МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИСТОРИЧЕСКИЙ ФАКУЛЬТЕТ

Вопросы истории, международных отношений и документоведения

Выпуск 7

Сборник материалов
Российской молодежной
научной конференции

Издательство Томского университета

2011

В федеральном законе определено, что международные договоры могут иметь самые различные наименования: соглашения, конвенции, трактаты, пакты и т.д. Однако название договора либо его отсутствие принципиального юридического значения не имеют. По структуре, независимо от их наименования и классификации, договор состоит из следующих элементов: названия, преамбулы, основной и заключительной частей, подписей сторон. Основная часть договора делится на статьи и разделы, которые в ряде случаев могут иметь собственные наименования. Подписи представителей государств под двусторонним документом располагаются друг против друга или одна под другой. Заключительная часть договора содержит условия его вступления в силу и прекращения действия, указание об аутентичности текстов на языках, на которых составлен договор.

Следуя положениям закона, тексты договоров печатаются на особой договорной бумаге, прошнуровываются специальной тесьмой национальных цветов соответствующего государства и скрепляются сургучной печатью с гербовым оттиском.

В законе подчеркивается, что международные договоры могут иметь приложение в виде протоколов, правил, обменных писем и др. Согласно международной практике и федеральному закону в экземпляре договора, предназначенном для данного государства – участника договора, название этого государства, подписи его уполномоченных, а также текст договора на языке этого государства ставится на первом месте. На экземпляре другого государства все эти атрибуты ставятся соответственно на второе место. Такого рода практика называется альтернатом (чередованием).

Кроме того, дипломатическая служба руководствуется ФЗ «О техническом регулировании» от 27.12.2002. регламентирующим работу с дипломатическими документами с использованием технических средств. Согласно его положениям, все подразделения министерства и российские загранпредставительства оснащены персональными компьютерами (ПЭВМ), телекоммуникационными системами, факсимильной связью, копировальными машинами, что существенно облегчает работу с документами. Разработаны и постоянно обновляются специальные программы для ПЭВМ, которые позволяют совершенствовать учет, контроль и прохождение документов через канцелярию, классифицировать и передавать материалы на архивное хранение [6].

В целом, нормативно-правовая база дипломатической службы, разработанная структурами государственного управления РФ и включающая в себя опыт международного законодательства, помогает дипломатическим служащим правильно ориентироваться в документационных потоках, квалифицированно и грамотно оформлять документы и обеспечивать компетентное решение внешнеполитических задач.

Литература

1. *Самойленко В.В.* Дипломатическая служба. М., 2010.
2. *Венская* Конвенция о дипломатических сношениях от 18 апреля 1961 г. [Электронный ресурс]. Режим доступа: http://www.allpravo.ru, свободный.
3. *Венская* Конвенция о консульских сношениях от 24 апреля 1963 г. // Консульское право. М., 2010.
4. *Государственная* система документационного обеспечения управления. Основные положения. Общие требования к документам и службам документационного обеспечения (ГСДОУ) от 1989 г. [Электронный ресурс]. Режим доступа: http://www.nivestnik.ru, свободный.
5. *ФЗ* «О международных договорах РФ» от 16 июня 1995 г. [Электронный ресурс]. Режим доступа: http://www.allpravo.ru, свободный.
6. *ФЗ* «О техническом регулировании» от 27 декабря 2002 г. [Электронный ресурс]. Режим доступа: http://www.allpravo.ru, свободный.

А.В. Шишкова

ПРАВОВАЯ ЗАЩИТА ИНФОРМАЦИИ ПРЕДПРИЯТИЯ (ПО МАТЕРИАЛАМ ТОМСКОГО ФИЛИАЛА ОАО «ТГК-11»)

Рассматривается организация правовой защиты информации в Томском филиале ОАО «ТГК-11».

Ключевые слова: *информационная безопасность, правовой элемент системы защиты информации, организация, защита информации.*

Развитие информационных технологий, их проникновение во все сферы человеческой деятельности приводят к тому, что проблемы информационной безопасности с каждым годом становятся всё более и более актуальными – и одновременно более сложными. Технологии обработки информации непрерывно совершенствуются, а вместе с ними меняются и практические методы обеспечения информационной безопасности. Обеспечение информационной безопасности – комплексная задача, потому что сама информационная среда есть сложный и многоплановый механизм, где могут присутствовать такие компоненты, как персонал, электронное оборудование, программное обеспечение и т.д.

Необходимой составляющей является правовой аспект защиты информации, так как это основа создания комплексной системы безопасности информации. Правовой элемент системы организации защиты информации на предприятии основывается на нормах информационного права и предполагает юридическое закрепление взаимоотношений фирмы и государства по поводу правомерности использования системы защиты информации, фирмы и персонала по поводу обязанности персонала соблюдать установленные меры защитного характера, ответственности персонала за нарушение порядка защиты информации. Этот элемент включает:

– наличие в организационных документах фирмы, правилах внутреннего трудового распорядка, трудовых договорах, в должностных инструкциях положений и обязательств по защите конфиденциальной информации;

– формулирование и доведение до сведения всех сотрудников положения о правовой ответственности за разглашение конфиденциальной информации, несанкционированное уничтожение или фальсификацию документов;

– разъяснение лицам, принимаемым на работу, положения о добровольности принимаемых ими на себя ограничений, связанных с выполнением обязанностей по защите информации.

В числе основных подсистем защиты информации в правовом плане можно считать:

– установление на объекте режима конфиденциальности;

– разграничение доступа к информации;

– правовое обеспечение процесса защиты информации;

– четкое выделение конфиденциальной информации как основного объекта защиты [1].

Рассмотрим комплекс учредительных, организационных и функциональных документов на примере Томского филиала (ТФ) ОАО «ТГК-11».

Основным учредительным документом ОАО «ТГК-11» является Устав ОАО «Территориальная генерирующая компания №11», который содержит пункты, затрагивающие сферу защиты информации, например, п. 7 ст. 23, обеспечивающий доступ к информации [2. С. 23]. Исходя из анализа данного документа, необходимо отметить, что правовая защита информации Общества, как и вся деятельность предприятия, базируется на нормах действующего законодательства.

Томский филиал ОАО «ТГК-11» создан на основании приказа от 28.06.2007 г. № 359 «О филиалах ОАО «ТГК-11». Предприятие действует на основании Положения о Томском филиале Открытого акционерного общества «Территориальная генерирующая компания № 11», которое является приложением к приказу [3]. Само Положение не содержит пунктов, напрямую касающихся информационной безопасности, это еще раз подтверждает, что Общество руководствуется законодательством в сфере защиты информации.

В коллективном договоре Томского филиала требования правовой защиты информации предусматриваются пунктом 7.3.5, в соответствии с которым представитель работников обязуется не разглашать и принять меры к охране информации, отнесенной к коммерческой, служебной и иной, охраняемой законом тайне, полученной от работодателя [4. С. 16]. Данный пункт предполагает не только обязанность работника о неразглашении, но и обязанность работодателя организовать режим коммерческой тайны.

Следовательно, трудовой коллектив принимает на себя обязательства по соблюдению установленных на предприятии требований по защите конфиденциальной информации, а администрация предприятия обязуется обеспечить разработку и осуществление мероприятий по определению и защите конфиденциальной информации.

Администрация должна включить требования защиты конфиденциальной информации в правила внутреннего трудового распорядка, обязывающие работников ОАО «ТГК-11» [5]:

1) соблюдать принятые в организации правила работы с персональными компьютерами и другой оргтехникой;

2) в соответствии с законодательством Российской Федерации и локальными нормативными актами не разглашать и принимать меры к охране информации, отнесенной к коммерческой, служебной и иной охраняемой законом тайне, полученной в рамках трудовых отношений;

3) соблюдать установленные в организации требования к работе с конфиденциальными и другими служебными документами, перечень которых утверждается работодателем отдельным локальным нормативным актом.

Работникам организации запрещается использование во внеслужебных целях персональных компьютеров, ресурсов сети Интернет, программного обеспечения, оргтехники и другого оборудования организации.

Представляется, что было бы целесообразно внести в правила внутреннего трудового распорядка дополнительные пункты, которые должны конкретизировать обязанности работодателя в области защиты информации, а именно:

- обеспечить строгое сохранение конфиденциальной информации, постоянно осуществлять организаторскую и воспитательно-профилактическую работу, направленную на защиту секретов предприятия;
- включать в должностные инструкции и положения обязанности по сохранению конфиденциальной информации.

Раздел «Заключение, изменение и прекращение трудового договора с Работником»:

- администрация обязуется: нарушителей требований по защите коммерческой тайны привлекать к административной и уголовной ответственности в соответствии с действующим законодательством;
- при поступлении рабочего или служащего на работу или переводе его в установленном порядке на другую работу, связанную с конфиденциальной информацией предприятия, а также при увольнении администрация обязана проинструктировать работника или служащего по правилам сохранения коммерческой тайны с оформлением письменного обязательства о ее неразглашении;
- администрация предприятия вправе принимать решение об отстранении от работ лиц, которые нарушают установленные требования по защите конфиденциальной информации.

Организационная структура Томского филиала «ТГК-11» включает предприятия, реализация угроз безопасности на которых может повлечь крупные техногенные аварии. Поэтому в целях создания условий для безопасного функционирования организации и обеспечения безопасности работников, в организации устанавливается пропускной и внутриобъектовый режимы, особенности реализации которых определяются локальными нормативными актами. Проход работников на территорию (объект) организации осуществляется по документам, дающим на это право. Работодатель предоставляет работникам соответствующие документы (удостоверения, пропуска и т.п.) при заключении трудового договора и продлевает их действие по мере необходимости.

В соответствии с правилами внутреннего трудового распорядка работникам запрещается:

- передавать свое удостоверение или иной документ, дающий право прохода на территорию (объект) организации, другим работникам и посторонним лицам;
- проносить (провозить) на территорию (объект) организации взрывчатые, радиоактивные, биологически и химически опасные вещества без специального разрешения работодателя;
- находиться на территории (объекте) организации во внерабочее время без разрешения. Разрешение на работу во внеслужебное время выдается в установленном в организации порядке.

Обязательства конкретного сотрудника, рабочего или служащего в части защиты информации обязательно должны быть оговорены в трудовом договоре (контракте).

Так, в трудовом договоре секретаря Томского филиала прописано обязательство работника о неразглашении сведений, отнесенных локальными нормативными актами Общества к конфиденциальной информации, к коммерческой тайне Общества и персональные данные работников Общества, ставшие известными работнику в результате выполнения его трудовой функции. Пункт 2.2 включает согласие Работника на хранение, комбинирование, передачу или любое другое использование его персональных данных на получение и передачу их третьей стороне, когда это необходимо в связи с установлением, изменением, прекращением трудовых отношений и в целях трудоустройства, а также в случаях, предусмотренных ТК РФ [6. С. 1]. Работодатель, в свою очередь, обязуется ознакомить Работника по роспись с локальными нормативными актами предприятия. Таким образом, работник включается в механизм обеспечения информационной безопасности.

Подводя итог анализу правовой системы защиты информации в ОАО «ТГК-11» следует отметить, что, опираясь на государственные правовые акты и учитывая ведомственные интересы на уровне конкретного предприятия, здесь были разработаны собственные нормативно-правовые документы, включающие:

- должностные обязанности руководителей, специалистов и служащих предприятия.
- положение об организации работы по обеспечению защиты информации, составляющей коммерческую тайну;
- положение о комиссии по отнесению информации к коммерческой тайне;
- инструкцию по работе с документами, содержащими коммерческую тайну;
- перечень информации, составляющей коммерческую тайну ОАО «ТГК-11»;
- инструкцию о порядке допуска сотрудников к сведениям, составляющим конфиденциальную информацию;
- перечень сведений, разрешенных к опубликованию в открытой печати;
- обязательство сотрудника о сохранности конфиденциальной информации.

Таким образом, в Томском филиале ОАО «ТГК-11» в целом создана система локальных нормативных актов, адекватная реальным угрозам информационной безопасности данного предприятия.

Литература

1. *Правовая* защита информации [Электронный ресурс]. Режим доступа: http://itsecblog.ru/pravovaya-zashhita-informacii, свободный.
2. *Устав* открытого акционерного общества «Территориальная генерирующая компания № 11». Новосибирск, 2008.
3. *Положение* о Томском филиале Открытого акционерного общества «Территориальная генерирующая компания №11». 2007.
4. *Коллективный* договор по регулированию социально-трудовых отношений на 2010–2011 гг. между работодателем ОАО "ТГК-11" в лице генерального директора ОАО "ТГК-11" и работниками в лице Совета представителей первичных профсоюзных организаций ОАО "ТГК-11".
5. *Правила* внутреннего трудового распорядка ОАО «ТГК-11», утвержденные приказом от 27.02.2008 № 69.
6. *Трудовой* договор секретаря Томского филиала ОАО «ТГК-11». 2010.