавку за выслугу лет |  | дней |  | месяцев | |  | | лет |
|  |  | дней |  | месяцев | |  | | лет |

|  |  |  |  |
| --- | --- | --- | --- |
| 9. Состояние в браке |  | Код по ОКИН |  |

|  |  |  |
| --- | --- | --- |
| 10. Состав семьи: |  |  |
| степень родства  (ближайшие родственники) | Фамилия, имя, отчество | Год рождения |
| 1 | 2 | 3 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 11. Паспорт: |  | | № | |  | | Дата выдачи | “ ” \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ года | | | |
| Выдан |  | |  | |  | |  | |  | |  |
| 12. Адрес места жительства: | | | |  | | | наименование органа, выдавшего паспорт | |  | |  |
|  | | Почтовый индекс | | | |  | | | |  | |
| По паспорту | |  | | | |  | | | |  | |
|  | |  | | | | | | | |  | |
|  | |  | | | |  | | | | | |
|  | | Почтовый индекс | | | |  | | | | | |
| Фактический | |  | | | |  | | | |  | |
|  | |  | | | | | | | |  | |

Дата регистрации по указанному месту жительства “ ” \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ года

Номер телефона \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**II. Сведения о воинском учете**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Категория запаса |  | | | |  | |  | | 6. Наименование военного  комиссариата по месту жительства | |  |
| 2. Воинское звание |  | | | |  | |  | |  | |  |
| 3. Состав (профиль) |  | | | |  | |  | | 7. Состоит на воинском учете: | |  |
| 4. Полное кодовое обозначение ВУС | |  | |  | |  | | а) общем (номер команды, партии) | | |  |
| 5. Категория годности к военной службе | |  | |  | |  | | б) специальном | | |  |
|  | | |  | |  | |  | | 8. |  | |

отметка о снятии с воинского учета

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Работник кадровой службы** | |  |  |  |  |  |
|  | | должность |  | подпись |  | расшифровка подписи |
| Работник |  |
|  | подпись |

“ ” \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20 года

**3**-я страница формы № Т-2

## **III. ПРИЕМ НА РАБОТУ**

## **И ПЕРЕВОДЫ НА ДРУГУЮ РАБОТУ**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Дата | Структурное  подразделение | Профессия  (должность), разряд, класс (категория) квалификации | Оклад (тарифная  ставка), надбавка,  руб | Основание | Подпись владельца трудовой книжки |
|
| 1 | 2 | 3 | 4 | 5 | 6 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

### **IV. АТТЕСТАЦИЯ**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Дата  аттестации | Решение комиссии | Документ (протокол) | | Основание |
| номер | дата |
| 1 | 2 | 3 | 4 | 5 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## **V. ПОВЫШЕНИЕ КВАЛИФИКАЦИИ**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Дата | | Вид  повышения  квалификации | Наименование  образовательного  учреждения, место его нахождения | Документ  (удостоверение, свидетельство) | | | Основание |
| начала  обучения | окончания  обучения |
| наименование | серия, номер | дата |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

### **VI. ПРОФЕССИОНАЛЬНАЯ ПЕРЕПОДГОТОВКА**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Дата | | Специальность  (направление,  профессия) | Документ  (диплом, свидетельство) | | | Основание |
| начала  переподготовки | окончания  переподготовки | наименование | номер | дата |
|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

4-я страница формы № Т-2

**VII. ПООЩРЕНИЯ И НАГРАДЫ**

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование награды | Документ | | |
| наименование | номер | дата |
| 1 | 2 | 3 | 4 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## **VIII. ОТПУСК**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Вид отпуска  (ежегодный, учебный, без сохранения заработной платы и др.) | Период работы | | Количество дней отпуска | Дата | | Основание |
| начала | окончания |
| с | по |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**IX. Социальные льготы,**

**на которые работник имеет право в соответствии с законодательством**

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование льготы | Документ | | Основание |
| номер | дата выдачи |
| 1 | 2 | 3 | 4 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**X. ДОПОЛНИТЕЛЬНЫЕ СВЕДЕНИЯ**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | |  | | | |  | | |  | | |
|  | | |  | | | |  | | |  | | |
|  | | |  | | | |  | | |  | | |
|  | | |  | | | |  | | |  | | |
|  | | |  | | | |  | | |  | | |
| **XI. Основание увольнения** | |  | | | | | | | | | |  |
| дата увольнения “ ” \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20 года | | | | | | | | | | | | |
| Приказ (распоряжение) № \_\_\_\_\_\_\_\_\_\_ от “ ” \_\_\_\_\_\_\_\_\_\_\_\_ 20 года | | | | | | | | | | | | |
|  | | | | | | | | | | | | |
| **Работник кадровой службы** | | | | |  |  |  | |  |  | |  |  |
|  | | | | | должность |  | подпись | |  | расшифровка подписи | | | |
| **Работник** | |  | | | |  | | | |  | |  |  |
|  | | подпись | | | |  | | | |  | |  |  |

***Унифицированная форма № Т-1***

***Утверждена постановлением Госкомстата России***

***от 6 апреля 2001 г. № 26***

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | | Код |
|  | Форма по ОКУД | | 0301001 |
|  | | по ОКПО |  |
| наименование организации | |  |  |

|  |  |  |
| --- | --- | --- |
|  | Номер документа | Дата |
| **ПРИКАЗ (РАСПОРЯЖЕНИЕ)** |  |  |
| **о приеме работника на работу** | | |

|  |  |  |
| --- | --- | --- |
|  |  | Дата |
| **Принять на работу** | с |  |
|  | по |  |

|  |  |
| --- | --- |
|  | Табельный номер |
|  |  |
| фамилия, имя, отчество |  |

|  |  |
| --- | --- |
| В |  |
| наименование структурного подразделения | |
|  | |
| наименование профессии (должности), разряд, класс (категория) квалификации | |
|  | |
|  | |
| условия приема на работу, характер работы | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| с окладом (тарифной ставкой) |  | руб. |  | коп. |
| надбавкой |  | руб. |  | коп. |

|  |  |  |
| --- | --- | --- |
| с испытательным сроком |  | месяцев |

О с н о в а н и е:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Трудовой договор (контракт) от « |  | » |  | 20 |  | года № |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Руководитель организации |  |  |  |  |  |
|  | должность |  | подпись |  | расшифровка подписи |

|  |  |
| --- | --- |
| С приказом (распоряжением) ознакомлен |  |
|  | подпись работника |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| « |  | » |  | 20 |  | года |
|  |  |  |  |  |  |  |

|  |
| --- |
| Унифицированная форма № Т- 5  Утверждена постановлением Государственного комитета РФ по статистике  от 06.04.01 № 26 |

|  |  |  |
| --- | --- | --- |
|  | | Код |
| Форма по ОКУД | | 0301004 |
|  | по ОКПО |  |
| наименование организации |  |  |

|  |  |  |
| --- | --- | --- |
|  | Номер документа | Дата |
| **ПРИКАЗ** |  |  |

(распоряжение)

о переводе работника на другую работу

|  |  |  |
| --- | --- | --- |
|  |  | Дата |
| Перевести на другую работу | с |  |
| по |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | | | | Табельный номер | | | |
|  | | | | |  | | | |
|  | фамилия, имя, отчество | | | |  | | | |
|  | | | | | | | | |
| вид перевода (постоянно, временно) | | | | | | | | |
| прежнее место  работы | |  | | | | | | |
|  | наименование структурного подразделения | | | | | |
|  | | | | | | |
|  | наименование профессии (должности), разряд, класс (категория) квалификации | | | | | |
|  | | | | | | |
|  | |  | причина перевода | | | | | |
|  | |  | | | | | | |
| новое место  работы | |  | наименование структурного подразделения | | | | | |
|  | наименование профессии (должности), разряд, класс (категория) квалификации | | | | | |
| оклад (тарифная ставка) | |  | | руб. |  | коп. |
|  | | надбавка | |  | | руб. |  | коп. |

**Основание**:

изменение к трудовому договору (контракту) от “ ” \_\_\_\_\_\_\_\_\_\_\_\_\_ 20 года № \_\_\_\_\_

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Руководитель организации |  | |  |  |  |  |
|  | должность | |  | подпись |  | расшифровка подписи |
|  |  | |  |  |  |  |
| **С приказом (распоряжением) ознакомлен** | |  | | |  |  |
|  | | подпись работника | | | “ ”\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20 года | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Унифицированная форма № Т- 8  Утверждена постановлением Государственного комитета РФ по статистике  от 06.04.01 № 26 | | | | | | |
|  | | | | | | | Код | |
|  | Форма по ОКУД | | | | | 0301006 | |
|  | | | | по ОКПО | |  | |
| наименование организации | | Трудовой договор (контракт) | | | номер |  | |
|  | | | | | дата |  | |

|  |  |  |  |
| --- | --- | --- | --- |
|  | | Номер документа | Дата |
| ПРИКАЗ | |  |  |
| (распоряжение)  о прекращении действия трудового договора (контракта) с работником | | | |

**Уволить “ ” \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20 года**

|  |  |  |
| --- | --- | --- |
|  | Табельный номер | |
|  |  | |
| фамилия, имя, отчество работника | |  |
|  | |  |
| наименование структурного подразделения | |  |
|  | |  |
| наименование профессии (должности), разряд, класс (категория) квалификации | |  |

|  |  |
| --- | --- |
| основание увольнения |  |

|  |  |
| --- | --- |
| Основание: |  |
|  |  |
|  |  |
|  |  |

Решение

профсоюзного органа

о согласии на увольнение

от “ ” \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20 года № \_\_\_\_\_\_\_\_

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Руководитель организации |  | |  |  | |  |  |
|  | должность | |  | подпись | |  | расшифровка подписи |
|  | |  | | |  | | | |
|  | |  | | |  | | | |
| С приказом (распоряжением) ознакомлен | |  | | | “ ” \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20 года | | | |
|  | | подпись работника | | |  | | | |

|  |
| --- |
| Унифицированная форма № Т- 11  Утверждена постановлением Государственного комитета РФ по статистике  от 06.04.01 № 26 |

|  |  |  |
| --- | --- | --- |
|  | | Код |
| Форма по ОКУД | | 0301026 |
|  | по ОКПО |  |
| наименование организации |  |  |

|  |  |  |
| --- | --- | --- |
|  | Номер документа | Дата |
| **ПРИКАЗ** |  |  |

(распоряжение)

о поощрении работника

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | |  | | | Табельный номер | | |
|  | |  | | |  | | |
|  | | фамилия, имя, отчество работника | | |  | | |
|  | | наименование профессии (должности) | | |  | | |
|  | | наименование структурного подразделения | | |  | | |
|  | |  | | |  | | |
|  | | мотив награждения | | |  | | |
|  | |  | | |  | | |
|  | |  | | |  | | |
|  | |  | | |  | | |
| вид поощрения (объявить благодарность, наградить ценным подарком или почетной грамотой, выдать премию и др.) | | | | | | | |
|  | | |  | |  | | |
|  | | |  | |  | | |
| в сумме |  | | | | | | |
| сумма прописью | | | | руб. | |  | коп. |
|  | | | |  | | | |

( \_\_\_\_\_\_\_\_\_\_\_\_\_\_ руб. \_\_\_\_ коп.)

**Основание**: представление

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Руководитель организации |  |  |  |  |  |
|  | должность |  | подпись |  | расшифровка подписи |

|  |  |  |
| --- | --- | --- |
| С приказом (распоряжением) ознакомлен |  | “ ” \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20 года |
|  | подпись работника |  |

1. Всеобщая декларация прав человека (принята на третьей сессии Генеральной Ассамблеи ООН резолюцией 217 А (III) от 10 декабря 1948 г.) [↑](#footnote-ref-1)
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.) статья 8. [↑](#footnote-ref-2)
3. Международный пакт о гражданских и политических правах (Нью-Йорк, 19 декабря 1966 г.) статья 17. [↑](#footnote-ref-3)
4. Конвенция о правах и основных свободах человека, 1995 год. [↑](#footnote-ref-4)
5. Конституция Российской Федерации от 12 декабря 1993 года. [↑](#footnote-ref-5)
6. Федеральный закон N 24-ФЗ "Об информации, информатизации и защите информации" от 20.02.1995 г. (СЗ РФ. 1995. №8. Ст. 609). [↑](#footnote-ref-6)
7. Перечень сведений конфиденциального характера (утв. Указом Президента РФ от 6 марта 1997 г. N 188). [↑](#footnote-ref-7)
8. Трудовой кодекс Российской Федерации от 30 декабря 2001 г. N 197-ФЗ (с изменениями от 24, 25 июля 2002 г., 30 июня 2003 г.). [↑](#footnote-ref-8)
9. Комментарий к Трудовому Кодексу РФ (Коршунов Ю.Н., Коршунова Т.Ю., Кучма М.И., Шеломов Б.А.) - Спарк, 2002 г.. Комментарий к статье 85 [↑](#footnote-ref-9)
10. Комментарий к Трудовому кодексу Российской Федерации (под ред. К.Н.Гусова) - ООО "ТК Велби", ООО "Издательство Проспект", 2003. Комментарий к статье 86. [↑](#footnote-ref-10)
11. «Кадровое дело», №4, апрель 2003. [↑](#footnote-ref-11)
12. Там же. [↑](#footnote-ref-12)
13. Е. Степанов. Кадровое дело. №9, 2001 год. [↑](#footnote-ref-13)
14. Кадровое дело. №9, 2003. [↑](#footnote-ref-14)
15. Постатейный Комментарий к Уголовному кодексу РФ 1996 г. (под ред. Наумова А.В.). [↑](#footnote-ref-15)
16. Комментарий к Кодексу Российской Федерации об административных правонарушениях (под ред. Ю.М.Козлова) - Юристъ, 2002. [↑](#footnote-ref-16)
17. Там же. [↑](#footnote-ref-17)
18. Кадровое дело, №4, 2003 год. [↑](#footnote-ref-18)