Приложение
к постановлению МПА СНГ
от 29.11.2013 г. № 39-15

Межпарламентская Ассамблея государств – участников Содружества Независимых Государств

КОММЕНТАРИИ
к модельному закону «О коммерческой тайне»

Раздел I
ОБЩИЕ ПОЛОЖЕНИЯ

Статья 1. Сфера действия настоящего Закона

1. Настоящий Закон регулирует отношения, связанные с отнесением информации к коммерческой тайне, передачей такой информации, охраной ее конфиденциальности и предупреждением недобросовестной конкуренции, а также определяет сведения, которые не могут составлять коммерческую тайну в государствах – участниках Содружества Независимых Государств (далее – государство-участник).

2. Положения настоящего Закона распространяются на информацию, составляющую коммерческую тайну, независимо от вида носителя, на котором она зафиксирована.

3. Положения настоящего Закона не распространяются на сведения, отнесенные в установленном порядке к государственной тайне, в отношении которой применяются положения национального законодательства о государственной тайне.

Комментарий к статье 1

1. В различные эпохи правителями государств создавались специальные законы, защищавшие интересы производителей, их хозяев и государств от возможного раскрытия секретов. Так, в Древнем Риме был принят закон, предусматривавший наказание в виде штрафа (который был равен удвоенной величине причиненных убытков) за принуждение чужих рабов к выдаче тайн своего хозяина. В античном мире родилась идея вести торговые книги, тайна которых являлась разновидностью коммерческой тайны. Промышленники, торговцы и банкиры обязаны были вести названные книги, отражавшие их деятельность и материальное положение. Ведение таких книг гарантировало защиту тайны на законном основании. Данные торговых книг могли быть сообщены только для целей правосудия, по фискальным соображениям (для уточнения налогов), по делам о наследовании имущества, в случаях прекращения существования товарищества или наступления банкротства.

В мировой практике законодательного регулирования коммерчески ценной информации употреблялись различные термины, обозначавшие суть данного понятия и использовавшие ключевое слово «тайна». Под промысловой тай-

ной понимались индивидуальные особенности производства и купечески организованного предприятия, включая сведения, составлявшие промышленную, фабричную или торговую тайну. Промышленной тайной считалось привнесение чего-либо нового в процесс создания благ. Под фабричной тайной понимался не только предмет патента, который первыми ввели Англия, Франция и Германия, но и любая особенность производства (речь идет о современном понятии «ноу-хау»). Торговую тайну составляли элементы индивидуальности, например знание мест закупки товаров, списки покупателей и иное. Коммерческая тайна включала особенности коммерческой деятельности предприятия. Тайной становились любые сведения, представлявшие для собственника коммерческую ценность, в современном понимании.

В законах Российской империи имелись нормы, предусматривавшие охрану фабричного секрета, торговой тайны и тайны кредитных установлений, которые являлись средством закрепления определенного положения предприятия в ряду конкурентов, удержания благоприятного сбыта. Режим промысловой тайны основан на принципе свободы конкуренции как на соревновании сил, способностей и труда каждого конкурента, но не на использовании работы соперника, потому что в противном случае речь идет о недобросовестной конкуренции. Чтобы не допустить разглашения промысловой тайны, предусматривалось правовое воздействие предохранительного (недопущение посторонних к торговым книгам, запрещение служащим оглашать известные им тайны предприятия и иное) и восстановительного характера (применение уголовных наказаний или взыскание убытков по гражданским искам).

В правовой обиход введены различные представления о тайне. Наряду с государственной, служебной, врачебной, коммерческой и иными вводится представление об адвокатской, нотариальной тайне, тайне следствия, биржевой тайне, банковской тайне, налоговой тайне, тайне вклада и тайне договора, тайне исповеди, тайне усыновления, тайне телефонных переговоров и множестве иных видов тайн.

С учетом того что в законодательстве часто встречается слово «тайна», следует уяснить его содержание и соотношение с термином «конфиденциальная информация». Закон, употребляя термин «тайна», часто не раскрывает его содержание. В русском языке «тайна» традиционно означает «все сокрытое, неизвестное, неведомое», а также «нечто скрытно хранимое, что скрывают от кого-либо». Таким образом, «тайна» имеет два смысловых значения: нечто абсолютно неизвестное всем и нечто относительно неизвестное для какого-либо круга лиц. Очевидно, что уголовно-правовой смысл имеет только второе значение. В. Даль толковал слово «тайна» как все сокрытое, неизвестное, неведомое или нечто скрываемое, секретное, не оглашаемое. Термин «нарушение целостности и конфиденциальности» широко используется в специальной литературе, когда рассматривается проблема безопасности информационных систем, базирующихся на применении информационной техники. Под конфиденциальностью же понимается предотвращение возможности использования информации лицами, которые не имеют к ней отношения. Слово «конфиденциальный» происходит от латинского слова «confidentia (доверие)» и означает «доверитель-

ный, не подлежащий огласке». Термин «коммерческая тайна» часто отождествляют с термином «конфиденциальная информация». В то же время понятие сведений конфиденциального характера шире, чем понятие коммерческой тайны. Термин «конфиденциальная информация» является родовым по отношению к термину «коммерческая тайна».

Налаженная в правовом отношении система защиты производственной и коммерческой тайны царской России и обеспечивавшие ее законы были отменены в ноябре 1917 года в связи с принятием Советской властью декрета о рабочем контроле. Однако новая власть весьма быстро осознала, что предприятие должно иметь право на защиту информации, обладающей экономической ценностью. На первых порах защите подлежали только сведения, касающиеся разработок и производства военного характера. В 1926 году ВЦИК утвердил перечень секретов, который позволял предприятиям защищать производственную и коммерческую тайну. В СССР отношение к коммерческой тайне на государственном уровне длительное время было негативным и основывалось на представлении о ней как об инструменте капиталистических фирм, используемом для утаивания части прибыли от налогообложения и иных правонарушений.

Правовая природа коммерческой тайны такова, что последняя может существовать в различных формах. Впервые о коммерческой тайне и праве на ее защиту упоминалось в статье 33 Закона СССР «О предприятиях в СССР», а затем в статье 28 Закона РСФСР «О предприятиях и предпринимательской деятельности», статье 30 Закона Украины «О предприятиях в Украине». Вопросы защиты коммерческой тайны нашли отражение в статьях 10 и 15 Закона РСФСР «О конкуренции и ограничении монополистической деятельности на товарных рынках». В мае 1991 года были приняты Основы гражданского законодательства Союза ССР и республик, в статье 151 которых устанавливался порядок правовой охраны секретов производства, действующий в настоящее время и регулирующий защиту «ноу-хау».

В последующем, после распада СССР, правовое регулирование вопросов, связанных с коммерческой тайной, в каждой из стран бывшего Советского Союза развивалось самостоятельно. Отдельные специальные законы об охране коммерческой тайны были приняты в Молдове (1994 год), Кыргызстане (1998 год), Туркменистане (2000 год), Азербайджане (2001 год), Российской Федерации (2004 год), Таджикистане (2008 год), Беларуси (2013 год).

В формулировке целей и сферы применения Закона, обозначенных в пункте 1 статьи 1, сказано, что Закон регулирует отношения, связанные с: 1) «отнесением информации к коммерческой тайне», 2) «передачей такой информации», 3) «охраной ее конфиденциальности» и 4) «предупреждения недобросовестной конкуренции».

Коммерческая тайна, согласно статье 3, представляет собой не просто разновидность информации, а ее определенное состояние – состояние конфиденциальности. Сведения же, в отношении которых установлен режим коммерческой тайны, именуются информацией, составляющей коммерческую тайну. Поэтому, следуя данной терминологии, Закон регулирует отношения, связан-

ные не просто с отнесением информации к коммерческой тайне, а с отнесением информации к информации, составляющей коммерческую тайну.

Дефиниция понятия «передача информации, составляющей коммерческую тайну» раскрывается в статье 3 Закона. Особой разновидностью передачи данной информации является ее предоставление, определение этого понятия дается в этой же статье.

Охрана конфиденциальности заключается в установлении режима коммерческой тайны посредством превентивных мер – правовых, организационных, технических и т. д. (подробнее см. пункт 4 комментария к статье 3).

Целями правового регулирования комментируемого Закона служат:

обеспечение баланса интересов обладателей информации, составляющей коммерческую тайну, и других участников регулируемых отношений, в том числе государства, на рынке товаров, работ, услуг;

предупреждение недобросовестной конкуренции.

Отметим, что право на пресечение недобросовестной конкуренции в статье 2 Конвенции об учреждении Всемирной организации интеллектуальной собственности названо в числе других объектов права интеллектуальной собственности. А в статье 1 (пункт 2) Парижской конвенции по охране промышленной собственности – пресечение недобросовестной конкуренции рассматривается как объект охраны промышленной собственности.

Недобросовестной конкуренцией признаются любые направленные на приобретение преимуществ в предпринимательской деятельности действия хозяйствующих субъектов, которые противоречат положениям действующего законодательства, обычаям делового оборота, требованиям добропорядочности, разумности и справедливости и могут причинять или причинили убытки другим хозяйствующим субъектам-конкурентам либо нанести ущерб их деловой репутации. К действиям недобросовестной конкуренции относятся также неправомерные сбор, разглашение и использование коммерческой тайны.

Кроме того, Закон определяет сведения, которые не могут составлять коммерческую тайну (см. статью 6 и комментарий к ней).

2. Вид носителя, даже весьма специфический, на котором содержится информация, составляющая коммерческую тайну, не может служить препятствием для действия норм комментируемого Закона. Этот вывод четко следует из содержания пункта 2 статьи 1. Положения Закона распространяются на указанную информацию независимо от вида носителя, на котором она зафиксирована. Эффективность защиты коммерческой тайны предприятия зависит от установления круга носителей информации. Выделяют четыре вида носителя информации: 1) документ, 2) человек, 3) изделие (предмет, материал) и 4) процесс. Виды носителей информации, составляющей коммерческую тайну: рукописи, черновики, документы, чертежи, магнитные ленты, перфокарты, перфоленты, диски, дискеты, распечатки на принтерах, кино- и фотопленки, модели, материалы и др.

3. В соответствии с пунктом 3 статьи 1 действие норм комментируемого Закона не охватывает сведения, составляющие государственную тайну. В от-

ношении таких сведений применяются положения законодательства о государственной тайне.

Очень важно понимать разницу между коммерческой и государственной тайнами. Государственная тайна – это защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-разыскной деятельности, распространение которых может нанести ущерб безопасности государства-участника. Носители сведений, составляющих государственную тайну, – материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов.

Государственную тайну составляют следующие группы сведений:

1) в военной области:

о содержании стратегических и оперативных планов, документов боевого управления по подготовке и проведению операций, стратегическому, оперативному и мобилизационному развертыванию Вооруженных сил государства-участника, других войск, воинских формирований и органов, об их боевой и мобилизационной готовности, о создании и об использовании мобилизационных ресурсов;

о планах строительства Вооруженных сил государства-участника, о направлениях развития вооружения и военной техники, о содержании и результатах выполнения целевых программ, научно-исследовательских и опытно-конструкторских работ по созданию и модернизации образцов вооружения и военной техники;

о разработке, технологии, производстве, об объемах производства, о хранении, утилизации ядерных боеприпасов, их составных частей, делящихся ядерных материалов, используемых в ядерных боеприпасах, технических средствах и (или) методах защиты ядерных боеприпасов от несанкционированного применения, а также о ядерных энергетических и специальных физических установках оборонного значения;

о тактико-технических характеристиках и возможностях боевого применения образцов вооружения и военной техники, о свойствах, рецептурах или технологиях производства новых видов ракетного топлива или взрывчатых веществ военного назначения;

о дислокации, назначении, степени готовности, защищенности режимных и особо важных объектов, их проектировании, строительстве и эксплуатации, а также об отводе земель, недр и акваторий для этих объектов;

о дислокации, действительных наименованиях, организационной структуре, вооружении, численности войск и состоянии их боевого обеспечения, а также о военно-политической и (или) оперативной обстановке;

2) в области экономики, науки и техники:

о содержании планов подготовки государства-участника и его отдельных регионов к возможным военным действиям, о мобилизационных мощностях промышленности по изготовлению и ремонту вооружения и военной техники, об объемах производства, поставок, запасах стратегических видов сырья и ма-

териалов, а также о размещении, фактических размерах и использовании государственных материальных резервов;

об использовании инфраструктуры в целях обеспечения обороноспособности и безопасности государства;

о силах и средствах гражданской обороны, дислокации, предназначении и степени защищенности объектов административного управления, степени обеспечения безопасности населения, о функционировании транспорта и связи в государстве-участнике в целях обеспечения безопасности государства;

об объемах, планах (заданиях) государственного оборонного заказа, выпуске и поставках (в денежном или натуральном выражении) вооружения, военной техники и другой оборонной продукции, наличии и наращивании мощностей по их выпуску, связях предприятий по кооперации, разработчиках или изготовителях указанных вооружения, военной техники и другой оборонной продукции;

о достижениях науки и техники, научно-исследовательских, опытно-конструкторских, проектных работах и технологиях, имеющих важное оборонное или экономическое значение, влияющих на безопасность государства;

3) в области внешней политики и экономики:

о внешнеполитической, внешнеэкономической деятельности государства-участника, преждевременное распространение которых может нанести ущерб безопасности государства;

о финансовой политике в отношении иностранных государств (за исключением обобщенных показателей по внешней задолженности), а также о финансовой или денежно-кредитной деятельности, преждевременное распространение которых может нанести ущерб безопасности государства;

4) в области разведывательной, контрразведывательной и оперативно-разыскной деятельности:

о силах, средствах, источниках, методах, планах и результатах разведывательной, контрразведывательной и оперативно-разыскной деятельности, а также данные о финансировании этой деятельности, если такие данные раскрывают перечисленные сведения;

о лицах, сотрудничающих или сотрудничавших на конфиденциальной основе с органами, осуществляющими разведывательную, контрразведывательную и оперативно-разыскную деятельность;

об организации, силах, средствах и методах обеспечения безопасности объектов государственной охраны, а также данные о финансировании этой деятельности, если такие данные раскрывают перечисленные сведения;

о системе президентской, правительственной, шифрованной, в том числе кодированной и засекреченной, связи, шифрах, разработке, изготовлении шифров и обеспечении ими, о методах и средствах анализа шифровальных средств и средств специальной защиты, информационно-аналитических системах специального назначения;

о методах и средствах защиты секретной информации;

об организации и фактическом состоянии защиты государственной тайны;

о защите государственной границы государства-участника, исключительной экономической зоны и континентального шельфа;

о расходах государственного бюджета, связанных с обеспечением обороны, безопасности государства и правоохранительной деятельности;

о подготовке кадров, раскрывающие мероприятия, которые проводятся в целях обеспечения безопасности государства.

Принципы отнесения сведений к государственной тайне и засекречивания этих сведений определены в законодательстве государства-участника.

Не подлежат отнесению к государственной тайне и засекречиванию сведения:

о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;

о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;

о привилегиях, компенсациях и льготах, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;

о фактах нарушения прав и свобод человека и гражданина;

о размерах золотого запаса и государственных валютных резервах;

о состоянии здоровья высших должностных лиц государства-участника;

о фактах нарушения законности органами государственной власти и их должностными лицами.

Граждане вправе обжаловать в суд решения о засекречивании перечисленных сведений либо о включении их в носители сведений, составляющих государственную тайну. Должностные лица, принявшие такие решения, несут уголовную, административную или дисциплинарную ответственность в зависимости от причиненного обществу, государству и гражданам материального и морального ущерба.

Статья 2. Законодательство об охране коммерческой тайны

Законодательство об охране прав на коммерческую тайну в государстве-участнике базируется на национальном законодательстве и учитывает положения настоящего Закона.

Отношения, связанные с охраной коммерческой тайны, регулируются настоящим Законом, гражданским кодексом, законодательством об интеллектуальной собственности, международными договорами, обязательными для государства-участника, другими актами законодательства, изданными на основании законов или постановлений правительства государства-участника.

Комментарий к статье 2

В правовой доктрине институт коммерческой тайны рассматривается, во-первых, как самостоятельный институт гражданского и коммерческого права, в котором доминирующее место занимают гражданско-правовые нормы, регулирующие гражданский (торговый) оборот коммерческой тайны и охрану ее кон-

фиденциальности. Во-вторых, данный институт включает другие нормы, регулирующие отношения по поводу использования и охраны конфиденциальности коммерческой тайны внутри организации (корпоративное и трудовое право), взаимоотношения с органами власти по поводу предоставления коммерческой тайны (административное право) и защищающие интересы обладателя коммерческой тайны в судебном порядке.

В цивилистической науке вопрос о самостоятельности правового института коммерческой тайны носит дискуссионный характер. Следует отметить наличие двух взаимоисключающих подходов при отнесении информации, составляющей коммерческую тайну, к объектам исключительных прав. Первый подход, сторонником которого является В. А. Дозорцев, исходит из отнесения прав на информацию к системе исключительных прав.

Второй подход, которого придерживаются И. А. Зенин, В. А. Северин, предполагает, что в отличие от охраняемого патентом изобретения, на ноу-хау не существует исключительного права, а есть лишь фактическая монополия. Фактическая монополия организации на такую информацию возможна при соблюдении определенной процедуры, связанной с установлением режима коммерческой тайны. Подобную позицию занимает и Э. П. Гаврилов, который считает, что коммерческая тайна не может быть объектом исключительных прав.

Несколько иную, компромиссную позицию занимает А. П. Сергеев, считая коммерческую тайну самостоятельным объектом интеллектуальной собственности (интеллектуальные права) (на этой же позиции стоит В. А. Дозорцев) и вместе с тем допуская монополию лица на такого рода информацию после принятия им превентивных мер охраны (по существу, разделяя позицию И. А. Зенина).

В последние годы в государствах-участниках было принято значительное число нормативных правовых актов, посвященных вопросам регулирования «информационных» отношений в обществе и затрагивающих данные отношения отдельными нормами.

Совокупность юридических норм, регулирующих «информационные» отношения, образует сравнительно новую и активно развивающуюся отрасль законодательства – «информационное право». В составе информационного права можно условно выделить некоторые законодательные ветви, относящиеся к вопросам, связанным с информацией: законодательство об информационной безопасности; законодательство о конфиденциальной информации; законодательство об информационных ресурсах, которое в свою очередь можно разделить на законодательство о правовой информации, законодательство о международном обмене информацией, законодательство о связи, законодательство о персональных данных, законодательство об архивном фонде и архивах, законодательство о библиотечном деле, законодательство о статистической информации; законодательство о государственной тайне; законодательство о средствах массовой информации.

Нормы об информации, относящейся к коммерческой тайне, содержатся также в законодательстве об интеллектуальной собственности (исключительных правах). Оно включает в себя: законодательство об авторском праве и

смежных правах; патентное законодательство; законодательство о средствах индивидуализации (товарных знаках, знаках обслуживания и наименованиях мест происхождения товаров; фирменных наименованиях); законодательство об открытиях.

Помимо комментируемого Закона коммерческой тайне посвящены положения Гражданского кодекса и других законов государств-участников.

В законодательство о коммерческой тайне входят также положения законодательства о конкуренции. Согласно закону недобросовестная конкуренция – это любые направленные на приобретение преимуществ в предпринимательской деятельности действия хозяйствующих субъектов, которые противоречат положениям действующего законодательства, обычаям делового оборота, требованиям добропорядочности, разумности и справедливости и могут причинить или причинили убытки другим хозяйствующим субъектам-конкурентам либо нанести ущерб их деловой репутации. Зафиксированные в этом определении требования добропорядочности, разумности и справедливости корреспондируют с общими нормами гражданского законодательства – презумпцией разумности и добросовестности участников гражданских правоотношений. Указанные категории носят оценочный характер, что расширяет доказательственную базу в сфере пресечения недобросовестной конкуренции. Использование таких критериев для оценки добросовестности конкуренции связано с принципом «доброй совести», который ведет свое происхождение от римской формулы «bona fides». Получение, использование, разглашение информации, составляющей коммерческую, служебную тайну и охраняемую законом тайну, является актом недобросовестной конкуренции.

Неотъемлемой частью законодательства о коммерческой тайне, безусловно, являются и нормы трудового законодательства. О соблюдении режима коммерческой тайны в процессе трудовых правоотношений между работником и работодателем см. статью 13 Закона и комментарий к ней.

Коммерческая тайна тесно связана с различными видами профессиональной и служебной тайн. Так, налоговая тайна не подлежит разглашению налоговыми органами, органами внутренних дел, органами государственных внебюджетных фондов и таможенными органами, их должностными лицами и привлекаемыми специалистами, экспертами, за исключением случаев, предусмотренных законом.

Налоговую тайну составляют любые полученные налоговым органом, органом внутренних дел, органом государственного внебюджетного фонда и таможенным органом сведения о налогоплательщике, за исключением следующих сведений: 1) разглашенных налогоплательщиком самостоятельно или с его согласия; 2) об идентификационном номере налогоплательщика; 3) о нарушениях законодательства о налогах и сборах и мерах ответственности за эти нарушения; 4) предоставляемых налоговым (таможенным) или правоохранительным органам других государств в соответствии с международными договорами (соглашениями), одной из сторон которых является государство-участник, о взаимном сотрудничестве между налоговыми (таможенными) или правоохранительными органами (в части сведений, предоставленных этим органам).

Таким образом, информация, составляющая коммерческую тайну налогоплательщика, которую налогоплательщик предоставил налоговым и иным указанным выше органам на основании законодательства, также не подлежит разглашению этими органами и составляет их служебную тайну. Сведения, составляющие налоговую тайну, имеют специальный режим хранения и доступа и могут разглашаться только в случаях, прямо указанных в законе.

К разглашению налоговой тайны относится, в частности, использование или передача другому лицу производственной или коммерческой тайны налогоплательщика, ставшей известной должностному лицу налогового органа, органа внутренних дел, органа государственного внебюджетного фонда или таможенного органа, привлеченному специалисту или эксперту при исполнении ими своих обязанностей.

Таможенные органы, их должностные лица, получившие доступ к информации, не вправе разглашать, использовать в личных целях либо передавать третьим лицам, в том числе государственным органам, информацию, составляющую государственную, коммерческую, банковскую, налоговую или иную охраняемую законом тайну, и другую конфиденциальную информацию, за исключением случаев, установленных законами государства-участника.

При проведении аудиторской проверки аудиторские организации и индивидуальные аудиторы обязаны в том числе обеспечивать сохранность документов, получаемых и составляемых в ходе аудиторской проверки, не разглашать их содержание без согласия аудируемого лица и (или) лица, заключившего договор оказания аудиторских услуг, за исключением случаев, предусмотренных законодательством.

Сведения, составляющие банковскую тайну, могут быть предоставлены только самим клиентам или их представителям. Государственным органам и их должностным лицам такие сведения могут быть предоставлены исключительно в случаях и порядке, предусмотренных законом. В случае разглашения банком сведений, составляющих банковскую тайну, клиент, права которого нарушены, вправе потребовать от банка возмещения причиненных убытков.

В соответствии с законом об адвокатской деятельности и адвокатуре адвокатской тайной являются любые сведения, связанные с оказанием адвокатом юридической помощи своему доверителю. К числу таких сведений нужно относить и информацию, составляющую коммерческую тайну доверителя, ставшую известной адвокату в процессе оказания доверителю юридической помощи.

Журналистская тайна предусмотрена нормами законодательства о средствах массовой информации. Согласно положениям данного закона редакция не вправе разглашать в распространяемых сообщениях и материалах сведения, предоставленные гражданином с условием сохранения в тайне. Редакция обязана сохранять в тайне источник информации и не вправе называть лицо, предоставившее сведения с условием неразглашения его имени, за исключением случая, когда соответствующее требование поступило от суда в связи с находящимся в его производстве делом.

Принципиальное отличие между коммерческой тайной и перечисленными выше видами тайн состоит в том, что коммерческая тайна – одна из «первичных» (естественных) тайн, которые непосредственно связаны с видом персонифицированного субъекта (наряду с личной тайной физического лица и государственной тайной органа государственной власти). Профессиональные тайны, которые составляет информация, передаваемая субъекту профессиональной деятельности в режиме личной тайны (врачебная тайна, тайна исповеди, тайна банковских вкладов, налоговая и другие тайны) либо коммерческой тайны (налоговая, банковская, нотариальная и другие тайны), являются тайнами «производными». И если в отношении «первичных» тайн у обладателя информации есть права на установление режима ограничения доступа (о чем будет подробно рассказано далее), то в отношении «производных» тайн возникает обязанность устанавливать соответствующий режим лицом, которому доверена такая информация.

Сведения могут менять свой статус, не меняя фактического содержания. Например, коммерческая тайна становится служебной либо банковской тайной, секретом производства (ноу-хау), а в некоторых случаях – государственной тайной. Критерием отнесения информации к различным тайнам (служебной или коммерческой) в таких случаях является различие субъектов, в собственность (распоряжение) которых поступили сведения.

Первым документом, имеющим международный статус и предусматривающим регулирование секретов производства, исследователи признают Соглашение о торговых аспектах прав интеллектуальной собственности (ТРИПС), хотя оно говорит о закрытой информации (undisclosed information).

В соответствии со статьей 39 Соглашения ТРИПС охрана закрытой информации предоставляется в контексте обеспечения эффективной защиты от недобросовестной конкуренции в понимании статьи 10-бис Парижской конвенции по охране промышленной собственности (1967 года). Физическим и юридическим лицам предоставляется возможность препятствовать тому, чтобы информация, правомерно находящаяся под их контролем, без их согласия была раскрыта, получена или использована другими лицами способом, противоречащим честной коммерческой практике, при условии, что такая информация: (а) является секретной в том смысле, что она в целом или в определенной конфигурации и подборе ее компонентов не является общеизвестной и легкодоступной лицам в тех кругах, которые обычно имеют дело с подобной информацией, (б) в силу своей секретности имеет коммерческую ценность и (в) является объектом надлежащих при данных обстоятельствах мер, направленных на сохранение ее секретности, со стороны лица, правомерно контролирующего эту информацию. В понятие способа, противоречащего честной коммерческой практике, Соглашение ТРИПС вкладывает нарушение условий контракта, доверия, побуждение к нарушению; приобретение закрытой информации третьими лицами, которые знали или допустили грубую неосторожность, не узнав, что действия, которые противоречат честной торговой практике, были допущены в процессе такого приобретения. Соглашение ТРИПС также регламентирует обязательства полномочных органов государств-участников ВТО по сохранению

коммерческой тайны, раскрытой им субъектами, которые выходят на рынок этих государств.

В Соглашении ТРИПС было закреплено три известных критерия режима коммерческой тайны: 1) секретность, 2) коммерческая ценность и 3) принятие адекватных мер для обеспечения секретности. Важность подхода к толкованию закрытой информации Соглашением ТРИПС вытекает из того, что статьями 41–47 Соглашения на страны-участницы возлагается обязанность создания национальных систем для внедрения признанных Соглашением прав интеллектуальной собственности. При этом страны должны обеспечить справедливые и равные процедуры для владельцев прав интеллектуальной собственности и такие средства защиты, как судебные запреты и компенсация ущерба. Важным также является распространение на отношения по охране закрытой информации или коммерческой тайны международной системы разрешения споров ВТО. Таким образом, статья 39 Соглашения ТРИПС установила минимальные стандарты, которым должно соответствовать законодательство стран – членов ВТО. Формулировки статьи оставляют место для определения конкретных схем, соответствующих правовым системам стран, но обязательным является включение упомянутых трех необходимых элементов и системы законного принуждения для реализации соответствующих положений.

Статья 3. Определение понятий

В настоящем Законе приведенные ниже понятия употребляются в следующем значении:

***доступ к коммерческой тайне* – ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации;**

***коммерческая тайна* – информация, являющаяся секретной в том понимании, что она в целом или в определенной форме и совокупности ее составляющих неизвестна и не легкодоступна для лиц, обычно имеющих дело с видом информации, к которому она принадлежит, в связи с этим имеет действительную или потенциальную коммерческую ценность и была предметом адекватных существующим обстоятельствам мер в отношении сохранения ее секретности, принятых лицом, которое законно контролирует эту информацию;**

Коммерческой тайной могут быть сведения научно-технического, технологического, организационного, коммерческого, производственного и иного характера (в том числе составляющие секреты производства (ноу-хау)), за исключением тех, которые в соответствии с законом не могут быть отнесены к коммерческой тайне;

***контрагент* – сторона гражданско-правового договора, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию;**

***ноу-хау* – охраняемые в режиме коммерческой тайны результаты интеллектуальной деятельности, которые могут быть переданы иному лицу и использованы им на законных основаниях, в том числе:**

– неопубликованные научно-технические результаты, технические решения, методы, способы использования технологических процессов и устройств, которые не обеспечены патентной защитой в соответствии с законодательством или по решению лица, которое владеет такой информацией на законном основании;

– знания и опыт в области реализации продукции и услуг, сведения о конъюнктуре рынка, результаты маркетинговых исследований;

– коммерческие, методические или организационно-управленческие идеи и решения;

***обладатель коммерческой тайны* – физическое или юридическое лицо, занимающееся предпринимательской деятельностью, правомерно владеющее информацией, имеющей действительную или потенциальную коммерческую ценность, ограничивающее доступ к этой информации на законном основании и принимающее меры к охране ее конфиденциальности;**

***передача коммерческой тайны* – передача обладателем коммерческой тайны зафиксированной на материальном носителе информации, составляющей эту коммерческую тайну, контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности;**

***предоставление коммерческой тайны* – передача обладателем коммерческой тайны зафиксированной на материальных носителях информации, составляющей эту коммерческую тайну, органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций;**

***промышленный шпионаж* – противоправные действия по сбору, присвоению и передаче сведений, составляющих коммерческую тайну, наносящие или могущие нанести ущерб ее владельцу;**

***разглашение коммерческой тайны* – деяние (действие или бездействие), в результате которого коммерческая тайна в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной (раскрытой) третьим лицам без согласия ее обладателя, а также вопреки трудовому или гражданско-правовому договору;**

***режим коммерческой тайны* – система правовых, организационных, технических и иных мер, принимаемых к охране конфиденциальности информации обладателем коммерческой тайны, а также лицами, правомерно ее получившими.**

Комментарий к статье 3

1. Определения основных понятий даны в статье 3 для целей комментируемого Закона. Это означает, что их формулировки могут не совпадать по содержанию с формулировками аналогичных терминов, которые содержатся в иных нормативных правовых актах.

Формулировка «для целей настоящего Закона» является стандартом в законодательной технике и широко используется, поскольку у каждого закона своя сфера применения. Кроме того, законодательство развивается, пытаясь соответствовать общественным отношениям, т. е. нормотворчество полностью подчинено текущим потребностям общества. Поэтому пересмотр и уточнение терминологии – естественный процесс.

2. Коммерческая тайна, как уже отмечалось выше, представляет собой не разновидность информации, а ее определенное состояние – конфиденциальность, которая позволяет обладателю информации при существующих или возможных обстоятельствах: увеличить доходы; избежать неоправданных расходов; сохранить положение на рынке товаров, работ, услуг; получить иную коммерческую выгоду.

Поскольку коммерческая тайна относится к «первичным» тайнам, необходимость защиты информации в режиме коммерческой тайны – это не обязанность, а право лица, ее создавшего.

3. Комментарий термина «информация, составляющая коммерческую тайну» необходимо начать с изучения понятия «информация», лежащего в его основе. Информация представляет собой разнообразные сведения в широком смысле слова. Это могут быть сведения о лицах, предметах, фактах, событиях, явлениях, процессах. Основной особенностью информации как правовой категории является то, что образующие ее сведения независимы от формы их представления. По общему правилу правовой статус информации не зависит от правового статуса объектов собственности (вещных прав), а также интеллектуальной собственности (исключительных прав), в которых она может содержаться, за исключением случаев, прямо указанных в законодательстве.

Согласно нормативным правовым актам «массовая информация» - это предназначенные для неопределенного круга лиц печатные, аудио-, аудиовизуальные и иные сообщения и материалы. Если считать, что в формулировке «предназначенные для неопределенного круга лиц» проявляется видовое отличие понятия «массовая информация» от более широкого понятия «информация», то сама информация – это печатные, аудио-, аудиовизуальные, иные сообщения и материалы. Таким образом, один закон понимает под информацией сведения, другой – сообщения и материалы.

Попытки соотнести эти понятия между собой, предпринятые юристами-цивилистами и исследователями из других областей знания, привели к получению различных результатов. По мнению первых, «сведения» составляют содержание «сообщений». Лингвисты же полагают, что эти понятия синонимичны, ибо определяются друг через друга.

Говоря о синонимичности понятий «сведения» и «сообщения», нельзя забывать о том, что термин «сообщения» используется законодателем неотрывно от термина «материалы».

Вернемся к изучению понятия «информация, составляющая коммерческую тайну». Такой информацией согласно комментируемой статье Закона является научно-техническая, технологическая, организационная, производственная или иная информация (в том числе составляющая секреты производства (ноу-хау)).

Из данной дефиниции Закона видно, что перечень содержащихся в ней видов информации, составляющей коммерческую тайну, не закрыт, так как он заканчивается словами «или иная информация».

Представляет интерес понятие «ноу-хау», используемое в комментируемом определении. Термин «ноу-хау» впервые был применен в США в 1916 г. в судебном деле Дюранда против Брауна. Он нашел применение в правовой литературе большинства зарубежных стран. Дословный перевод термина означает «знать, как» (сокращение от «знать, как делать»). Под ноу-хау традиционно понимается некая информация, составляющая секрет производства. Однако как на законодательном уровне, так и в юридической литературе не сложилось единого подхода к конкретизации данного понятия, четкому определению его содержания. Кроме того, в научном сообществе до сих пор не достигнут компромисс и по поводу того, объектом каких прав является ноу-хау. Одни специалисты полагают, что ноу-хау – объект исключительных прав, т. е. является интеллектуальной собственностью. Другие употребляют в отношении ноу-хау термин «квазиправо», сходный по содержанию с исключительными правами, но не являющийся таковым. Третья группа цивилистов считают, что в отношении ноу-хау (как и в отношении иных видов информации, составляющей коммерческую тайну) действует лишь фактическая монополия его владельца, выражающаяся в возможности устанавливать режим доступа к сведениям, составляющим ноу-хау, принимать в отношении них превентивные меры.

Ноу-хау можно условно разделить на три большие группы:

1) информация о сущности незапатентованного изобретения, полезной модели или промышленного образца;

2) сведения о методах, процессах, технологиях, профессиональном опыте и иных объектах, имеющих коммерческую ценность, но лишенных способности охраняться патентом;

3) добавочная информация, получаемая при использовании запатентованных технологий, которая, не будучи патентоспособной сама по себе, позволяет более эффективно использовать запатентованные устройство или способ.

Первая группа сведений приобретает конфиденциальный характер с момента подачи документов в орган исполнительной власти по интеллектуальной собственности. Момент соответствующей государственной регистрации и официального опубликования этих сведений определяет изменение их правового режима – они переходят из разряда конфиденциальной информации в разряд объектов интеллектуальной собственности.

Сведения о патентоспособных объектах (до их официальной публикации) можно считать разновидностью как конфиденциальной информации в широком смысле, так и информации, составляющей коммерческую тайну (ноу-хау), в частности, но только при соответствии трем ее признакам, включая необходимость принятия обладателем этой информации превентивных мер, направленных на обеспечение ее конфиденциальности.

Соотношение коммерческой тайны и ноу-хау можно рассматривать как соотношение общего и частного. Информация, содержащая в себе ноу-хау, должна обязательно включаться в состав коммерческой тайны как наиболее ценная и значимая, утрата которой может обернуться потерей устойчивых прибылей и привести предприятие к банкротству. Термин «ноу-хау» широко распространен в международных правовых актах (упоминается более чем в 180 международных соглашениях), законодательстве развитых государств. Коммерческая тайна и ноу-хау одновременно являются и правовым режимом охраны, и объектом, подлежащим защите. Коммерческая тайна и ноу-хау – это прежде всего информация, наделенная определенными признаками, позволяющими идентифицировать их в качестве названных объектов. В то же время режимы защиты данного вида информации – это комплекс организационных и правовых норм, с помощью которых достигается возможность защиты ценной информации от разглашения и возможность защиты интересов ее обладателей от несанкционированного разглашения. Если владелец коммерческой тайны сохраняет ее для себя, для собственного пользования, то ноу-хау является объектом передачи и соответствующих сделок.

Вернемся к дефиниции «информация, составляющая коммерческую тайну». Законодатель устанавливает три признака данной информации:

1) она имеет действительную или потенциальную коммерческую ценность в силу неизвестности третьим лицам;

2) к ней нет доступа на законном основании;

3) ее обладателем введен режим коммерческой тайны.

Данная норма Закона практически полностью дублирует соответствующее положение модельного Кодекса интеллектуальной собственности. Рассмотрим указанные три критерия. Итак, во-первых, информация, составляющая коммерческую тайну, должна иметь коммерческую ценность. Как отмечается в литературе, ценность информации – комплексный показатель ее качества, мера пригодности для принятия решений в конкретной сфере. Отсюда коммерческая ценность информации – это показатель ее пригодности (полезности) для принятия решений в коммерческой деятельности. Данный показатель, с учетом сложившейся деловой практики, имеет три составляющие: 1) достоверность информации; 2) ее актуальность; 3) полнота информации.

Коммерческая ценность поставлена законодателем в зависимость от неизвестности информации третьим лицам – субъектам, не являющимся сторонами связанных с ней отношений. Отсюда берет начало второй неотъемлемый признак информации, составляющей коммерческую тайну, – ее недоступность на законном основании. Предполагается, что третьи лица могут получить указанную информацию только незаконным путем либо в результате небрежности

ее обладателя. Однако многие разновидности ресурсов ограниченного доступа, такие как, например, клиентские базы, юридически не защищены от «независимых открытий».

Последний признак информации, составляющей коммерческую тайну, – принятие превентивных мер, препятствующих общему доступу к ней, иными словами – введение режима коммерческой тайны. Само по себе установление договорных обязательств и других превентивных мер, препятствующих общей доступности к информации, еще не говорит о том, что информация составляет коммерческую тайну. Введение режима коммерческой тайны – замыкающий критерий правовых основ обеспечения интересов ее обладателя, не имеющий юридической силы вне связи с двумя другими рассмотренными критериями.

Современные международные стандарты в области коммерческой тайны установлены Парижской конвенцией по охране промышленной собственности и Соглашением о торговых аспектах прав интеллектуальной собственности (ТРИПС). Согласно пункту 1 статьи 39 Соглашения ТРИПС в процессе обеспечения эффективной защиты от недобросовестной конкуренции, как это предусмотрено в статье 10-бис Парижской конвенции (1967 года), страны-члены охраняют закрытую информацию. На основании пункта 2 статьи 39 Соглашения ТРИПС лицо может препятствовать раскрытию, получению или использованию правомерно находящейся под его контролем информации способом, противоречащим честной коммерческой практике, при условии, что такая информация:

является секретной в том смысле, что она в целом или в определенной конфигурации и подборе ее компонентов не относится к общеизвестной или легкодоступной лицам в тех кругах, которые обычно имеют дело с подобной информацией;

ввиду своей секретности имеет коммерческую ценность;

является объектом надлежащих в данных обстоятельствах действий, направленных на сохранение ее секретности, со стороны лица, правомерно контролирующего эту информацию.

Данное в статье 3 модельного Закона определение коммерческой тайны полностью корреспондируется с международными нормами (статьи 39 Соглашения ТРИПС). Такой подход принят также в законах «О коммерческой тайне» Кыргызстана (статьи 1, 2), Молдовы (статьи 1, 2), Азербайджана (статьи 2, 3), Таджикистана (статьи 3), Туркменистана (статьи 4).

Так, согласно статье 4 Закона Туркменистана от 19 декабря 2000 года № 53-II «О коммерческой тайне» информация, составляющая коммерческую тайну, должна соответствовать следующим требованиям: иметь действительную или потенциальную ценность для ее обладателей в силу неизвестности ее третьему лицу (лицам); не являться общеизвестной или общедоступной согласно законодательству Туркменистана; обеспечиваться соответствующими мерами защиты ее конфиденциальности, включая разработку внутренних правил ограничения пользования, введения соответствующей маркировки документов и иных носителей информации, организации учета, хранения и применения.

Гражданский кодекс Республики Казахстан в статье 126 гарантирует защиту информации, составляющей служебную или коммерческую тайну, в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности.

Еще одним немаловажным моментом является соотношение понятий «информация, составляющая коммерческую тайну» и «конфиденциальная информация».

«Конфиденциальность» появляется в нормативных правовых актах СССР после 1990 года и присутствует только в трех документах. В настоящее время этот термин встречается в 84 национальных законах и 706 международных (в том числе межправительственных) соглашениях.

Исходя из анализа норм законодательных актов, образующих отрасль информационного права, очевидно, что «информация, составляющая коммерческую тайну» не является синонимом «конфиденциальной информации» (хотя в определенных случаях она условно может быть использована в качестве такового), но является ее особой разновидностью.

К конфиденциальной информации, в свою очередь, относится не только информация, составляющая коммерческую тайну, но и следующие виды сведений: сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных национальными законами случаях; сведения, составляющие тайну следствия и судопроизводства; сведения, доступ к которым ограничен органами государственной власти в соответствии с законами (служебная тайна); сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т. д.); сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Нередко перечисленные категории смешиваются. Например, известны попытки отнесения к информации, составляющей коммерческую тайну, некоторых видов персональных данных. Последние представляют собой сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность. Не допускаются сбор, хранение, использование и распространение информации о частной жизни, а равно информации, нарушающей личную тайну, семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений физического лица без его согласия, кроме как на основании судебного решения. В литературе предложено более емкое определение этой категории: «сведения о личности, которые включаются в информационную систему государственных, общественных и частных, корпоративных организаций по инициативе индивида или в силу закона в целях реализации его прав и обязанностей в процессе участия в самых разных

социальных процессах и отношениях. Это та часть частной жизни, которая определенным образом представлена и присутствует в публичном и гражданском секторах правовых отношений индивида с другими субъектами права».

Определению правового статуса персональных данных на международном уровне, в частности, посвящены:

Директива 95/46/ЕС о защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных;

Директива 97/66/ЕС об обработке персональных данных и защите конфиденциальности в телекоммуникационном секторе.

Порядок получения и использования персональных данных в процессе трудовых отношений регламентируется нормами трудового кодекса. Персональные данные работника определяются как информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника; получение, хранение, комбинирование, передача или любое другое использование персональных данных работника сведено к общему понятию «обработка персональных данных работника».

Безусловно, незаконное получение и использование персональных данных индивидуального предпринимателя или сотрудников руководящего звена фирмы может нанести ущерб их бизнесу. Сведения о частной жизни рядовых сотрудников в руках шантажистов могут служить инструментом для получения более ценной информации о «судьбах предприятия». Однако правовые режимы информации, составляющей коммерческую тайну, и персональных данных различны по содержанию. Охрана последних обеспечивается в основном за счет норм о неприкосновенности частной жизни.

4. Режим коммерческой тайны – это меры по охране конфиденциальности информации, составляющей коммерческую тайну.

Данные меры принято делить на правовые, организационные и технические, которые тесно взаимосвязаны между собой. Более того, большинство превентивных мер изначально включают в себя и правовую, и организационную, и техническую составляющие. Например, чтобы воплотить в жизнь какое-либо техническое решение в области безопасности на предприятии (например, внедрить систему шифрования в корпоративную информационную сеть), необходимо сначала найти ему юридическое обоснование, собрать необходимые разрешения на проведение соответствующих работ (если они требуют лицензирования или прохождения иных процедур, предусмотренных законодательством), продумать возможные последствия такого внедрения (например, возможность нарушения конституционных и иных прав сотрудников). Затем нужно разработать ряд внутрифирменных инструкций (положений, приказов) и провести полномасштабное обучение персонала компании. Другими словами, во исполнение одной технической меры нередко необходимо принять множество мер юридического и организационного характера. Точно так же во исполнение одной меры безопасности организационного плана, например усиления режима доступа на объект или организации системы фиксирования посещений этого объекта, необходимо внедрить различные технические (электронные) устройства, и это должно быть сделано грамотно не только технически, но и юридически.

Каждая из перечисленных мер сама по себе достаточно емкая и может включать в себя множество более простых по содержанию мер, за счет которых она и реализуется. Однако такие категории как, например, «работа с людьми» и тем более «защита от промышленного шпионажа», вообще некорректно именовать мерами, поскольку одна такая «мера» может включать в себя абсолютно все охранные мероприятия, проводимые в организации (и не только в отношении доступа к информации, составляющей коммерческую тайну).

Технические меры охраны конфиденциальности информации с течением времени приобретают все большее значение. Большинство предприятий, организаций и учреждений имеют доступ к Интернету, который, являясь открытой информационной средой, предоставляет широкие возможности для различных злоумышленных действий в отношении информации и объектов интеллектуальной собственности, таких, например, как интернет-сайты и программное обеспечение.

Из комментируемой дефиниции Закона следует, что обладателем информации, составляющей коммерческую тайну, могут приниматься не только правовые, организационные и технические, но и «иные меры» для обеспечения конфиденциальности данной информации.

Отметим, что превентивные меры, принимаемые обладателем информации, составляющей коммерческую тайну, в целях обеспечения ее конфиденциальности, должны быть адекватны ценности указанной информации. Обладатель информации должен не только осознавать риск утери своей монополии в отношении нее, но и прогнозировать, какие меры (средства) могут быть использованы третьими лицами для получения доступа к ней.

В некоторых случаях обязанность обладателя информации принимать в отношении нее превентивные меры установлена законодательством. Так, если иное не предусмотрено договорами на выполнение научно-исследовательских, опытно-конструкторских и технологических работ, стороны обязаны обеспечить конфиденциальность сведений, касающихся предмета договора, хода его исполнения и полученных результатов. Наряду с этим объем сведений, признаваемых конфиденциальными, определяется в договоре, и каждая из сторон обязуется публиковать полученные при выполнении работы сведения, признанные конфиденциальными, с согласия контрагента. Таким образом, стороны договоров на выполнение НИОКР полностью свободны в определении объема конфиденциальных сведений, в любой момент могут сделать их общедоступными по обоюдному согласию и, кроме того, учитывая диспозитивный характер нормы, могут установить в договоре «иное», т. е. заведомо придать описаниям и результатам НИОКР статус неконфиденциальной информации.

Следует отметить, что выбор превентивных мер, необходимых для обеспечения конфиденциальности соответствующих ресурсов информации, составляющей коммерческую тайну, и объединение их в четко работающую систему мер информационной безопасности организации – процесс интеллектуальный и достаточно трудоемкий. Одни хозяйствующие субъекты для этого заказывают проведение дорогостоящих исследований, осуществляют подбор соответствующих кадров, которые смогли бы оценить текущее состояние информационной

безопасности предприятия и создать надежную систему контроля за использованием коммерчески значимой информации и доступом к ней. Другие субъекты рынка идут более «дешевым» (с их точки зрения) путем, снабжая грифами конфиденциальности все документы и носители информации без разбора («для верности»). Однако перебор в использовании превентивных мер, препятствующих общей доступности к информации, равно как и ее утечка, может привести к неблагоприятным последствиям, как то: излишняя формализация отношений, отрицательно сказывающаяся на производительности труда; недовольство и увольнение ценных кадров и, как следствие, вероятность еще большей утечки конфиденциальной информации; споры с антимонопольными органами, судебные тяжбы и издержки.

5. Обладателем информации, составляющей коммерческую тайну, является лицо, которое: владеет информацией, составляющей коммерческую тайну, на законном основании; ограничило доступ к этой информации; установило в отношении этой информации режим коммерческой тайны.

Второй и третий признаки обладателя информации, составляющей коммерческую тайну, представляются идентичными по своему содержанию, поскольку ограничение доступа к указанной информации – неотъемлемая (а нередко и единственная) составляющая режима коммерческой тайны.

6. Под «доступом к информации, составляющей коммерческую тайну» понимается ознакомление определенных лиц с этой информацией, осуществляемое на законном основании (в том числе с согласия ее обладателя) и при условии сохранения конфиденциальности этой информации. Норма не называет способы и средства для предоставления доступа. Поэтому доступ к информации, составляющей коммерческую тайну, может предоставляться любыми способами и с помощью любых средств по согласованию между обладателем информации и лицом, которому предоставляется доступ.

7. Под «передачей информации, составляющей коммерческую тайну» Закон понимает передачу указанной информации ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности. При этом передаваемая таким образом информация, составляющая коммерческую тайну, должна быть обязательно зафиксирована на материальном носителе. Передача информации в устной форме не является «передачей информации, составляющей коммерческую тайну» по смыслу комментируемого Закона.

8. Под «контрагентом» в комментируемом Законе понимается сторона гражданско-правового договора, которая получила информацию, составляющую коммерческую тайну, от ее обладателя.

Лицо, состоящее с обладателем информации, составляющей коммерческую тайну, в трудовых отношениях, использующее данную информацию в процессе выполнения своих трудовых функций и принявшее на себя обязательства по сохранению ее конфиденциальности, не является контрагентом в смысле положений комментируемого Закона.

9. Закон предусматривает дефиницию, сходную с уже рассмотренной выше «передачей информации, составляющей коммерческую тайну» – «предоставление информации, составляющей коммерческую тайну». Два указанных понятия практически аналогичны по содержанию, за исключением субъективного состава. Если «передача информации...» осуществляется между обладателем информации и его контрагентом, то субъектами, получающими доступ к информации, составляющей коммерческую тайну, в результате «предоставления...», являются органы государственной власти, иные государственные органы, органы местного самоуправления.

Предоставление информации осуществляется исключительно в целях выполнения функций указанных органов. О порядке предоставления информации, составляющей коммерческую тайну, см. статью 15 и комментарий к ней.

10. Разглашение информации, составляющей коммерческую тайну, – это действие или бездействие, в результате которого информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

Наряду с разглашением в законодательстве и литературе встречаются и другие понятия, связанные с несанкционированным получением информации третьими лицами и влекущие за собой полную или частичную (в том числе временную) потерю субъектом фактической монополии в отношении своей конфиденциальной информации. Среди них можно назвать следующие:

«утечка информации» – процесс, в результате которого информация стала известной определенному лицу (кругу лиц), несмотря на наличие охранных мер, принятых законным владельцем информации (может произойти как в результате активных действий, например хищения или разглашения информации, так и в результате оплошности ее владельца или недостаточности принятых им превентивных мер);

«хищение информации» – нарушение режима доступа к информации посредством активных противоправных действий, направленных на получение данной информации;

«утрата информации» – это: 1) утрата контроля за информацией, произошедшая в результате ее утечки, в том числе разглашения, хищения или копирования; 2) потеря, порча, блокирование, уничтожение или хищение единственного носителя данной информации и невозможность ее восстановления (в этом смысле можно различать временную и окончательную утрату); 3) утрата целостности или первоначальных свойств информации, в том числе в результате подмены, искажения или модификации информации;

«искажение информации» – процесс (событие), в результате которого произошли изменения в содержании или форме представления информации без воли на то ее владельца, повлекшие за собой потерю первоначальных свойств данной информации;

«подделка информации» – создание документа одним субъектом с целью выдачи его за документ другого субъекта, не имеющего к созданию данного

документа никакого отношения (первый субъект при создании поддельного документа обычно использует реквизиты, идентифицирующие второго субъекта);

«уничтожение информации» – несанкционированное действие, которое может заключаться в стирании информации в памяти компьютера или с иных носителей, невосстановимой порче бумажного документа и т. д., направленное на потерю данной информации ее законным владельцем;

«модификация информации» – как правило, заключается в несанкционированном внесении изменений в документ;

«копирование информации» – ее дублирование и устойчивая фиксация на каком-либо материальном носителе, которые не влекут за собой порчи или уничтожения оригинала (носителя, с которого делается копия);

«блокирование информации» – также не связанное с уничтожением или порчей активное действие, результатом которого является затруднение доступа к информации.

Раздел II
СУБЪЕКТЫ И ОБЪЕКТЫ КОММЕРЧЕСКОЙ ТАЙНЫ

Статья 4. Субъекты коммерческой тайны

1. К субъектам коммерческой тайны относятся физические и юридические лица государства-участника, а также других государств, занимающиеся предпринимательской деятельностью на территории государства-участника.

2. Государство гарантирует право субъекта коммерческой тайны на ее соблюдение и защиту в предусмотренном законодательством порядке.

Комментарий к статье 4

В доктрине права различают понятия субъекта права и субъекта правоотношений. Субъект права – это лицо, обладающее правосубъектностью, т. е. лицо, потенциально (вообще) способное быть участником правоотношений, а субъект правоотношения – это реальный участник данных правовых отношений. В таком понимании субъектом права на коммерческую тайну является лицо, которое потенциально может приобретать и осуществлять права и обязанности относительно коммерческой тайны и, соответственно, быть участником регулятивных правоотношений относительно коммерческой тайны. Понятие субъекта права на коммерческую тайну, таким образом, шире понятия субъекта правоотношений, складывающихся по поводу коммерческой тайны. Последним является участник правоотношений, которому принадлежат субъективные права на коммерческую тайну. Участник правоотношений, которому принадлежат права на коммерческую тайну, является активной стороной этих правоотношений (субъектом права). Другой стороной (субъектом обязанности) правоотношений по коммерческой тайне могут выступать разные лица – в зависимости от вида складывающихся правоотношений. В абсолютных правоотношениях относительно коммерческой тайны субъекту права противостоит неограниченный круг лиц, все и каждый из которых обязаны не нарушать права на коммерче-

скую тайну ее владельца. То есть такие отношения только односторонне индивидуализированы. Высшую степень индивидуализации имеют относительные правоотношения по коммерческой тайне, в которых субъекту права противостоит конкретное лицо. Например, в охранительных правоотношениях это нарушитель права на коммерческую тайну, в трудовых – это работник. В договорных и других относительных гражданских правоотношениях по коммерческой тайне каждая из сторон может одновременно выступать субъектом права и субъектом обязанности по коммерческой тайны. Субъективные права на коммерческую тайну прекращаются и лицо перестает быть участником правоотношений по коммерческой тайне с прекращением таких правоотношений. При этом, необходимо отметить, оно не перестает быть субъектом права на коммерческую тайну.

Важные законодательные положения для выяснения круга субъектов права на коммерческую тайну вообще и субъектного состава правоотношений относительно коммерческой тайны в частности содержатся в части 2 статьи 97 модельного Кодекса интеллектуальной собственности, где указано, что имущественные права интеллектуальной собственности на коммерческую тайну принадлежат лицу, которое правомерно определило информацию коммерческой тайной, если иное не установлено договором. Анализ этой нормы позволяет сделать несколько выводов.

Во-первых, субъектом прав на коммерческую тайну не может быть лицо, которое неправомерно определило информацию коммерческой тайной, например, включило в нее сведения, которые не могут составлять коммерческую тайну в соответствии с законом, не обладают необходимыми признаками конфиденциальности или коммерческой ценности, или сведения, которыми такое лицо завладело противоправно.

Во-вторых, права на коммерческую тайну могут принадлежать только тому лицу, которое определило информацию коммерческой тайной, т. е. своим волеизъявлением показало намерение удерживать определенные коммерчески ценные сведения в режиме конфиденциальности и приняло адекватные действия по сохранению такого состояния неизвестности информации. У лиц, не совершивших никаких активных действий, направленных на обеспечение правовой охраны коммерческой тайны, права на нее не возникают.

Субъектами «коммерческой тайны» являются: 1) субъект предпринимательской деятельности; 2) персонал, работники субъекта предпринимательской деятельности; 3) служебные лица государственных органов и организаций, которые проводят проверку предприятия. Субъектом предпринимательской деятельности – собственником сведений, составляющих коммерческую тайну, – являются как юридические лица, так и физические лица – предприниматели. Для удобства изложения в дальнейшем по тексту будем именовать обе категории субъектов предпринимательской деятельности предпринимателями. Организационная форма и форма собственности не имеют значения для отнесения субъекта права к категории предпринимателей. Главное, чтобы деятельность, осуществляемая таким лицом, была направлена на получение прибыли, носила коммерческий характер и это было зафиксировано в учредительных документах

(если наличие таковых является обязательным условием осуществления предпринимательской деятельности). Состав и объем сведений, составляющих коммерческую тайну, порядок работы с ними и их защиты определяются предпринимателем самостоятельно.

Работники имеют право пользоваться сведениями, составляющими коммерческую тайну, для выполнения своих трудовых обязанностей. Степень доступа каждого из работников к такой информации определяется предпринимателем самостоятельно, а условия пользования – документами, утвержденными предпринимателем, и трудовым договором (контрактом).

Служащие государственных органов и организаций, проводящие проверки предпринимателя, получают доступ к коммерческой тайне на основании соответствующих актов государственных органов и организации. Информацию о коммерческой тайне предпринимателя они получают в рамках административных правоотношений. Объем их доступа к такой информации ограничивается направлением проверки, о чем должно быть указано в документах на проверку. За разглашение коммерческой тайны служащие государственных органов и организаций несут ответственность, установленную законодательством государства-участника. Требования о неразглашении коммерческой тайны распространяются на всех служебных лиц государственных органов и организаций. Но такое требование может быть предусмотрено законодательным актом, регулирующим правовое положение отдельно от государственного органа или организации. В частности, законом о государственной налоговой службе предусмотрена ответственность сотрудников налоговых органов за разглашение сведений, составляющих коммерческую тайну.

Подытоживая изложенное, следует отметить, что субъектами прав на коммерческую тайну могут быть все участники гражданских отношений, названные в гражданском кодексе государства-участника, а именно: физические и юридические лица (в том числе иностранные или апатриды), государство, территориальные общины, иностранные государства и другие субъекты публичного права.

Статья 5. Объекты коммерческой тайны

1. Объектами коммерческой тайны (ноу-хау) являются преднамеренно скрываемые экономические интересы и сведения о различных сторонах и сферах интеллектуальной, научно-технической, производственно-хозяйственной, управленческой, финансовой деятельности хозяйствующего субъекта, охрана которых обусловлена интересами конкуренции и возможной угрозой экономической безопасности хозяйствующего субъекта.

2. Содержание и объем сведений, составляющих коммерческую тайну, определяются хозяйствующим субъектом.

3. Необоснованное отнесение общедоступной информации к коммерческой тайне не допускается.

Комментарий к статье 5

Рассмотрение информационного отражения процессов производства и сбыта позволяет выделить структурные элементы перечня сведений, составляющих коммерческую тайну предприятия. Перечень включает в себя следующие блоки информации: производство; управление производством; планирование; финансовое состояние; технология производства; НИОКР; рыночная политика и состояние рынка; партнеры и конкуренты; переговоры и контракты; цены; сбыт; собственная безопасность предприятия.

Для того чтобы принять решение о включении тех или иных данных о деятельности предприятия в перечень сведений, составляющих коммерческую тайну, целесообразно на первом этапе определить возможные отрицательные последствия в случае их разглашения.

К отрицательным последствиям относятся: разрыв деловых отношений с партнерами предприятия; срыв переговоров, утрата возможности заключения выгодного контракта; снижение уровня сотрудничества с деловыми партнерами; невыполнение договорных обязательств; необходимость проведения дополнительных рыночных исследований; отказ от решений, ставших неэффективными в результате разглашения информации, и необходимость принятия дополнительных мер, связанных с финансовыми затратами; использование конкурентами полученных сведений для повышения эффективности экономического соперничества; потеря возможности патентования и продажи лицензий; сокращение затрат конкурентов на проведение НИОКР, совершенствование технологий; снижение цен на продукцию или уменьшение объемов продажи; нанесение ущерба авторитету фирмы; снижение уровня экономической безопасности; опережающий вывод аналогичного товара на рынок конкурентом; ухудшение условий получения кредитов; появление трудностей в снабжении, приобретении оборудования; увольнение ведущих специалистов предприятия.

Для того чтобы избежать необоснованной классификации сведений, специалисты предприятия должны руководствоваться дополнительными критериями отнесения информации к коммерческой тайне. Наиболее общими из них являются: получение выигрыша во времени для предприятия сравнительно с конкурирующими фирмами; уникальность разработки; наличие новизны (новая функция потребления, новая технология, применение в новых областях); преимущества технико-экономических характеристик товара перед изделиями конкурента; оригинальное применение материалов, технологий; наличие преимуществ в ценовой конкуренции; значительные трудозатраты для получения информации; монополия предприятия на информацию по данному направлению производственно-коммерческой деятельности; вероятность использования информации конкурентами в случае ее опубликования; перспективы самостоятельного и быстрого получения закрываемых конкурентами сведений; появление возможности выхода на международный рынок; степень влияния на формирование у потребителей положительного представления о фирме; возможность обеспечения сохранности на предприятии информации в случае ее отнесения к коммерческой тайне.

Структура и содержание перечня зависят от характеристики предприятия. В перечне указываются сроки пересмотра отнесенных к коммерческой тайне сведений и перевода их в разряд общедоступных.

Практика организации защиты информации показывает, что в определенных случаях даже при поставках товара на рынок конкретные сведения о его производстве и сбыте достаточно длительное время могут охраняться как интеллектуальная собственность предприятия.

При отнесении сведений к коммерческой тайне руководствуются экономической целесообразностью, так как ограничение на пользование информацией может существенно мешать эффективному функционированию предприятия. Сведения сохраняются в тайне в том случае, если они являются составной частью основного качества изделия (например, приборы и устройства охраны, специальные замки, сейфы) или технология изготовления товара такова, что не позволяет конкуренту в процессе реконструирования получить скрытые данные.

Дж. Н. А. Пули в своей книге «Коммерческая тайна» рекомендует выделить в производственно-коммерческой деятельности предприятия все то, что отличает его от конкурентов, что не следовало бы раскрывать им.

В первую очередь надо защищать ценную информацию, утечка которой способна нанести ущерб, значительно превышающий затраты на ее защиту. При анализе важно установить: какая информация нуждается в защите; кого она может заинтересовать, какова ее ценность для конкурентов; какие элементы информации наиболее ценны; каков срок существования сведений, составляющих коммерческую тайну; во что обойдется защита.

Сведения, отнесенные к коммерческой тайне, должны иметь следующие признаки: не являться государственными секретами; относиться к производственной деятельности предприятия; не наносить ущерба интересам общества; иметь действительную или потенциальную коммерческую ценность и создавать преимущества в конкурентной борьбе; иметь ограничения в доступе, устанавливаемые руководителем предприятия на законном основании; предприятие (фирма) принимает меры к их охране.

К коммерческой тайне могут быть отнесены: технология производства; технологические приемы и оборудование; модификация ранее известных технологий и процессов; результаты и программы НИОКР; перспективные методы управления; ценовая и сбытовая политика; сравнительные характеристики собственного ассортимента и товаров конкурентов с точки зрения качества, внешнего вида, упаковки и т. д.; производственные, коммерческие и финансово-кредитные отношения с партнерами; планы предприятия по расширению (свертыванию) производств; факты ведения переговоров по вопросу купли-продажи; данные, которые могут быть использованы для нанесения ущерба репутации предприятия (фирмы); информация о кадрах (текучесть кадров, ведущие специалисты и места их работы по совместительству); наличие средств и условий для защиты коммерческой тайны.

Иностранные фирмы рассматривают в качестве промышленной собственности изобретения, данные об оборудовании, инструменте, разработанные

или приобретенные ими и недоступные для широкого пользования. К промышленным секретам фирмы относят основные производственные показатели, проекты, технологические инструкции, результаты проверок и испытаний, описание образцов продукции на сырье, сущность экспериментов, оценку качества процессов и изделий, исследовательские отчеты, карты контроля качества, инструкции по подготовке кадров, стоимостные показатели, исследования рынка, список покупателей, условия поставок и стратегия на рынке, прогнозы и т. д.

Перечень сведений, которые необходимо защищать в условиях рынка, может быть довольно обширен. Представляют интерес данные о том, что хотели бы знать иностранные фирмы о своих конкурентах.

Перечень сведений, которые необходимо защищать в условиях рынка

– Информация о рынке: цены, скидки, условия договоров, спецификация продукта; объем, тенденция и прогноз для данного продукта; доля на рынке и тенденция ее изменения; рыночная политика и планы; отношения с потребителями и репутация; численность и размещение торговых агентов; каналы, политика и методы сбыта; программа рекламы.

– Информация о производстве и продукции: оценка качества и эффективности; номенклатура изделий; технология и оборудование; уровень издержек; производственные мощности; размещение и размер производственных подразделений и складов; способ упаковки; доставка; возможности проведения НИОКР.

– Информация об организационных особенностях и финансах: лица, принимающие ключевые решения; философия лиц, принимающих ключевые решения; финансовые условия и перспективы; программы расширения и приобретений; главные проблемы и возможности; программы НИОКР.

Более детальная расшифровка сведений, представляющих первоочередной интерес для конкурентов, дается также в другом перечне. Его оценка позволяет сделать вывод, что именно эти сведения с большей степенью вероятности могут быть коммерческой тайной предприятия.

– Информация в финансово-экономической сфере: результаты производственной деятельности банков и предприятий за квартал, полугодие, год; выводы и рекомендации экспертов по вопросам тактики и стратегии экономической деятельности, переговоров с партнерами, данные об объемах закупки-продажи товаров, услуг, уровне максимально уторгованных цен, объемах имеющихся валютных средств, используемых для повышения эффективности сделок; номенклатура и количество товаров по взаимным обязательствам, объемы перевозок, транзита грузов и транспортные расходы; себестоимость товаров, услуг, кредитные и платежные условия; фактическое состояние расчетов с теми или иными партнерами; экспортно-импортная продукция, финансовые плановые и фактические показатели этой продукции; методика расчета конкурентных цен по товарам, работам и услугам; время выхода на рынок при закупках или продаже товаров и услуг, выбор партнеров по заключению сделок с дефицитной продукцией; планируемые кредиты, условия и их размеры; планируемое создание совместных, смешанных, малых, акционерных предприятий; неудовлетворительное финансовое положение предприятия; эффективность и целесообраз-

ность закупки лицензий, заинтересованность заказчиков в той или иной валюте и ее количестве; состав торговых клиентов, посредников предприятия, товарооборот с ними.

– Информация в научно-технической и технологической сферах: основные производственные фонды, их мощности и эффективность; направления расширения (свертывания) производства, применяемые (готовящиеся к внедрению) технологии, оборудование; модификация и модернизация применяемой ранее техники, технологии; отдельные узлы готовых изделий, новые разработки высокой конкурентоспособности; применяемые (готовящиеся к применению) методы управления производством, программное и компьютерное обеспечение производства, возможные пути получения информации, хранящейся в ЭВМ и ПЭВМ руководства, главные специалисты предприятия; ведущиеся НИОКР, проектные работы и их результаты; цели совещаний, заседаний органов управления предприятия.

На стадии НИОКР целесообразно обеспечить защиту следующей информации: возможная прибыльность разрабатываемого изделия; уровень патентной защиты; вероятность конструкторского и технологического решения проблемы; предполагаемые расходы на экспериментальной стадии и требуемые капиталовложения в организацию нового производства или в модернизацию существующего; срок окупаемости данного проекта нового товара; сроки завершения этапов работ; возможные трудности технического, финансового, кадрового и иного характера, намечаемые способы их преодоления; возможная длительность жизненного цикла разрабатываемого изделия; возможное эмоциональное воздействие товара на покупателя; возможное время создания коммерчески завершенного товара; возможность производства по конкурентоспособной цене.

За рубежом к категории закрытой информации в области научных исследований, подлежащих защите, относят: отчеты о проделанных научных исследованиях; оригинальные работы; результаты экспериментального исследования; расчеты, относящиеся к определенным видам изделий; сведения о результатах проверки рабочих гипотез; данные анализов, данные о лабораторных и производственных испытаниях.

Решение о защите принимается в отношении таких сведений, без которых невозможно воспроизвести полученные научно-технические решения. Следует отметить, что организация защиты не исключает возможности открытой публикации о защищаемой НИОКР, но закрытые сведения не упоминаются в открытых публикациях.

– Информация в социальной сфере: интеллектуальный потенциал коллектива, его ведущие специалисты, их моральные и деловые качества, наличие компрометирующих их связей, биографические данные; используемая в коллективе система стимулов, укрепляющих дисциплину, повышающих производительность труда, сохранность коммерческой тайны; различные аспекты, касающиеся экономической безопасности предприятия; любые возможности нанесения морального ущерба предприятию, понижения его престижа в обществе и конкурентоспособности; планируемые рекламные акции; имеющиеся противоречия между коллективом предприятия и госструктурами, интересами

общественности; личные отношения ведущих специалистов как между собой, так и с руководителями экологических, экономических, административных организаций; возможные противоречия, конфликты внутри коллектива, их конкретные участники; наличие у членов коллектива, руководства, руководителей подразделений намерений начать свое дело, финансовые и моральные проблемы.

Исследования механизма противоборства в торгово-экономической сфере позволяют выделить сведения, которые можно отнести к коммерческой тайне при заключении контрактов.

– Информация в связи с подписанием контракта: объемы экспортных поставок и услуг; цена на поставляемые товары и услуги; валютно-финансовые условия; суммы поступлений от реализации контрактов; факт ведения переговоров, партнеры на переговорах.

Нераспространение, сокрытие от вероятных конкурентов вышеупомянутой информации затрудняет их действия, обеспечивает предприятию экономические преимущества.

Обеспечение сохранности коммерческой тайны создает предпосылки для монопольных действий в конкретной сфере бизнеса, является своеобразной форой в экономическом соревновании.

В последние годы в промышленно развитых странах службы безопасности стали принимать меры по защите информации, которую соперничающие фирмы могут получить при анализе отходов продукции, поступающих в утилизацию или на рынок. Главной формой защиты является сохранение в тайне фирмами, специализирующимися на продаже отходов производств, сведений о предприятиях – поставщиках этого сырья.

Как отмечалось выше, прибыль в основном зависит от производственных и рыночных факторов. Поэтому большой блок защищаемой информации отражает специфику взаимодействия изготовителя (поставщика) и потребителя (заказчика).

В связи с этим особый интерес представляет Закон Азербайджанской Республики «О коммерческой тайне». В нем (раздел IV «Особенности правовой охраны “ноу-хау” в режиме коммерческой тайны») детально урегулированы отношения, касающиеся ноу-хау. Последнее включает в себя сведения, отнесенные как результат умственной деятельности к коммерческой тайне, которые не охраняются патентом в соответствии с законодательством или по желанию владельца. Согласно статье 12 указанного закона ноу-хау как объект интеллектуальной собственности охраняется в режиме коммерческой тайны. В законе установлены условия возникновения права собственности на ноу-хау, которое явилось следствием выполнения служебного задания (статья 14), выполнения гражданско-правового договора (статья 15), отношений с органами государственной власти (статья 16), а также условия передачи прав собственности на ноу-хау. К правам владельца ноу-хау относятся: использование ноу-хау в личном производстве с включением его в состав нематериальных активов; передача на договорной основе другому лицу в предусмотренном данным законом порядке всех прав или определенной части прав на ноу-хау; вознаграждение за

использование ноу-хау в предусмотренных настоящим законом случаях; права владельца ноу-хау возникают с фактом появления ноу-хау и принятия в отношении него охранных мер. Предоставление прав собственности на ноу-хау не требует определенного оформления (прохождения регистрации, получения свидетельства и пр.).

Статья 6. Сведения, которые не могут составлять коммерческую тайну.

1. Хозяйствующий субъект несет ответственность за необоснованное отнесение общедоступной информации к коммерческой тайне.

2. К коммерческой тайне не могут относиться:

а) учредительные документы и документы, разрешающие заниматься предпринимательской или хозяйственной деятельностью и ее отдельными видами;

б) информация по всем установленным формам государственной отчетности;

в) данные, необходимые для проверки исчисления и уплаты налогов и других обязательных платежей;

г) сведения о численности и составе работающих, системе оплаты труда, а также о наличии свободных рабочих мест;

д) сведения об уплате налогов и обязательных платежей;

е) сведения о загрязнении окружающей природной среды, несоблюдении безопасных условий труда, реализации продукции, наносящей вред здоровью, а также об иных нарушениях национального законодательства и о размерах нанесенных при этом убытков;

ж) документы о платежеспособности;

з) сведения об участии должностных лиц предприятия в кооперативах, малых предприятиях, союзах, объединениях и других организациях, занимающихся предпринимательской деятельностью;

и) сведения об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;

к) сведения о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;

л) сведения, обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными законами государства-участника.

Комментарий к статье 6

В статье перечислены разновидности сведений, которые не могут составлять коммерческую тайну лиц, осуществляющих предпринимательскую деятельность.

До принятия комментируемого Закона эти сведения содержались в различных нормативных правовых актах государств-участников. Аналогичный

подход принят в законах «О коммерческой тайне» Кыргызстана (статья 4), Молдовы (статья 5), Азербайджана (статья 4). Вместе с тем Закон уточнил и в некоторых случаях расширил данный перечень.

Как следует из этого перечня, законами могут быть предусмотрены и иные виды сведений, которые не могут быть отнесены к информации, составляющей коммерческую тайну. Такие сведения, в частности, указаны в Федеральном законе от 22 апреля 1996 года № 39-ФЗ «О рынке ценных бумаг» (в редакции от 23 июля 2013 года). Например, согласно указанному закону организатор торговли на рынке ценных бумаг (т. е. профессиональный участник рынка ценных бумаг, осуществляющий деятельность по организации торговли на рынке ценных бумаг) обязан раскрыть любому заинтересованному лицу следующую информацию: правила допуска участника рынка ценных бумаг к торгам; правила допуска к торгам ценных бумаг; правила заключения и сверки сделок; правила регистрации сделок; порядок исполнения сделок; правила, ограничивающие манипулирование ценами; расписание предоставления услуг организатором торговли на рынке ценных бумаг; регламент внесения изменений и дополнений в вышеперечисленные позиции; список ценных бумаг, допущенных к торгам.

Раздел III
ОБЛАДАНИЕ КОММЕРЧЕСКОЙ ТАЙНОЙ И ЕЕ ЗАЩИТА

Статья 7. Права обладателя информации, составляющей коммерческую тайну

1. Права обладателя коммерческой тайны в соответствии со статьей 12 настоящего Закона возникают с момента установления им в отношении этой информации режима коммерческой тайны.

2. Обладатель коммерческой тайны имеет право:

а) устанавливать, изменять и отменять в письменной форме режим коммерческой тайны в соответствии с настоящим Законом и гражданско-правовым договором;

б) использовать коммерческую тайну для собственных нужд в порядке, не противоречащем национальному законодательству;

в) разрешать или запрещать доступ к коммерческой тайне, определять порядок и условия доступа к этой информации;

г) вводить в гражданский оборот коммерческую тайну на основании договоров, предусматривающих включение в них условий об охране конфиденциальности этой информации;

д) требовать от юридических и физических лиц, получивших доступ к коммерческой тайне, органов государственной власти, иных государственных органов, органов местного самоуправления, которым предоставлена коммерческая тайна, соблюдения обязанностей по охране ее конфиденциальности;

е) требовать от лиц, получивших доступ к коммерческой тайне в результате действий, осуществленных случайно или по ошибке, охраны

конфиденциальности этой информации, в том числе возмещения издержек, связанных с соблюдением обязанностей по охране коммерческой тайны;

ж) защищать в установленном законом порядке свои права в случае разглашения, незаконного получения или незаконного использования третьими лицами коммерческой тайны, в том числе требовать возмещения убытков, причиненных в связи с нарушением его прав.

Комментарий к статье 7

1. Статья посвящена правам обладателя информации, составляющей коммерческую тайну.

Пункт 1 статьи устанавливает, что права обладателя указанной информации возникают лишь с момента установления им в отношении такой информации режима коммерческой тайны в соответствии со статьей 12 комментируемого Закона.

2. В пункте 2 перечислены права обладателя информации, составляющей коммерческую тайну.

В совокупности данные права обеспечивают фактическую монополию субъекта в отношении информации, составляющей коммерческую тайну, которой он обладает на законном основании.

Отметим, что как таковых исключительных и иных прав на информацию (о которых нередко говорится в литературе) не существует. В отношении информации как таковой (в том числе составляющей коммерческую тайну) может быть установлена лишь фактическая монополия, которая сводится к правам обладателя данной информации принимать превентивные меры по ограничению доступа к ней, а также требовать от других лиц не нарушать установленный режим доступа. В связи с этим такие словосочетания, как «защита информации» или «защита прав на информацию», некорректны с юридической точки зрения (хотя и являются более понятными для обывателя). В данном случае речь может идти лишь о защите законных интересов (фактической монополии) обладателя информации.

Кроме того, напомним, что сущность «защиты» заключается в принятии мер восстановительного характера уже после того, как некое незаконное (противоправное) действие свершилось. Так, защита интересов законного обладателя информации, составляющей коммерческую тайну, может осуществляться путем требования применить санкции ответственности к хакерам, создателям и распространителям компьютерных вирусов, которые причинили ему ущерб своими несанкционированными действиями в отношении ценных ресурсов.

Статья 8. Обладатель коммерческой тайны при выполнении служебных обязанностей

1. Обладателем коммерческой тайны в отношении информации, созданной работником в связи с выполнением им служебных обязанностей или по заданию работодателя, является работодатель, если договором между ним и работником не предусмотрено иное.

2. Условия выплаты и размер вознаграждения работника (автора), создавшего информацию, отнесенную к коммерческой тайне, в том числе способную к правовой охране в качестве изобретения, полезной модели, промышленного образца, определяются в соответствии с национальными законами и иными нормативными правовыми актами.

Комментарий к статье 8

В современных условиях подавляющее большинство (около 90%) результатов научно-технической деятельности и объектов патентного права (изобретения, полезные модели, промышленные образцы) создаются в результате научно-технических разработок на промышленных предприятиях, в научно-исследовательских институтах, лабораториях и научных центрах. В связи с этим важную роль играет наличие эффективного правового регулирования отношений между работодателем и работником (создателем научно-технической разработки), которое могло бы обеспечить заинтересованность в разработке и использовании технических новинок работодателей, а также обеспечить материальную заинтересованность работников в их создании. Третьей заинтересованной стороной в урегулировании этих сложных и многоаспектных отношений выступает государство, заинтересованное в техническом прогрессе в целом.

Субъектами правоотношений в сфере служебного изобретательства являются работодатель и служащий. В качестве работодателя может выступать любое предприятие, учреждение или организация независимо от формы собственности, в сфере деятельности которых создается служебная разработка и с которыми работники находятся в трудовых отношениях, а в качестве служащего – любое физическое лицо, работающее по найму на предприятии или находящееся в других трудовых отношениях с работодателем.

В соответствии со статьей 8 комментируемого Закона обладателем информации, составляющей коммерческую тайну, созданной работником в связи с выполнением им служебных обязанностей или по заданию работодателя, является работодатель.

В случае получения работником в связи с выполнением трудовых обязанностей или конкретного задания работодателя результата, способного к правовой охране в качестве изобретения, полезной модели, промышленного образца, программы для электронных вычислительных машин или базы данных, отношения между работником и работодателем регулируются в соответствии с законодательством государства-участника об интеллектуальной собственности.

Существуют определенные методы расчета размера вознаграждения. На практике, в зависимости от ситуации, размер вознаграждения может определяться одним из трех методов: по аналогии с определением стоимости лицензии, по объему фактического использования, методом экспертных оценок.

Статья 9. Обладатель коммерческой тайны при выполнении государственного контракта для государственных нужд

1. Обладателем коммерческой тайны в отношении информации, созданной при выполнении работ по государственному контракту для государственных нужд, является исполнитель (подрядчик), если государственным контрактом не установлено, что им является государственный заказчик.

2. В случае если обладателем коммерческой тайны в отношении информации, созданной при выполнении работ для государственных нужд, является не государственный заказчик, ее обладатель по требованию государственного заказчика обязан заключить с указанными им лицами договор о безвозмездном предоставлении права на использование информации, составляющей коммерческую тайну, при изготовлении товаров или выполнении подрядных работ для государственных нужд.

3. Режим коммерческой тайны и условия его применения устанавливаются исполнителем (подрядчиком) и государственным заказчиком в соответствии с государственным контрактом или отдельным соглашением, являющимся дополнением к этому контракту.

Комментарий к статье 9

Согласно нормам гражданского кодекса по договору на выполнение научно-исследовательских работ исполнитель обязуется провести обусловленные техническим заданием заказчика научные исследования, а по договору на выполнение опытно-конструкторских и технологических работ – разработать образец нового изделия, конструкторскую документацию на него или новую технологию, а заказчик обязуется принять работу и оплатить ее. Условия таких договоров должны соответствовать законам и иным нормативным правовым актам об исключительных правах (интеллектуальной собственности).

К государственным контрактам на выполнение научно-исследовательских работ, опытно-конструкторских и технологических работ для государственных нужд применяются правила положений о подрядных работах для государственных нужд.

Предмет государственного контракта на выполнение подрядных работ для государственных нужд таков: подрядчик обязуется выполнить строительные, проектные и другие связанные со строительством и ремонтом объектов производственного и непроизводственного характера работы и передать их государственному заказчику, а государственный заказчик обязуется принять выполненные работы и оплатить их или обеспечить их оплату. Государственным заказчиком может выступать государственный орган, обладающий необходимыми инвестиционными ресурсами, или организация, наделенная соответствующим государственным органом правом распоряжаться такими ресурсами, а подрядчиком – юридическое лицо или гражданин.

Как следует из статьи 9 комментируемого Закона, стороны государственного контракта на выполнение научно-исследовательских, опытно-конструкторских, технологических или иных работ для государственных нужд

или нужд субъекта государства-участника должны определить объем сведений, являющихся конфиденциальными, и указать их в государственном контракте. Кроме того, стороны государственного контракта также должны урегулировать вопросы, касающиеся установления в отношении полученной информации режима коммерческой тайны.

Если иное не предусмотрено договорами на выполнение научно-исследовательских работ, опытно-конструкторских и технологических работ, стороны обязаны обеспечить конфиденциальность сведений, касающихся предмета договора, хода его исполнения и полученных результатов. Объем сведений, признаваемых конфиденциальными, определяется в договоре. При этом каждая из сторон обязуется публиковать полученные при выполнении работы сведения, признанные конфиденциальными, только с согласия другой стороны.

В соответствии с патентным законодательством право на получение патента на изобретение, полезную модель или промышленный образец, созданные при выполнении работ по государственному контракту для государственных нужд или нужд субъекта государства-участника, принадлежит исполнителю (подрядчику), если государственным контрактом не установлено, что это право принадлежит субъекту государства-участника, от имени которого выступает государственный заказчик. В случае если в соответствии с государственным контрактом право на получение патента принадлежит государству или его субъекту, государственный заказчик может подать заявку на выдачу патента в течение шести месяцев с момента его уведомления в письменной форме исполнителем (подрядчиком) о получении результата, способного к правовой охране в качестве изобретения, полезной модели или промышленного образца. Если в течение указанного срока государственный заказчик не подаст заявку, право на получение патента имеет исполнитель (подрядчик).

Статья 10. Имущественные права на коммерческую тайну

1. Имущественными правами на коммерческую тайну являются:

а) право на использование коммерческой тайны;

б) исключительное право разрешать использование коммерческой тайны;

в) исключительное право препятствовать неправомерному разглашению, сбору или использованию коммерческой тайны;

г) иные имущественные права интеллектуальной собственности, установленные законом.

2. Имущественные права на коммерческую тайну относящиеся к деятельности предприятия, входят в состав предприятия как имущественного комплекса и отражаются на балансе юридического лица в соответствии с законодательством государства-участника.

Комментарий к статье 10

Согласно подпункту «а» пункта 1 комментируемой статьи к имущественным правам интеллектуальной собственности на коммерческую тайну относится право на ее использование. Использованием коммерческой тайны следует

считать внедрение в гражданский оборот сведений, которые в соответствии с действующим законодательством составляют коммерческую тайну, лицом, которому эти сведения были доверены в установленном порядке или стали известны в связи с выполнением служебных обязанностей. Использование коммерческой тайны может иметь место только при внедрении или учете таких сведений при осуществлении хозяйственной деятельности, т. е. такой, которая направлена на получение прибыли. Размер потенциальной материальной выгоды, полученной в результате использования сведений, составляющих коммерческую тайну, гражданским законодательством не определяется. Оценка стоимости прав на информацию, которая является коммерческой тайной, должна осуществляться по правилам оценки нематериальных активов.

Еще одним имущественным правом интеллектуальной собственности на коммерческую тайну является исключительное право разрешать ее использование иным лицам. Это право осуществляется прежде всего путем передачи права на использование коммерческой тайны на основании договора и установления в нем запрета на ее разглашение третьим лицам. Использование коммерческой тайны может иметь место только с разрешения правообладателя или уполномоченного законом или договором лица. Любое использование коммерческой тайны без разрешения указанных лиц считается незаконным. Незаконным, а следовательно, и неправомерным использование коммерческой тайны будет тогда, когда информация внедряется в производство или учитывается при планировании хозяйственной деятельности вопреки воле ее законного правообладателя, т. е. без разрешения уполномоченного на то лица. Лицо, которое противоправно использует коммерческую тайну, право интеллектуальной собственности на которую принадлежит субъекту хозяйствования, обязано возместить причиненные ему такими действиями убытки в соответствии с действующим законодательством государства-участника.

Другим видом имущественных прав интеллектуальной собственности на коммерческую тайну является исключительное право правообладателя препятствовать не только неправомерному использованию коммерческой тайны, но и ее разглашению или уборке. Под разглашением коммерческой тайны следует понимать ознакомление со сведениями, ее составляющими, других лиц без согласия ее правообладателя лицом, которому эти сведения были доверены в установленном порядке или стали известны в связи с выполнением служебных обязанностей. Неправомерным сбором сведений, составляющих коммерческую тайну, считается получение противоправным путем сведений, если это причинило или могло причинить ущерб субъекту хозяйствования. С правовой точки зрения коммерческая тайна является средством защиты от недобросовестной конкуренции в рамках осуществления прав интеллектуальной собственности. Именно поэтому не допускается недобросовестная конкуренция, к которой, в частности, относится неправомерное разглашение и использование коммерческой тайны без согласия субъекта права интеллектуальной собственности на нее. Самым сложным с практической и теоретической точек зрения является вопрос о сохранении коммерческой тайны работником, которому она была известна в соответствии с выполняемой работой после его увольнения. Во многих

случаях трудно отделить опыт и знания, полученные работником в процессе его профессиональной деятельности на предприятии, от незаконного разглашения конфиденциальной информации, права на которую принадлежат бывшему работодателю. От решения этого вопроса зависит оценка поведения работника: можно квалифицировать его как заговор с конкурентом, или это другое противоправное действие, подпадающее под нарушение законодательства о защите от недобросовестной конкуренции и разглашении конфиденциальной информации.

Пункт 1 комментируемой статьи не содержит исключительного перечня имущественных прав интеллектуальной собственности на коммерческую тайну, допуская, что такие права могут быть установлены законом в будущем, поскольку сегодня законодательство не содержит каких-либо указаний относительно других имущественных прав интеллектуальной собственности на коммерческую тайну.

2. Субъектом, которому могут принадлежать имущественные права интеллектуальной собственности на коммерческую тайну, может быть как физическое, так и юридическое лицо, осуществляющее хозяйственную деятельность и имеющее монопольное право на информацию, являющуюся с их точки зрения коммерческой тайной. Такие лица являются первичными субъектами права интеллектуальной собственности на коммерческую тайну. Ко вторичным субъектам права интеллектуальной собственности на коммерческую тайну относятся правопреемники первичных субъектов. Это физические и юридические лица, которым в силу служебного положения или на ином законном основании известна информация, составляющая коммерческую тайну.

Статья 11. Механизм определения порядка защиты коммерческой тайны

Субъектами коммерческой тайны разрабатываются инструкции, положения по обеспечению сохранности коммерческой тайны, в которых определяются:

а) состав и объем сведений, составляющих коммерческую тайну;

б) порядок присвоения грифа «Коммерческая тайна» сведениям, работам и изделиям и его снятия;

в) процедура допуска работников хозяйствующего субъекта, а также лиц, привлекаемых к его деятельности, к сведениям, составляющим коммерческую тайну;

г) порядок использования, учета, хранения и маркировки документов и иных носителей информации, изделий, сведения о которых составляют коммерческую тайну;

д) организация контроля за порядком использования сведений, составляющих коммерческую тайну;

е) процедура принятия взаимных обязательств хозяйствующими субъектами по сохранению коммерческой тайны при заключении договоров о проведении каких-либо совместных действий;

ж) порядок применения предусмотренных законодательством мер дисциплинарного и материального воздействия на работников, разгласивших коммерческую тайну;

з) возложение ответственности за обеспечение сохранности коммерческой тайны на должностное лицо хозяйствующего субъекта.

Комментарий к статье 11

В системе организационных, административных, правовых и других мер, позволяющих качественно решать задачи информационного обеспечения научно-производственной и коммерческой деятельности, физической сохранности материальных носителей закрытых сведений, предотвращения их утечки, разглашения коммерческой тайны важное место занимает определение системы доступа исполнителей к классифицированным документам и сведениям.

Руководитель предприятия (фирмы) вне зависимости от формы собственности может устанавливать специальные правила доступа к сведениям, составляющим коммерческую тайну, и ее носителям, тем самым обеспечивая их сохранность.

В системе мер безопасности существенное значение имеет оптимальное распределение производственных, коммерческих и финансово-кредитных сведений, составляющих тайну предприятия, между конкретными исполнителями соответствующих работ и документов. При распределении информации, с одной стороны, необходимо обеспечить предоставление конкретному сотруднику для качественного и своевременного выполнения порученных ему работ полного объема данных, а с другой стороны, следует исключить ознакомление исполнителя с излишними, не нужными ему для работы классифицированными сведениями.

В целях обеспечения правомерного и обоснованного доступа исполнителя к сведениям, составляющим коммерческую тайну фирмы, рекомендуется разрабатывать и внедрять на предприятиях соответствующую разрешительную систему.

Под доступом понимается получение письменного разрешения руководителя предприятия (или, с его санкции, других руководящих лиц) на выдачу тому или иному сотруднику конкретных (или в полном объеме) закрытых сведений с учетом его служебных обязанностей (должностных полномочий).

Оформление доступа к коммерческой тайне может производиться в соответствии с утвержденным руководителем предприятия положением о разрешительной системе доступа, где юридически закрепляются полномочия должностных лиц предприятия по распределению информации и пользованию ею. Руководитель предприятия может разрешить пользование любой охраняемой информацией любому работнику данного предприятия или лицу, прибывшему на объект из другой организации для решения каких-либо вопросов, если в отношении этих сведений не установлены ограничения на ознакомление со стороны производственно-коммерческого партнера по совместному производству и т. п.

На небольших предприятиях с ограниченным объемом закрытых работ (документов или изделий) руководитель имеет возможность лично распределять всю закрытую информацию, поступающую извне или создаваемую внутри предприятия, между работниками независимо от занимаемых ими должностей. В этом случае осуществляется так называемое прямое распределение классифицированной информации. Однако прямое распределение становится невозможным на предприятии с большим объемом закрытых работ, рассредоточенных по различным подразделениям и участкам, в которых принимают участие специалисты различных должностных категорий. В этих условиях руководитель предприятия физически не имеет возможности лично регулировать потоки классифицированной информации и распределять ее между работниками. Возрастает вероятность ошибок в виде неправильного адресования сведений или разрешения на доступ лицам, не имеющим к ним прямого производственного отношения.

Для качественного выполнения управленческих функций в данных условиях руководитель предприятия часть своих прав распоряжаться движением классифицированных сведений передает (делегирует) руководителям нижестоящих уровней. При определении полномочий каждого нижестоящего руководителя выполняется ряд условий. Эти полномочия должны соответствовать и осуществляться в рамках его должностного положения (прав и обязанностей). Полномочия, данные ему директором, должны распространяться только на определенные категории исполнителей закрытых работ и документов.

Важнейшее значение в деле обеспечения сохранности коммерческой тайны имеет надежность сотрудника, которому разрешают работать с ценной информацией. Степень надежности шифра определяется прежде всего надежностью шифровальщика.

В связи с этим система доступа должна базироваться на убеждении, что лица, получающие разрешение на доступ к закрытым сведениям, лояльны по отношению к предприятию (фирме). Такой вывод могут сделать в процессе совместной деятельности служба безопасности и отдел кадров предприятия. Эти подразделения утверждают у руководителя предприятия список сотрудников, кто в силу своих личных качеств может быть допущен (или не допущен) к работе со сведениями, составляющими коммерческую тайну. Соответствующие выписки из списка передаются для учета руководителям подразделений, которым руководителем предприятия делегировано право давать разрешение на доступ к конкретным сведениям, входящим в перечень охраняемой информации.

Руководитель, как правило, оставляет за собой право распоряжаться наиболее ценными сведениями, составляющими коммерческую тайну (конфиденциальные договоры с фирмами, отчеты о результатах работ по перспективным изделиям и т. п.). Перечень таких документов, утвержденный руководителем предприятия, должен находиться в службе безопасности. В соответствии с этим перечнем вся классифицированная информация и изделия, поступившие извне или созданные на предприятии, предоставляются руководству службы безопасности. Остальная информация поступает из службы безопасности непосредственно руководителям нижестоящих уровней в соответствии с действую-

щей на предприятии разрешительной системой. Они и распределяют ее между исполнителями. Количество уровней должностной иерархии и должностных лиц, которым могут быть предоставлены полномочия на распределение классифицированной информации, зависит от структуры предприятия, количества и сложности проводимых закрытых работ.

Эффективная работа разрешительной системы возможна только при соблюдении определенных правил.

Во-первых, разрешительная система в качестве обязательного для исполнения правила включает в себя дифференцированный подход к разрешению доступа, учитывающий важность классифицированных сведений, в отношении которых решается вопрос о доступе.

Во-вторых, необходимо документальное отражение выданного разрешения на право пользования теми или иными защищаемыми сведениями. Это означает, что руководитель, давший разрешение на право пользования, должен его в обязательном порядке зафиксировать в письменном виде на соответствующем документе или в действующей на предприятии учетной форме. Никакие устные указания и просьбы о доступе кого бы то ни было (за исключением руководителя предприятия) не должны иметь юридической силы и не обязательны для работников службы безопасности. Это требование относится и к руководителям всех уровней, работающих с классифицированной информацией и ее носителями. Таким образом, только письменное разрешение руководителя (в рамках полномочий) является разрешением для выдачи тому или иному лицу охраняемых сведений.

В-третьих, следует строго соблюдать принцип контроля со стороны службы безопасности. Это означает, что любое разрешение (здесь возможны исключения из правила по согласованию с директором) на ознакомление с закрытыми документами, сведениями и объектами должно быть согласовано с начальником службы безопасности. Каждое решение должно иметь дату его оформления или выдачи.

Широкое распространение имеет такой традиционный вид разрешения, как резолюция руководителя на самом классифицированном документе. Такое разрешение должно содержать перечень фамилий работников, обязанных ознакомиться с документами или их исполнить, срок исполнения, другие указания, подпись руководителя и дату.

Руководитель при необходимости может предусмотреть ограничения в доступе конкретных сотрудников к определенным сведениям.

Резолюция как вид разрешения применяется главным образом для оперативного доведения до заинтересованных лиц закрытой информации, содержащейся в документах и изделиях, поступающих на предприятие извне или создаваемых на предприятии. Руководитель предприятия может дать разрешение на доступ в распорядительных документах: приказах, указаниях, распоряжениях по предприятию. В них должны содержаться фамилии, должности лиц, конкретные классификационные документы и изделия, к которым они могут быть допущены (ознакомлены).

Другим видом разрешений могут быть пофамильные списки лиц, имеющих право ознакомлять или производить какие-либо действия с классификационными документами и изделиями. Пофамильные списки утверждаются директором предприятия или, согласно действующей разрешительной системе, соответствующими руководителями, как правило, не ниже должностей руководителей структурных подразделений.

Пофамильные списки лиц могут использоваться при организации доступа к определенным классифицированным документам и изделиям, имеющим особо важное значение для предприятия, при оформлении доступа в режимные помещения, на различного рода закрытые мероприятия (конференции, совещания, выставки, заседания научно-технических советов и т. п.). В пофамильных списках могут быть определены конкретные руководители, которые директором допускаются ко всем закрытым документам и изделиям без оформления соответствующих письменных разрешений. В них указываются фамилия, имя, отчество исполнителя работ, отдел, занимаемая должность, категория документов и изделий, к которым он допущен. На практике применим также вариант должностных списков, в которых указываются должность исполнителя, объем документов (категории документов) и типы изделий, которыми необходимо пользоваться работникам предприятия, занимающим соответствующую списку должность. Следует отметить, что для предприятий с небольшим объемом классифицированных документов и изделий может оказаться достаточным использование таких видов разрешений, как резолюция руководителя на самом документе, пофамильные списки, должностные списки.

В организационном плане пофамильные списки, как правило, должны готовиться заинтересованными руководителями структурных подразделений. Перечень сотрудников, вошедших в список, визируется начальником службы безопасности и утверждается руководителем предприятия. Руководитель предприятия может делегировать права утверждения другим конкретным лицам из числа дирекции.

Наряду со списками могут быть использованы персональные электронные карточки – разрешения на доступ к классифицированной информации и изделиям.

Разрешительная система должна отвечать следующим требованиям:

1) распространяться на все виды классифицированных документов и изделий, имеющихся на предприятии, независимо от их места нахождения и создания;

2) определять порядок доступа всех категорий сотрудников, получивших право работать с коммерческой тайной, а также специалистов, временно прибывающих на предприятие и имеющих отношение к совместным закрытым заказам;

3) устанавливать простой и надежный порядок оформления разрешений на доступ к охраняемым документам и изделиям, позволяющий незамедлительно реагировать на изменения в области информации на предприятии;

4) четко разграничивать права руководителей различных должностных уровней в оформлении доступа соответствующих категорий исполнителей;

5) исключать возможность бесконтрольной и несанкционированной выдачи документов и изделий кому бы то ни было;

6) не допускать внесения лицами, допущенными к классифицированной информации и объектам, изменений в учетные данные, а также подмены учетных документов.

При разработке разрешительной системы особое внимание должно быть обращено на выделение главных, особо ценных для предприятия сведений, что позволит обеспечить строго ограниченный к ним доступ. Если имеют место совместные работы с другими предприятиями (организациями), иностранными фирмами или их отдельными представителями, необходимо предусмотреть порядок их доступа к коммерческой тайне предприятия. Целесообразно определить порядок взаимодействия с представителями обслуживающих государственных организаций: технадзором, санэпидемстанцией и др.

В пределах разрешительной системы руководители среднего звена управления фирмой могут:

– давать разрешение (в рамках полномочий) на доступ к классифицированным документам и сведениям исполнителям своего подразделения, исполнителям других подразделений по ходатайству их руководителей и в пределах их функциональных обязанностей;

– отменять документы, неправильно адресованные руководителями подчиненных подразделений;

– требовать от службы безопасности выдачи исполнителям документов и изделий, необходимых для выполнения производственных заданий, в пределах их функциональных обязанностей.

Для соблюдения режима руководители обязаны:

– знать требования разрешительной системы, свои права в управлении доступом сотрудников предприятия, точно их выполнять и правомерно их использовать;

– знать степень важности проводимых работ, разрабатываемых и находящихся в работе документации и изделий, задачи и функциональные обязанности своих подчиненных;

– незамедлительно сообщать в службу безопасности изменения функциональных обязанностей сотрудников, не допуская адресования им документов и изделий до переоформления функциональных обязанностей в специальных решениях;

– не допускать со стороны подчиненных действий, влекущих за собой нарушение требований разрешительной системы, принимать меры к исключению неоправданного ознакомления с теми сведениями, которые не относятся к выполняемым обязанностям работника;

– осуществлять контроль за адресованием классифицированных документов и изделий, ознакомлением с ними командированных лиц.

Сотрудники службы безопасности предприятия (фирмы) должны контролировать:

– правомочность выдачи охраняемой информации и изделий сотрудникам предприятия и командированным лицам;

– правомерность адресования классифицированных документов и изделий из одного подразделения в другое;

– порядок оформления на доступ к коммерческой тайне фирмы.

В положении о разрешительной системе фирмы необходимо указать, что передача классифицированных документов и изделий от исполнителя к исполнителю возможна только в пределах структурного подразделения и с разрешения его руководителя. Передача, возврат таких документов и изделий производятся в установленном на предприятии порядке и только в интервале рабочего времени данного дня.

Вся классифицированная документация и изделия, поступившие на предприятие или разработанные на предприятии, принимаются и учитываются сотрудниками службы безопасности. После регистрации документация передается на рассмотрение руководителю предприятия под расписку. Указанные руководители могут передавать документы и изделия на исполнение только через службу безопасности после их регистрации.

Предварительное рассмотрение оперативной переписки, оценка степени важности изделий осуществляются начальником (либо специально выделенным референтом руководителя фирмы), который определяет необходимость доклада полученной информации руководителю фирмы. Документы и изделия, не требующие обязательного рассмотрения руководителем фирмы, предоставляются другим руководителям или начальникам структурных подразделений. Рассмотренные руководителем фирмы входящие и внутреннего исполнения документы и изделия адресуются соответствующим руководителям и исполнителям структурных подразделений фирмы. Начальники структурных подразделений, которым адресованы документы и изделия вышестоящими руководителями, дают письменное разрешение на самих документах (сопроводительных листах к изделиям) соответствующим подчиненным им исполнителям. Контроль за правильностью адресования документов и изделий осуществляется руководством подразделения экономической безопасности.

Переадресование классифицированных документов и изделий производится руководителями фирмы, указанными в разрешительной системе, начальниками структурных подразделений — в пределах своего подразделения. В случае несоответствия назначенного документа и изделия функциональным обязанностям исполнителя вопрос решается на соответствующем уровне с участием службы безопасности.

Командированные лица могут быть допущены к закрытым сведениям и изделиям только с разрешения руководителя фирмы или его заместителей, которым такое право передано. Разрешение на доступ дается письменно. Письменное разрешение должно четко определять объем коммерческой тайны и круг вопросов, по которым можно предоставлять информацию. В разрешении в обязательном порядке указывается должностное лицо фирмы, ответственное за работу с командированными.

В карточке о допуске командированного руководитель должен указать, какие объекты, службы, помещения имеет право посетить командированный.

Командированный может присутствовать на совещаниях, советах только по тем вопросам, которые определены руководством фирмы.

В положении о разрешительной системе целесообразно указать, что служебные совещания по закрытым вопросам проводятся только с разрешения руководителя фирмы или его заместителей. Особые требования могут распространяться на заседания ученых советов, совещания по рассмотрению результатов НИОКР, финансово-коммерческой деятельности и т. п. На подобные мероприятия рекомендуется в обязательном порядке составлять разрешительные списки и включать в них только тех сотрудников предприятия, которые имеют непосредственное отношение к планируемым мероприятиям и чье участие вызывается служебной необходимостью.

Как отмечалось выше, сотрудники других фирм могут участвовать в закрытых совещаниях только с персонального разрешения руководства фирмы. Готовит списки, как правило, ответственный за организацию совещания в контакте с заинтересованными руководителями структурных подразделений. Список является основанием для организации контроля за допуском на данное совещание. Перед началом совещания сотрудник службы безопасности может предупредить присутствующих, что подлежащая обсуждению информация носит закрытый характер и не подлежит распространению за пределы установленной фирмой сферы обращения, определяет порядок ведения записей.

Важно подчеркнуть, что установление внутри фирмы определенного порядка обращения с закрытой информацией и изделиями существенным образом повышает надежность защиты коммерческой тайны, снижает вероятность разглашения, утраты носителей этих сведений.

Статья 12. Режим коммерческой тайны

1. Порядок защиты коммерческой тайны в соответствии с настоящим Законом определяется хозяйствующим субъектом или назначенным им руководителем, который доводит его до работников, имеющих доступ к сведениям, составляющим коммерческую тайну.

2. Меры по охране коммерческой тайны, принимаемые ее обладателем, должны включать в себя:

а) определение перечня информации, составляющей коммерческую тайну;

б) ограничение доступа к коммерческой тайне путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

в) учет лиц, получивших доступ к коммерческой тайне, и (или) лиц, которым эта информация была предоставлена или передана;

г) регулирование отношений по использованию коммерческой тайны работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

д) нанесение на материальные носители (документы), содержащие коммерческую тайну, грифа «Коммерческая тайна» с указанием обладателя этой информации (для юридических лиц – полное наименование и ме-

сто нахождения, для индивидуальных предпринимателей – фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

3. Режим коммерческой тайны считается установленным после принятия обладателем коммерческой тайны мер, указанных в пункте 2 настоящей статьи.

4. Индивидуальный предприниматель, являющийся обладателем коммерческой тайны и не имеющий работников, с которыми заключены трудовые договоры, принимает меры по охране коммерческой тайны, указанные в пункте 2 настоящей статьи, за исключением подпунктов «а» и «б», а также положений подпункта «г», касающихся регулирования трудовых отношений.

5. Наряду с мерами, указанными в пункте 2 настоящей статьи, обладатель коммерческой тайны вправе применять при необходимости средства и методы технической защиты коммерческой тайны, другие не противоречащие законодательству государства-участника меры.

6. Меры по охране коммерческой тайны признаются разумно достаточными, если:

а) исключается доступ к коммерческой тайне любых лиц без согласия ее обладателя;

б) обеспечивается возможность использования коммерческой тайны работниками и передачи ее контрагентам без нарушения режима коммерческой тайны.

7. Режим коммерческой тайны не может быть использован в целях, противоречащих требованиям защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны и безопасности государства-участника.

8. Государство содействует хозяйствующему субъекту в создании необходимых условий для обеспечения сохранности коммерческой тайны.

Комментарий к статье 12

Режим коммерческой тайны – это меры по охране конфиденциальности информации, составляющей коммерческую тайну.

Данные меры принято делить на правовые, организационные и технические, которые тесно взаимосвязаны между собой. Более того, большинство превентивных мер изначально включают в себя и правовую, и организационную, и техническую составляющие. Чтобы воплотить в жизнь какое-либо техническое решение в области безопасности на предприятии (например, внедрить систему шифрования в корпоративную информационную сеть), необходимо сначала найти ему юридическое обоснование, собрать необходимые разрешения на проведение соответствующих работ (если они требуют лицензирования или прохождения иных процедур, предусмотренных законодательством), продумать возможные последствия такого внедрения (например, возможность нарушения конституционных и иных прав сотрудников). Затем нужно разработать ряд внутрифирменных инструкций (положений, приказов) и провести полномас-

штабное обучение персонала компании. Другими словами, во исполнение одной технической меры необходимо принять множество мер юридического и организационного характера. Точно так же во исполнение одной меры безопасности организационного плана, например усиления режима доступа на объект или организации системы фиксирования посещений этого объекта, необходимо внедрить различные технические (электронные) устройства, и это должно быть сделано грамотно не только технически, но и юридически.

Проиллюстрируем сказанное на примере таблицы мер по защите документации, предложенной Э. Я. Соловьевым[*]:

Меры по защите документации

Организационные меры	**Технические меры**	**Специальные меры**
Работа с людьми	Установка сигнализации и контроль за ее работой	Применение средств защиты от копирования документов
Контроль режима защиты документов	Использование специальных замков и других средств	Применение устройств скрытого фиксирования незаконного доступа к документам
Определение формы и содержания документов	Использование устройств для уничтожения документов	Защита от промышленного шпионажа
Классификация и простановка грифа	Обеспечение сотрудников сейфами и специальными контейнерами для хранения документов	Проведение служебного расследования при утере документов

Каждая из перечисленных мер сама по себе достаточно емкая и может включать в себя множество более простых по содержанию мер, за счет которых она и реализуется. Однако такие категории, например, как «работа с людьми» и, тем более, «защита от промышленного шпионажа», вообще некорректно именовать мерами, поскольку одна такая «мера» может включать в себя абсолютно все охранные мероприятия, проводимые в организации (и не только в отношении доступа к информации, составляющей коммерческую тайну).

[*] Соловьев Э. Я. Коммерческая тайна и ее защита. М.: Ось-89, 2001. С. 23

Технические меры охраны конфиденциальности информации с течением времени приобретают все большее значение. Большинство предприятий, организаций и учреждений имеют доступ к Интернету, который, являясь открытой информационной средой, предоставляет широкие возможности для различных злоумышленных действий в отношении информации и объектов интеллектуальной собственности, таких, например, как интернет-сайты и программное обеспечение.

В настоящее время одной из наиболее актуальных угроз в области информационной безопасности является утечка конфиденциальных данных от несанкционированных действий пользователей. Это обусловлено тем, что большая часть традиционных средств защиты, таких как антивирусы, межсетевые экраны и системы аутентификации, не способны обеспечить эффективную защиту от внутренних нарушителей. Целью такого рода нарушителей (инсайдеров) является передача информации за пределы компании для ее последующего несанкционированного использования – продажи, опубликования в открытом доступе и т. д. Системы DLP – это технологии, позволяющие предотвратить утечку конфиденциальной информации. В течение последних нескольких лет использовалась обширная терминология: Information Leakage Protection (ILP), Information Leak Protection (ILP), Information Leakage Detection & Prevention (ILDP), Content Monitoring and Filtering (CMF), Extrusion Prevention System (EPS) и др. Но окончательным и наиболее точным термином принято считать Data Leak Prevention (DLP, предложен агентством Forrester в 2005 году). В качестве русского аналога принято словосочетание «системы защиты конфиденциальных данных от внутренних угроз». При этом под внутренними угрозами подразумевают как умышленные, так и непреднамеренные злоупотребления сотрудниками своими правами доступа к данным. В рамках создания таких систем решаются задачи предотвращения утечек конфиденциальной информации по основным каналам передачи даннях: исходящий вебтрафик (HTTP, FTP, P2P и др.); исходящая электронная почта; внутренняя электронная почта; системы мгновенного обмена сообщениями; сетевая и локальная печать; контроля доступа к устройствам и портам ввода-вывода, к которым относятся дисководы, CD-ROM, USB-устройства, инфракрасные, принтерные (LPT) и модемные (COM) порты.

Как показывают опубликованные данные опроса Deloitte ведущих мировых финансовых компаний, 49% респондентов зафиксировали внутренние инциденты (связанные с IT-безопасностью). В 31% случаев инсайдеры занесли вирусы изнутри корпоративной сети, а с инсайдерским мошенничеством столкнулись 28% респондентов; 18% организаций стали жертвами утечки приватной информации клиентов, а 10% обнаружили, что инсайдеры скомпрометировали корпоративную сеть. Организации, которые пострадали от внутренней утечки, признаются, что большая доля угроз является следствием безалаберности или халатности служащих (человеческий фактор – 42%, операционные ошибки – 37%), а не злого умысла инсайдеров. Правда, 28% стали жертвой тщательно продуманного и профессионального мошенничества, а 18% компаний лишились приватной информации клиентов именно из-за того, что инсайдеры целе-

направленно допустили утечку. Чтобы не допустить такие инциденты в будущем, 80% опрошенных финансовых компаний осуществляют мониторинг действий служащих, а 75% вводят различные ограничительные меры на использование тех или иных технологий либо устройств. По данным исследовательского центра компании InfoWatch, специализирующейся на производстве и продаже систем DLP, 42% утечек информации происходит неумышленно по неаккуратности или забывчивости пользователей, вследствие нарушений политики корпоративной безопасности организации. Более 40% информации уходит по интернет-каналам, 30% – по мобильным устройствам. Свыше 65% информации утекает из коммерческих предприятий, около 20% из образовательных и 24% из государственных предприятий.

Информация является одним из важнейших элементов управления деятельностью любого предприятия. В условиях рынка от наличия информации в значительной степени зависит успех предпринимательской деятельности. На сегодняшний день организации нередко сталкиваются с проблемой утечки информации и необходимостью построения системы защиты коммерческой тайны. Создание такой системы – сложный и многоплановый процесс, который затрагивает все структурные подразделения организации, в том числе отдел кадров. Система защиты коммерческой тайны создается в целях: достижения устойчивых позиций в условиях конкурентной борьбы на рынке товаров и услуг; сохранения конфиденциальной информации в течение определенного промежутка времени; получения возможности проверить каждый из вероятных каналов утечки информации; предотвращения негативных последствий текучести кадров.

По мере функционирования предприятия накапливается определенный объем информации, разглашение которой, в том числе самими работниками, способно ухудшить его экономическое положение. В связи с этим собственник информации вправе придать ей статус охраняемой путем отнесения к коммерческой тайне и тем самым закрыть свободный доступ к ней на законном основании. Лишь сохранение этой информации в тайне придает ей коммерческую ценность.

Практикой выработаны рекомендации, которые могут быть полезны предприятию, решающему проблему сохранности своей коммерческой информации. При вводе системы защиты информации, возлагая на работников соответствующие обязанности и ответственность, необходимо учитывать требования закона.

В соответствии с действующим законодательством разработка и реализация практических мер по организации защиты коммерческой тайны возлагается на ее собственника, который должен разработать систему защиты сведений, составляющих коммерческую тайну, и обеспечить ее эффективное функционирование. Предприятие создает систему защиты имеющейся у него конфиденциальной информации самостоятельно, опираясь на действующее законодательство, с учетом размера данного предприятия, типа используемой технологии, характера коммерческой деятельности и деловой информации, возможных ка-

налов утечки информации, исходя из имеющихся в наличии средств и своих финансовых возможностей.

Разрабатывая систему защиты коммерческой тайны, необходимо прежде всего конкретизировать объект, предмет и цели защиты коммерческой информации на предприятии. Объектом защиты информации являются сведения различных категорий, собранные в процессе деятельности предприятия, к которым может проявить интерес его конкурент. Предметом защиты информации являются носители информации, на которых зафиксированы, отображены защищаемые сведения: документы, изделия, материалы, предметы, вещества. В качестве носителя защищаемой информации выступает также человек. Именно на охрану носителей засекреченной информации и направлены главным образом усилия предприятия.

Основная цель функционирования системы защиты коммерческой тайны – установить оптимальный режим работы предприятия с таким расчетом, чтобы ограничить распространение сведений, содержащих коммерческую тайну, сделать эти сведения недоступными для посторонних лиц, предотвратить их утечку и создать необходимые условия работы лицам, имеющим к ним законный доступ. Именно поэтому участие в данном процессе специалистов отдела кадров обязательно.

На первом заседании экспертной комиссии организации следует выработать план действий по созданию системы защиты коммерческой тайны в организации:

1) определить, какие категории сведений являются коммерческой тайной организации;

2) установить места накопления такой информации и их носители, выявить потенциальные каналы утечки информации;

3) отработать систему доступа к сведениям, составляющим коммерческую тайну;

4) предусмотреть вопросы защиты коммерческой тайны в ходе внешних контактов работников организации;

5) распределить функции по созданию системы защиты между структурными подразделениями;

6) определить примерный объем затрат на создание системы защиты коммерческой тайны;

7) разработать порядок проведения контроля за функционированием всей системы в целом.

Проблема засекречивания информации и определения степени секретности сведений является одной из стержневых во всей деятельности по защите информации. Именно поэтому на первом этапе должна быть проведена работа по определению информации, являющейся коммерческой тайной организации. Вопрос об отнесении сведений к категории коммерческой тайны можно решить на основе следующих критериев: оценка возможного ущерба предприятию при разглашении (утечке) таких сведений (утрата предприятием своего выгодного положения на рынке; осложнение отношений с деловыми партнерами, клиен-

тами и т. д.); учет всех ограничений на засекречивание информации, вводимых законодательством государства-участника.

Экспертная комиссия организации должна выяснить два обстоятельства: 1) имеются ли у фирмы достижения в сфере маркетинговых разработок, организации труда, торговых отношений и другие, которые дают ей преимущества в конкурентной борьбе; 2) утратит ли она эти преимущества, если сведения о ее достижениях станут известны конкурентам и будут использованы ими.

При положительном ответе на оба вопроса комиссия должна внести предложение об отнесении данных сведений к коммерческой тайне.

В таблице были выделены категории информации, подлежащей защите и, следовательно, засекречиванию, и определены сроки ограничения доступа к такой информации.

Категории информации, подлежащей защите

Категория информации	**Сведения, составляющие данную категорию информации**	**Предполагаемые последствия разглашения данных сведений**	**Срок установления ограничения доступа к информации**
Строго конфиденциальная информация	Состояние рынка сбыта	Возможное банкротство организации	Не ограничен
Конфиденциальная информация	Сведения о перспективах развития организации, клиентах, сроках и суммах кредитования	Возможное лишение организации устойчивой прибыли на какое-либо время	3 года
Тайна фирмы	Адреса и телефоны руководителей и работников, текущие планы работы	Неблагоприятные последствия, не оказывающие существенного влияния на работу организации	1 год

Остальные сведения отнесены к открытым.

Во избежание лишних затрат на обеспечение режима защиты коммерческой тайны целесообразно периодически (один раз в год) пересматривать обоснованность охраны конфиденциальности конкретных сведений. Основанием для отмены мер, ограничивающих свободный доступ к информации, могут быть изменения объективных обстоятельств, вследствие которых дальнейшая защита указанных сведений становится нецелесообразной. Правовое обеспечение деятельности организации по защите коммерческой тайны рекомендуется начинать с подготовки и создания организационно-распорядительных докумен-

тов. Следует отметить, что система правовой регламентации защиты конфиденциальной информации на предприятии всегда является двухуровневой.

Двухуровневая система правовой регламентации защиты информации

Уровень	Вид документа	Содержание
1	Законодательные акты государства-участника	Нормы, регламентирующие деятельность организаций по защите коммерческой тайны; нормы, определяющие объем прав и обязанностей в этой области
2	Локальные нормативные акты организации (устав, коллективный договор, правила внутреннего трудового распорядка, инструкции, положения о подразделениях и др.)	Локальные нормы, определяющие механизм защиты коммерческой тайны в конкретной организации

На законодательном уровне установлен ряд ограничений на право собственника владеть, пользоваться и распоряжаться имеющейся у него информацией. Так, установлен перечень сведений, которые не могут составлять коммерческую тайну. К таким сведениям, в частности, относятся: учредительные документы и устав предприятия или учреждения; документы, дающие право заниматься предпринимательской деятельностью; сведения по установленным формам отчетности о финансово-хозяйственной деятельности и иные сведения, необходимые для проверки правильности исчисления и уплаты налогов; сведения о численности и составе работающих, их заработной плате и условиях труда, а также о наличии свободных рабочих мест; документы об уплате налогов и обязательных платежах; сведения о загрязнении окружающей среды, нарушении антимонопольного законодательства, несоблюдении безопасности условий труда, а также о других нарушениях законодательства.

В процессе обмена информацией с государственными структурами субъекты хозяйственной деятельности нередко вынуждены сообщать по требованию их представителей сведения, выходящие за пределы указанного выше перечня и составляющие коммерческую тайну предприятия. Такая информация охраняется как совместная собственность государственных органов и представивших ее хозяйствующих субъектов. Ответственность за ее сохранность в государственных учреждениях несут государственные служащие.

При составлении перечня сведений, которые могут составлять коммерческую тайну, может возникнуть сложность, так как методика отнесения тех или иных сведений к коммерческой тайне в государствах-участниках еще не разработана. Отсюда следует, что любая информация, за исключением отмеченной

выше, представляющая для субъектов предпринимательской деятельности интерес с точки зрения получения прибыли от ее использования, может быть отнесена ими к коммерческой тайне и, следовательно, может подлежать защите.

На каждом предприятии в качестве коммерческой тайны засекречивается различная информация. Однако можно выделить основной перечень сведений, обеспечивающих любой фирме преимущества в конкурентной борьбе.

Перечень сведений, защита которых влияет на конкурентоспособность фирмы

Сфера интересов	Перечень сведений
Административная деятельность	Предмет совещаний органов управления, перечень представителей и посредников организации, методы организации труда, отбора и подготовки персонала фирмы
Производственная деятельность	Технология изготовления продукции, данные о разработке новых и модернизации ранее известных технологических процессов, выявленные недостатки выпускаемой продукции и намеченные пути их устранения, характер и цели проводимых исследовательских работ, результаты проведенных испытаний, планируемые изменения номенклатуры, объема и качества выпускаемой продукции, планы развития фирмы и привлечения инвестиций
Коммерческая стратегия	Бюджет организации, новые маркетинговые проекты, состояние рынка сбыта
Финансовая сфера	Источники финансирования, финансовая устойчивость организации, размеры и условия банковских кредитов, состояние материально-технической базы организации
Торговая сфера	Структура цен на выпускаемую продукцию, планируемые закупки и размер выделенных на них средств, факты ведения переговоров с целью заключения договора, размер предоставляемых скидок, кредитные условия и условия платежа и др.

В перечне должны быть перечислены категории сведений, имеющих особую ценность для деятельности организации, с разбивкой по сферам обращения и, соответственно, по структурным подразделениям. В связи с тем что информация, подлежащая оценке, постоянно обновляется, в перечне должны быть указаны критерии отнесения сведений к коммерческой тайне фирмы. При подготовке перечня следует установить степень конфиденциальности каждой группы коммерческой информации, примерные сроки, на которые она засекречивается, а также условия, с наступлением которых информация рассекречивается. Перечень подлежит периодическому пересмотру в целях исключения из него сведений, утративших коммерческую ценность, и включения новых, а также изменения при необходимости степени секретности.

Перечень утверждается руководителем фирмы и доводится начальниками структурных подразделений в индивидуальном порядке под роспись до всех работников в части, их касающейся. При установлении системы защиты информации базовым локальным нормативным документом должно быть положение о коммерческой тайне организации, устанавливающее порядок организации работы с коммерческой тайной, регламентирующее основные направления деятельности, механизм защиты конфиденциальной информации, закрепляющее права и обязанности работников, которые могут возникнуть в связи с их допуском к коммерческой тайне, а также объем их ответственности. Один из самостоятельных разделов Положения целесообразно посвятить участию структурных подразделений в создании системы защиты сведений, составляющих коммерческую тайну.

Статья 13. Охрана коммерческой тайны в рамках трудовых отношений

1. В целях охраны коммерческой тайны работодатель обязан:

а) ознакомить под расписку работника, доступ которого к коммерческой тайне необходим для выполнения им своих трудовых обязанностей, с перечнем информации, составляющей коммерческую тайну, обладателями которой являются работодатель и его контрагенты;

б) ознакомить под расписку работника с установленным работодателем режимом коммерческой тайны и с мерами ответственности за его нарушение;

в) создать работнику необходимые условия для соблюдения им установленного работодателем режима коммерческой тайны.

2. Доступ работника к коммерческой тайне осуществляется с его согласия, если это не предусмотрено его трудовыми обязанностями.

3. В целях охраны коммерческой тайны работник обязан:

а) выполнять установленный работодателем режим коммерческой тайны;

б) не разглашать коммерческую тайну, обладателями которой являются работодатель и его контрагенты, и без их согласия не использовать эту информацию в личных целях;

в) не разглашать коммерческую тайну, обладателями которой являются работодатель и его контрагенты, после прекращения трудового договора в течение срока, предусмотренного соглашением между работником и работодателем, заключенным в период срока действия трудового договора, или в течение трех лет после прекращения трудового договора, если указанное соглашение не заключалось;

г) возместить причиненный работодателю ущерб, если работник виновен в разглашении коммерческой тайны, ставшей ему известной в связи с исполнением им трудовых обязанностей;

д) передать работодателю при прекращении или расторжении трудового договора имеющиеся в пользовании работника материальные носители информации, содержащие коммерческую тайну.

4. Работодатель вправе потребовать возмещения причиненных убытков лицом, прекратившим с ним трудовые отношения, в случае, если это лицо виновно в разглашении коммерческой тайны, доступ к которой это лицо получило в связи с исполнением им трудовых обязанностей, и если разглашение такой информации последовало в течение срока, установленного в соответствии с подпунктом «в» пункта 3 настоящей статьи.

5. Причиненные ущерб либо убытки не возмещаются работником или прекратившим трудовые отношения лицом, если разглашение коммерческой тайны явилось следствием непреодолимой силы, крайней необходимости или неисполнения работодателем обязанности по обеспечению режима коммерческой тайны.

6. Трудовым договором с руководителем организации должны предусматриваться его обязательства по обеспечению охраны коммерческой тайны, обладателем которой являются организация и ее контрагенты, и ответственность за обеспечение охраны ее конфиденциальности.

7. Руководитель организации возмещает организации убытки, причиненные его виновными действиями в связи с нарушением законодательства государства-участника о коммерческой тайне. При этом убытки определяются в соответствии с гражданским законодательством государства-участника.

8. Работник имеет право обжаловать в судебном порядке незаконное установление режима коммерческой тайны в отношении информации, к которой он получил доступ в связи с исполнением им трудовых обязанностей.

Комментарий к статье 13

1. Статья регулирует некоторые вопросы, возникающие по поводу использования информации, составляющей коммерческую тайну, в трудовых отношениях.

Как показывает практика, в условиях глобальной компьютеризации наибольшую угрозу утечки конфиденциальной информации (в том числе информации, составляющей коммерческую тайну) представляет не стремительный рост числа компьютерных вирусов и хакеров, а действия персонала, как

умышленные, так и неосторожные. Человек остается самым слабым звеном в системе информационной безопасности. Известна статистика (данные Интерпола), согласно которой 25% служащих фирмы готовы продать ее секреты в любое время кому угодно, 50% идут на это в зависимости от обстоятельств и только 25% являются патриотами своего предприятия.

Законодательство об охране коммерческой тайны направлено на обеспечение баланса между различными вариантами политики в области конкуренции. С одной стороны, необходимо поощрять инновации и творчество и обеспечить охрану компаниям, инвестирующим средства в инновационную и творческую деятельность. С другой – необходимо поощрять здоровую конкуренцию и свободу занятости. О сложности таких разных и нередко конфликтующих политических подходов свидетельствует применение в странах общего права «доктрины неизбежного раскрытия» и «доктрины трамплина».

«Доктрина неизбежного раскрытия» возникла в связи с необходимостью решения проблемы перехода работников в другие похожие компании. Ее основной принцип заключается в том, что работники, которые имели доступ к конфиденциальной информации, неизбежно раскроют эту информацию будущему работодателю, если последний осуществляет свою деятельность в той же области. Из доктрины следует, что даже если работник руководствуется благими намерениями, он автоматически или инстинктивно передаст приобретенную на прежнем месте информацию, навыки и знания своему следующему работодателю, если последний осуществляет деятельность в той же отрасли. С другой стороны, обществу необходимо охранять конфиденциальную информацию своих предприятий, однако оно не может ограничить свободу занятости своих членов.

Судебные решения в этой сфере зависят от фактов и обстоятельств каждого конкретного спора. Как правило, судебный запрет на переход работника в другую компанию выносится в случае, если устанавливается, что существует высокая вероятность передачи бывшим работником новому работодателю информации, которая не является широко известной или не может быть легко «выведенной» конкурентами в соответствующей области. Необходимо проводить разграничение между конкретной конфиденциальной информацией и обычными навыками и знаниями, которые работник приобрел во время работы в своей прежней компании. Он не может быть лишен возможности использовать такие полученные навыки и знания.

«Доктрина трамплина» применяется с целью помешать работнику, который во время работы у бывшего работодателя мог иметь доступ к конфиденциальной информации, использовать такую информацию в своих собственных интересах и тем самым получить необоснованное преимущество по отношению к бывшему работодателю.

Доктрина трамплина также может применяться, даже если соответствующая информация уже перешла в сферу общественного достояния, с тем, чтобы запретить бывшему работнику, который приобрел у бывшего работодателя конкретные производственные знания (технические навыки), использовать эти знания (навыки) для производства конкурирующего продукта. Это обусловлено

тем, что такие знания дали бы бывшему работнику «несправедливую фору» по отношению к тем, кто имеет доступ к опубликованной информации.

Однако добиться установления судебного запрета не просто, поскольку вопрос о конфиденциальности имеет сложный характер: трудно четко определить и разграничить знания, которые работник уже имел на момент прихода в компанию, и знания, которые он получил во время работы в ней.

В последние несколько десятилетий произошли изменения в условиях труда и, как следствие, в степени лояльности работника, что повысило вероятность нарушения психологического договора. Лояльность сотрудников к своему работодателю зависит от размеров предприятия. Статистические данные свидетельствуют о том, что почти 80% работников малых и средних предприятий лояльны к своим предприятиям, тогда как в крупных компаниях этот показатель составляет менее 50%.

Поэтому необходимо обратить большее внимание на проблему повышения лояльности работников как одного из средств обеспечения охраны коммерческой тайны. От этого работодатель только выиграет, поскольку принятие соответствующих мер позволит повысить производительность и – что еще важнее – закрепить кадры, уменьшить их текучесть и благодаря этому свести к минимуму риск разглашения коммерческой тайны.

В литературе отмечается, что менее всего от утечки информации страдает японский бизнес. Причина этого кроется в устоявшихся веками традициях управления, в том числе в системе так называемого пожизненного найма. Японским работодателям, пожалуй, пока лучше всех в мире удается воспитывать в сотрудниках чувство преданности своей организации. Многие национальные компании активно перенимают опыт зарубежных коллег, внедряя и развивая системы мотивации и адаптации, в том числе пытаются разрабатывать так называемую политику карьерного роста (ступенчатое продвижение по службе). Однако общий уровень кадрового менеджмента можно оценить лишь как «удовлетворительный». Поэтому введение в национальное законодательство положений, касающихся обеспечения режима коммерческой тайны в трудовых правоотношениях, представляется отнюдь не лишним. При этом законодателя трудно обвинить в какой-либо предвзятости относительно установления прав и обязанностей сторон трудового договора, т. е. в лоббировании чьих-то интересов, что очень важно.

Пункт 1 комментируемой статьи устанавливает три непременных обязанности работодателя, которые он должен выполнить в целях охраны конфиденциальности информации, составляющей его коммерческую тайну.

В пункте 3 предусмотрены обязанности работника, использующего при осуществлении своих трудовых функций информацию, составляющую коммерческую тайну работодателя или его контрагентов, в том числе не разглашать указанную информацию после прекращения трудового договора в течение срока, предусмотренного соглашением между работником и работодателем. Данное соглашение о неразглашении может быть заключено между сторонами трудовых правоотношений только в период действия трудового договора, т. е. не

перед его заключением и не после увольнения сотрудника (до осуществления окончательного расчета с ним, как это часто бывает на практике).

Закон не устанавливает временных рамок исполнения обязательства о неразглашении, которое принимает на себя работник в соответствии с указанным соглашением. Заметим, что речь идет именно о соглашении, т. е. работник вправе отказаться от его подписания. Если такое соглашение сторонами не заключено (из-за отказа работника или по иным причинам), то действует императивная норма Закона, согласно которой работник обязан соблюдать режим коммерческой тайны в течение трех лет с момента прекращения трудовых отношений с ним.

2. Если работник в период действия трудового договора или в нарушение сроков неразглашения, установленных в соглашении с работодателем (или, при отсутствии такого соглашения, в течение трех лет с момента прекращения трудового договора), разгласил информацию, составляющую коммерческую тайну работодателя (его контрагентов), то работодатель вправе потребовать возмещения работником причиненных убытков, но при условии вины работника в разглашении данной информации.

Отсутствие вины доказывается лицом, нарушившим обязательство. Лицо признается невиновным, если при той степени заботливости и осмотрительности, какая от него требовалась по характеру обязательства и условиям оборота, оно приняло все меры для надлежащего исполнения обязательства.

Отметим, что обязанность не разглашать и не использовать конфиденциальную информацию работодателя в иных целях, не связанных с выполнением трудовых функций или заданий работодателя, не входит в перечень основных обязанностей работника, который приводится в трудовом кодексе, но включение такой обязанности в трудовой договор допускается. В любом случае работник обязан соблюдать правила внутреннего трудового распорядка организации и добросовестно исполнять трудовые обязанности, возложенные на него трудовым договором.

Правила внутреннего трудового распорядка организации – это локальный нормативный акт, регламентирующий в соответствии с Трудовым кодексом и иными законами порядок приема и увольнения работников, основные права, обязанности и ответственность сторон трудового договора, режим работы, время отдыха, применяемые к работникам меры поощрения и взыскания, а также иные вопросы регулирования трудовых отношений в организации. В нем, равно как и в трудовом договоре, может быть предусмотрен порядок использования информации, составляющей коммерческую тайну работодателя, работниками в процессе выполнения их трудовых функций.

Однократное грубое нарушение работником трудовых обязанностей в виде разглашения конфиденциальной информации является основанием для расторжения трудового договора по инициативе работодателя, а также одним из случаев, когда на работника может быть возложена материальная ответственность в полном размере причиненного ущерба.

Работник обязан возместить работодателю причиненный ему прямой действительный ущерб, а также ущерб, возникший у работодателя в результате

возмещения им ущерба иным лицам (например, контрагентам, доверившим работодателю свою информацию, составляющую коммерческую тайну, в соответствии с гражданско-правовыми договорами). Неполученные доходы (упущенная выгода) взысканию с работника не подлежат.

Работник, виновный в причинении ущерба работодателю, может добровольно возместить его полностью или частично. По соглашению сторон трудового договора допускается возмещение ущерба с рассрочкой платежа. В этом случае работник представляет работодателю письменное обязательство о возмещении ущерба с указанием конкретных сроков платежей. В случае увольнения работника, который дал письменное обязательство о добровольном возмещении ущерба, но отказался возместить указанный ущерб, непогашенная задолженность взыскивается в судебном порядке.

Возмещение ущерба производится работником независимо от его привлечения к дисциплинарной, административной или уголовной ответственности за действия или бездействие, которыми причинен ущерб работодателю.

3. Если разглашение работником информации, составляющей коммерческую тайну работодателя (его контрагентов), явилось следствием неисполнения работодателем обязанности по обеспечению режима коммерческой тайны, то убытки, причиненные разглашением этой информации, работником не возмещаются, равно как и в случае, если разглашение конфиденциальной информации явилось следствием непреодолимой силы или крайней необходимости.

Под «непреодолимой силой» понимаются чрезвычайные и непредотвратимые при данных условиях обстоятельства, к которым не относятся, в частности, нарушение обязанностей со стороны контрагентов должника, отсутствие на рынке нужных для исполнения товаров, отсутствие у должника необходимых денежных средств.

Вред, причиненный в состоянии крайней необходимости, т. е. для устранения опасности, угрожающей самому причинителю вреда или другим лицам, если эта опасность при данных обстоятельствах не могла быть устранена иными средствами, должен быть возмещен лицом, причинившим вред. Учитывая обстоятельства, при которых был причинен такой вред, суд может возложить обязанность его возмещения на третье лицо, в интересах которого действовал причинивший вред, либо освободить от возмещения вреда полностью или частично как это третье лицо, так и причинившего вред.

4. Пункты 6 и 7 комментируемой статьи регулируют вопросы обеспечения конфиденциальности информации в отношениях между организацией и ее руководителем.

Руководитель организации – это физическое лицо, которое в соответствии с законом или учредительными документами организации осуществляет руководство этой организацией, в том числе выполняет функции ее единоличного исполнительного органа.

Комментируемая статья предусматривает необходимость включения в трудовой договор с руководителем организации его обязательств по обеспечению охраны конфиденциальности информации, обладателями которой являют-

ся организация и ее контрагенты, а также ответственность за обеспечение охраны ее конфиденциальности.

В случаях, предусмотренных законом, руководитель организации возмещает организации убытки, причиненные его виновными действиями. Такой случай как раз предусмотрен пунктом 7 комментируемой статьи Закона: руководитель организации возмещает организации убытки, причиненные его виновными действиями в связи с нарушением законодательства о коммерческой тайне.

Руководитель организации несет полную материальную ответственность за прямой действительный ущерб, причиненный организации. Расчет убытков осуществляется в соответствии с нормами, предусмотренными гражданским законодательством государства-участника.

5. Наибольшая сложность обеспечения режима коммерческой тайны в процессе трудовых взаимоотношений заключается в создании таких условий, при которых превентивные меры по обеспечению конфиденциальности производственной и иной информации не препятствовали бы полноценной работе сотрудников и нормальному течению бизнес-процессов компании. В этом деле работодателю предоставляется «свобода творчества». Главное – чтобы принимаемые им меры соответствовали законодательству. Часть 8 комментируемой статьи предусматривает право работника обжаловать в судебном порядке незаконное установление режима коммерческой тайны в отношении информации, к которой он получил доступ в связи с исполнением трудовых обязанностей.

Статья 14. Охрана коммерческой тайны в рамках гражданско-правовых отношений

1. Отношения между обладателем коммерческой тайны и его контрагентом в части, касающейся охраны коммерческой тайны, регулируются законом и договором.

2. В договоре должны быть определены условия охраны коммерческой тайны, в том числе в случае реорганизации или ликвидации одной из сторон договора в соответствии с гражданским законодательством, а также обязанность контрагента по возмещению убытков при разглашении им этой информации вопреки договору.

3. В случае если иное не установлено договором между обладателем коммерческой тайны и контрагентом, контрагент в соответствии с законодательством государства-участника самостоятельно определяет способы защиты коммерческой тайны, переданной ему по договору.

4. Контрагент обязан незамедлительно сообщить обладателю коммерческой тайны о допущенном контрагентом либо ставшем ему известным факте разглашения или угрозы разглашения, незаконного получения или незаконного использования коммерческой тайны третьими лицами.

5. Обладатель коммерческой тайны, переданной им контрагенту, до окончания срока действия договора не может разглашать коммерческую тайну, а также в одностороннем порядке прекращать охрану ее конфиденциальности, если иное не установлено договором.

6. Сторона, не обеспечившая в соответствии с условиями договора охрану коммерческой тайны, переданной по договору, обязана возместить другой стороне убытки, если иное не предусмотрено договором.

Комментарий к статье 14

1. По своей сути договорные отношения, связанные с информацией, составляющей коммерческую тайну, основаны не на акте передачи прав на использование данной информации (например, «прав на ноу-хау», как это часто формулируется в хозяйственных договорах). Поскольку содержание прав, возникающих в отношении результатов интеллектуальной деятельности, и информации, составляющей коммерческую тайну, далеко не равнозначно (в отношении информации не возникает исключительных прав, как уже отмечалось выше), договорные отношения между обладателем информации, составляющей коммерческую тайну, и его контрагентами строятся на раскрытии данной информации ее обладателем, в том числе посредством предоставления доступа к ней каким-либо способом, на определенных условиях.

Информация, составляющая коммерческую тайну, может передаваться как в рамках договоров коммерческой концессии (франчайзинг), так и на основе отдельных соглашений (лицензий). При этом стороны могут принимать на себя различные обязательства, во многом сходные с теми, что принимают на себя стороны договоров о передаче прав на объекты интеллектуальной собственности (исключительных прав).

Вместе с тем нельзя не признать, что владелец секрета может выдать лицензию на его использование третьим лицам – производителям в данной отрасли. Однако если каждая компания отрасли использует данный технологический процесс, то его нельзя не признать общеизвестным приемом производства.

Заключая большое количество договоров о передаче информации, составляющей коммерческую тайну (предоставлении доступа к ней), ее обладатель рискует не только быстро потерять контроль за этой информацией, поскольку отслеживать и пресекать случаи нарушения контрагентами принятых договорных обязательств с каждым разом будет все труднее, но и значительно ускорить момент ее перехода в «общественное достояние».

Согласно пункту 2 статьи 39 Соглашения ТРИПС именно известность информации широкому кругу специалистов, обычно работающих с подобной информацией, делает ее не конфиденциальной. Исходя из российского законодательства момент прекращения режима коммерческой тайны (независимо от воли обладателя информации) связан с фактом известности данной информации, составляющей коммерческую тайну, третьим лицам. Пока трудно прогнозировать, какими критериями оценки общеизвестности будет руководствоваться суд в случае возникновения соответствующего спора. Отсюда следует вывод: при заключении договоров о передаче ноу-хау или иной информации конфиденциального характера очень важно не переступить количественный предел таких заключенных договоров, при котором контрагенты, набрав некую критическую массу, обретают статус третьих лиц. Определять этот количественный

предел придется в каждом конкретном случае и, видимо, не без помощи судебных органов.

2. Пункт 2 комментируемой статьи говорит о необходимости включения в гражданско-правовой договор, заключаемый в отношении информации, составляющей коммерческую тайну:

условия охраны ее конфиденциальности, в том числе в случае реорганизации или ликвидации одной из сторон договора (обладателя конфиденциальной информации или его контрагента) в соответствии с гражданским законодательством;

обязанности контрагента по возмещению убытков при разглашении им этой информации вопреки договору.

3. Стороны гражданско-правового договора, заключенного в отношении информации, составляющей коммерческую тайну, могут предусмотреть в этом договоре конкретные превентивные меры, которые должны быть приняты контрагентом, получающим конфиденциальную информацию от ее обладателя, в целях обеспечения конфиденциальности данной информации.

Если указанные меры прямо не предусмотрены сторонами договора, то контрагент определяет способы обеспечения конфиденциальности информации, составляющей коммерческую тайну, полученной им по данному договору, самостоятельно, руководствуясь при этом законодательством.

4. Пункт 4 комментируемой статьи устанавливает непременные обязанности стороны гражданско-правового договора, т. е. контрагента, получившего на основании этого договора некую информацию, составляющую коммерческую тайну. Контрагент обязан незамедлительно сообщить обладателю информации, составляющей коммерческую тайну: о допущенном контрагентом разглашении или незаконном использовании данной информации; о ставшем ему известным факте разглашения или угрозы разглашения, незаконного получения или незаконного использования указанной информации третьими лицами.

Указанные обязанности возникают у контрагента в момент получения им информации, составляющей коммерческую тайну, от ее обладателя независимо от указания этих обязанностей в гражданско-правовом договоре.

5. В соответствии с диспозитивной нормой, установленной в пункте 5 комментируемой статьи, обладатель информации, составляющей коммерческую тайну, если данная информация была передана им контрагенту по гражданско-правовому договору, не вправе до окончания срока действия договора: разглашать эту информацию; в одностороннем порядке прекращать охрану конфиденциальности этой информации.

Вместе с тем в договоре стороны могут предусмотреть и иное, например договориться о каких-либо определенных случаях, когда обладатель передаваемой по договору информации вправе ее разглашать третьим лицам или прекращать охрану ее конфиденциальности без согласия своего контрагента.

6. Если иное не предусмотрено гражданско-правовым договором, то сторона, не обеспечившая в соответствии с его условиями охрану конфиденциальности информации, переданной по договору, обязана возместить другой стороне убытки, возникшие у последней в связи с таким необеспечением. Данная

обязанность по возмещению убытков относится к обеим сторонам договора: к обладателю информации, составляющей коммерческую тайну и передаваемой в рамках данного договора, и к его контрагенту.

Статья 15. Охрана коммерческой тайны при ее предоставлении

1. Органы государственной власти, иные государственные органы, органы местного самоуправления в соответствии с настоящим Законом и иными законами государства-участника обязаны создать условия, обеспечивающие охрану коммерческой тайны, предоставленной им юридическими лицами или индивидуальными предпринимателями.

2. Должностные лица органов государственной власти, иных государственных органов, органов местного самоуправления, государственные или муниципальные служащие указанных органов без согласия обладателя коммерческой тайны не вправе разглашать или передавать другим лицам, органам государственной власти, иным государственным органам, органам местного самоуправления ставшую известной им в силу выполнения должностных (служебных) обязанностей коммерческую тайну, за исключением случаев, предусмотренных настоящим Законом, а также не вправе использовать эту информацию в корыстных или иных личных целях.

3. В случае нарушения коммерческой тайны должностными лицами органов государственной власти, иных государственных органов, органов местного самоуправления, государственными и муниципальными служащими указанных органов эти лица несут ответственность в соответствии с законодательством государства-участника.

Комментарий к статье 15

1. Пункт 1 комментируемой статьи устанавливает обязанность государственных органов и органов местного самоуправления создать условия, обеспечивающие охрану конфиденциальности информации, предоставленной им юридическими лицами или индивидуальными предпринимателями.

Помимо данной обязанности государство выполняет также и другие функции по регулированию и обеспечению информационных отношений, предусмотренные другими нормативными правовыми актами.

Основными направлениями государственной политики в сфере информатизации являются в том числе: обеспечение условий для развития и защиты всех форм собственности на информационные ресурсы; создание и совершенствование системы привлечения инвестиций и механизма стимулирования разработки и реализации проектов информатизации; развитие законодательства в сфере информационных процессов, информатизации и защиты информации.

Таким образом, государство призвано создавать условия для деятельности субъектов информационных отношений, во-первых, посредством юридических мер – создания необходимой нормативной базы (разработка и принятие законодательных актов, стандартов, инструкций, классификаторов и т. д.). Во-вторых, посредством мер организационного характера и инвестирования. По-

следнее подразумевает как привлечение инвестиций в рассматриваемую сферу, так и вливание в нее бюджетных средств. Государство может выступать инициатором конкурсов на выполнение научно-исследовательских и опытно-конструкторских работ, предметом которых могут быть в том числе исследования в области безопасности информации, создание новых технических и иных преград для негласного получения конфиденциальной информации и т. д.

Законодательство об информации и защите информации государств-участников устанавливает для органов государственной власти определенные обязанности (функции):

осуществлять контроль за соблюдением требований к превентивным мерам, принимаемым в отношении информации;

контролировать эксплуатацию специальных программно-технических средств, направленных на сохранение конфиденциальности информации;

обеспечивать организационные меры защиты информационных систем, обрабатывающих информацию с ограниченным доступом в негосударственных структурах.

В соответствии с законодательством государств-участников основными направлениями внутренней политики государства является:

утверждение положения о лицензировании конкретных видов деятельности;

определение органов исполнительной власти, осуществляющих лицензирование конкретных видов деятельности;

устанавление видов деятельности, лицензирование которых осуществляется органами исполнительной власти.

Лицензированию подлежат некоторые виды деятельности, связанные с обеспечением конфиденциальности информации и разработкой для этих целей специальных средств. К таковым видам деятельности относятся: деятельность по распространению шифровальных (криптографических) средств; деятельность по техническому обслуживанию шифровальных (криптографических) средств; предоставление услуг в области шифрования информации; разработка, производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем; деятельность по выдаче сертификатов ключей электронных цифровых подписей, регистрации владельцев электронных цифровых подписей, оказанию услуг, связанных с использованием электронных цифровых подписей, и подтверждению подлинности электронных цифровых подписей; деятельность по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя); деятельность по разработке и (или) производству средств защиты конфиденциальной информации; деятельность по технической защите конфиденциальной информации; разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными

предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность.

2. Пункт 2 комментируемой статьи устанавливает принципиально важное условие обеспечения конфиденциальности информации, составляющей коммерческую тайну, при ее предоставлении государственным органам и органам местного самоуправления: должностные лица, государственные или муниципальные служащие указанных органов не вправе разглашать или передавать полученную информацию другим лицам, в том числе другим органам государственной власти и местного самоуправления, без разрешения обладателя указанной информации.

3. Должностные лица, государственные и муниципальные служащие несут ответственность за разглашение и несанкционированное использование информации, составляющей коммерческую тайну, в соответствии с законодательством государства-участника.

Статья 16. Защита коммерческой тайны при взаимодействии хозяйствующих субъектов

1. При осуществлении хозяйствующими субъектами торгово-экономических, научно-технических, валютно-финансовых и других деловых связей, в том числе с иностранными партнерами, договаривающиеся стороны специально оговаривают характер, состав сведений, составляющих коммерческую тайну, а также взаимные обязательства по обеспечению ее сохранности в соответствии с законодательством государства-участника.

2. При заключении договора с иностранными партнерами условия конфиденциальности деятельности должны соответствовать законодательству страны, где заключается договор, если иное не предусмотрено межгосударственными соглашениями.

Комментарий к статье 16

Экономическая безопасность предприятия (фирмы) – это состояние защищенности жизненно важных интересов предприятия от внутренних и внешних угроз (источников опасности), формируемое администрацией и коллективом предприятия путем реализации системы мер правового, экономического, организационного, инженерно-технического и социально-психологического характера. В этом определении следует особо отметить два момента: состояние защищенности имеет динамичный характер; угроза, исходящая изнутри предприятия (фирмы), не менее опасна, чем исходящая извне.

Результатом защиты экономической безопасности предприятия является стабильность (надежность) его функционирования, эффективность финансово-коммерческой деятельности (прибыльность), личная безопасность персонала.

К ресурсам обеспечения надежного существования и прогрессивного развития предприятия относятся персонал предприятия, материальные и интеллектуальные (информационные) ресурсы.

С учетом этого деятельность по обеспечению экономической безопасности предприятия включает четыре основных направления: 1) защиту материальных и финансовых ценностей; 2) защиту персонала; 3) защиту интеллектуальной собственности (в том числе коммерческой тайны); 4) информационное обеспечение экономической деятельности предприятия в рыночных условиях.

По оценкам некоторых экспертов, затраты на создание системы безопасности фирмы и ее оптимальное функционирование могут достигать 25% затрат в процессе производства.

Эффективной может быть лишь комплексная система защиты, сочетающая в себе следующие меры: законодательные; физические (создание препятствий для доступа к охраняемому имуществу, оборудованию, информации); административные (введение соответствующего режима, порядка прохода и выхода и т. п.); технические (использование технических средств охраны); криптографические; программные; экономические; морально-этические.

Для каждого предприятия используется соответствующий комплекс мер, адекватных обстановке на нем и в его окружении.

Переход к рыночным отношениям потребовал от специалистов по безопасности способности ориентироваться в таких новых областях деятельности, как организация защиты коммерческой тайны и персонала предприятия.

Обеспечение сохранности коммерческой тайны (сведений) – это не только правовая, организационная, но и психологическая задача. Приступая к данной работе, важно понять ее ценность, необходимость.

В основе появления тайны (государственной, коммерческой, служебной) лежит недоверие между субъектами деятельности. И чем больше степень недоверия, тем больше тайн, используемых как средство обороны или нападения, получения выгод.

Рыночное производство включает в себя экономическую свободу и конкуренцию. Для того чтобы заработал механизм товарно-рыночного саморегулирования, необходимо огромное количество товаропроизводителей, которые будут иметь и реализовывать на практике свои экономические интересы.

В условиях насыщения рынка товарами и услугами покупатель получает возможность выбора более подходящего ему товара из массы аналогичных: возникает рынок покупателей. Конкуренция товаров резко обостряет и конкуренцию (соперничество) их изготовителей и поставщиков. Чтобы создать условия для активной экономической деятельности, производителям товаров необходимо не только ориентироваться на удовлетворение потребностей покупателей, но и выпускать изделия, имеющие определенные преимущества перед продукцией конкурентов. Любое преимущество, реализуемое с помощью ценовой и неценовой конкуренции, может быть отражено конкретными сведениями. Фактор же преимущества в процессе экономического соперничества будет существовать только до тех пор, пока эти сведения не выйдут из владения собственника.

Таким образом, в основе конкурентных отношений, борьбы за потребителя, получения благ в виде прибыли лежит различие экономических интересов субъектов рыночных отношений, определенное недоверие между ними.

По аналогии с природой рынок функционирует как система отбора, где предприятия, которые не в состоянии идти в ногу с конкурентами в повышении эффективности производства, обречены на экономическое вымирание. Выживут производители и продавцы, которые лучше всего приспособлены к окружающим условиям. Именно таким образом рынок обеспечивает оптимальное использование ресурсов общества. Характерной особенностью рыночной экономики является и то, что собственный интерес человека служит мотивационной основой его деятельности. В период становления рынка во взаимоотношениях между партнерами будет преобладать недоверие. Проблема состоит в том, что многие субъекты подозревают своих партнеров по сделкам в таких же неблаговидных мыслях, какие они имеют сами. Это неизбежное следствие системы эгоистической мотивации для получения прибыли.

Коммерческая тайна является порождением рыночных конкурентных отношений. Неправомерное овладение чужими информационными ресурсами с целью их использования представляет собой опасную форму недобросовестной конкуренции. Защита коммерческой тайны – важное условие получения предприятием максимальной прибыли, предотвращения банкротства. Переход к рыночным отношениям неизбежно ведет к усилению конкуренции между предприятиями (фирмами). Зарубежный опыт показывает: кто не заботится о защите своей интеллектуальной собственности, теряет до 30% возможной выручки.

Соблюдение конфиденциальности информации – фундамент успеха в бизнесе. Поэтому неразглашение закрытых сведений необходимо на всех этапах – предварительной проработки, экспериментальных работ, НИОКР, маркетинга, подготовки и ведения переговоров. В противном случае результаты исследований и предпринимательской деятельности и затраченные средства могут быть потеряны навсегда. К конфиденциальной информации могут быть отнесены любые сведения о деятельности фирмы, которые нежелательно отправлять неопределенному (и даже определенному) кругу лиц. Сюда следует отнести необнародованную информацию, касающуюся технологии, НИОКР, методов ведения дел, учета, списков покупателей, клиентов, поставщиков и т. п., т. е. конструкторскую документацию, результаты опытов и протоколы испытаний, перечень проведенных НИОКР, общепринятые таблицы и результаты расчетов, статистические расчеты, формулы и рецепты, данные о качестве материалов, список деталей, чертежи поставляемого оборудования, включая инструкции по обработке и т. п. Сюда включаются и другие требования: не разглашать перечни, которые дают сведения о результатах проведенных работ по разработке НИОКР (стандартов, нормалей и т. п.), о проведенных улучшениях, рабочие планы с указанием времени и допусков, технологические и (или) энергетические инструкции, чертежи и другую документацию по изготовлению изделий, отчеты о выпущенной продукции, оптимальное количество стандартных деталей, приемочные и испытательные предписания (инструкции), строительные и строительно-монтажные отчеты, перечни аппаратуры, количественные калькуляции наружного монтажа, данные работ по программированию, обучению персонала другого предприятия, сведения об организации производства, техническую документацию, связанные со сбытом, транспортировкой.

Как известно, во время зарубежных командировок и переговоров специалисты государств-участников контактируют только с руководством иностранной фирмы. Подобное правило (порядок) необходимо перенять и ни в коем случае не знакомить партнеров с изобретателями, технологами, а также с лицами, обладающими производственными секретами, предотвращать нежелательные и несанкционированные контакты с ними представителей фирм-партнеров. Кроме того, сотрудник должен быть связан с фирмой контрактом, предусматривающим пункты о неразглашении конфиденциальной информации и применении санкций за ее разглашение.

Статья 17. Доступ к коммерческой тайне

1. Доступ к коммерческой тайне имеют работники, круг которых определен хозяйствующим субъектом.

2. Государственные органы в пределах установленной им законодательством компетенции имеют право на основании письменного заявления, подписанного уполномоченным лицом, запрашивать и получать бесплатно сведения, составляющие коммерческую тайну.

3. В случае неправомерного отказа обладателя коммерческой тайны предоставить ее органу государственной власти, иному государственному органу, органу местного самоуправления обладатель коммерческой тайны несет ответственность согласно законам государства-участника.

4. Должностные лица органов государственной власти, иных государственных органов, органов местного самоуправления несут предусмотренную законодательством ответственность за разглашение сведений, составляющих коммерческую тайну хозяйствующего субъекта.

5. Иные органы и организации, в том числе средства массовой информации, правом истребования у хозяйствующего субъекта сведений, составляющих коммерческую тайну, не обладают.

Комментарий к статье 17

Вопрос доступа к сведениям, составляющим коммерческую тайну, урегулирован в государствах-участниках применительно к практике подразделений, осуществляющих расследование деятельности организованных преступных формирований. Согласно национальному законодательству банковская и коммерческая тайна не является препятствием для получения органами внутренних дел и иными компетентными ведомствами в установленном ими порядке сведений и документов о финансово-экономической деятельности, вкладах и операциях по счетам физических и юридических лиц, причастных к совершению бандитских нападений и других тяжких преступлений, совершенных организованными преступными группами.

Для получения органами внутренних дел справок по операциям и счетам юридических лиц и граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, а также по счетам и вкладам физических лиц необходимы три обязательных условия. Запрос должен быть сделан:

органом предварительного следствия; по делу, находящемуся в его производстве; согласован с прокурором.

Биржевые правонарушения могут быть отнесены к особому разряду неправомерных отношений в области правового регулирования сведений, не подлежащих публичному доступу. Правонарушения нередко связаны с инсайдерской деятельностью или с использованием участниками отношений инсайдерской информации. Манипулятор, называясь инсайдером или осведомленным лицом и распространяя нередко ложную информацию об эмитенте, создает повышенный спрос на определенные ценные бумаги, способствует повышению их цены, затем продает ценные бумаги по повышенным ценам. После совершения подобных операций цена на рынке возвращается к исходному уровню, а рядовые инвесторы оказываются в убытке. Данная схема используется при недостатке или отсутствии информации о компаниях, ценные бумаги которых редко торгуются. Инсайдером является лицо, имеющее в силу своего служебного или семейного положения доступ к конфиденциальной информации о делах компании. К таким лицам могут быть отнесены должностные лица, директор или один из основных акционеров корпорации с широким владением акциями и их ближайшие родственники. В эту группу также включаются те, кто добывает конфиденциальную информацию о корпорации и используют ее в целях личного обогащения.

Инсайдерская информация обладает определенными признаками, позволяющими выделить ее из более общей категории информации, составляющей служебную и коммерческую тайну. В частности, инсайдерская информация: а) не является общедоступной (к ней «нет свободного доступа на законном основании»; б) всегда имеет прямое или косвенное отношение к предмету биржевой торговли; в) характеризуется такой взаимосвязью между ее использованием и изменением биржевой ситуации, при которой инсайдерская информация оказывает непосредственное ощутимое воздействие на ценообразующие факторы биржевого рынка.

В связи с этим представляет интерес Директива Совета ЕС 89/592 «О координации положений об инсайдерской деятельности» от 13 ноября 1989 года, которая в статье 1 устанавливает, что инсайдерская информация, не являясь общеизвестной, «в случае опубликования привела бы к значительным изменениям курса» соответствующих ценных бумаг. Зарубежное законодательство подразумевает под инсайдерской информацией не только сведения, зафиксированные на определенных носителях, но и сведения, не получившие такого отображения (например, сформулированные в устной форме квалифицированные суждения или коммерческие предложения).

В международной практике следует различать первичных и вторичных инсайдеров: оформление правового режима их деятельности различно. Первичные инсайдеры – это физические лица, имеющие прямой доступ к инсайдерской информации вследствие существующих правоотношений с обладателем инсайдерской информации или на ином законном основании. Квалифицирующим признаком первичных инсайдеров является их правовой статус или правовой режим деятельности. Под вторичными инсайдерами понимаются лица, по-

лучившие инсайдерскую информацию от третьих лиц (непосредственно или косвенным путем). Следовательно, вторичными инсайдерами могут быть и лица, не имеющие никаких правоотношений с обладателем этой информации.

Рассмотрим виды инсайдерской деятельности, признаваемые противоправными.

Прежде всего следует назвать использование инсайдерской информации при совершении биржевых сделок. Запрет на использование инсайдерской информации действует не только при заключении сделок, но и на всех этапах проведения биржевых торгов. Противоправной является передача инсайдерской информации третьим лицам (разглашение). Под понятие инсайдерского правонарушения подпадает также и умышленное незаконное приобретение инсайдерской информации.

Международная практика выделяет еще один вид инсайдерских правонарушений, а именно: предоставление основанных на инсайдерской информации рекомендаций и других консультационных услуг относительно осуществления биржевой деятельности (статья 6 Директивы Совета ЕС 89/592). При этом само содержание инсайдерской информации остается неизвестным третьим лицам. Ограничения инсайдерской деятельности вторичных инсайдеров в национальных законодательствах неодинаковы. Передавать инсайдерскую информацию и предоставлять на ее основе рекомендации запрещается вторичным инсайдерам только в Великобритании, Ирландии и Бельгии. Применение санкций к вторичным инсайдерам предусматривает, что они знали или должны были знать о наличии у используемой ими информации качества инсайдерской.

В некоторых странах существует еще более жесткая регламентация инсайдерской деятельности. Лица, получившие рекомендацию указанного типа и знавшие о ее инсайдерской сущности, рассматриваются в качестве вторичных инсайдеров, и на них распространяется общий запрет на использование инсайдерской информации.

Факт инсайдерского правонарушения устанавливается в судебном порядке, а биржевые сделки, совершенные с использованием инсайдерской информации, признаются судом недействительными. На лиц, совершивших инсайдерское правонарушение, распространяется положение о возмещении убытков. Основаниями возникновения гражданско-правовой ответственности являются нарушение принятых обязательств и деликт. Право требовать возмещения убытков принадлежит обладателю инсайдерской информации, а в некоторых случаях лицам, чьи права и охраняемые законом интересы нарушены в результате совершения биржевых сделок с ее использованием. В целом привлечение инсайдеров к гражданско-правовой ответственности представляется несколько проблематичным. Определенные сложности создают договорные конструкции, используемые в биржевой торговле. Между инсайдером и другими участниками биржевой торговли, как правило, не возникает непосредственных договорных отношений или даже личного контакта (например, при проведении электронных биржевых торгов и наличии клиринговой организации). Большинство биржевых сделок совершается биржевыми посредниками от собственного имени, но в интересах третьих лиц, которые нередко и выступают в качестве ин-

сайдеров. Вследствие этого многие страны не обращаются более к гражданско-правовой ответственности инсайдеров. Для стран ЕС исключение составляют лишь законодательство Ирландии (Sec. 109 Companies Act 1990) и Португалии (Art. 449 Codigo des Sociedades).

Статья 18. Предоставление коммерческой тайны

1. Обладатель коммерческой тайны по мотивированному требованию органа государственной власти, иного государственного органа, органа местного самоуправления предоставляет им на безвозмездной основе коммерческую тайну. Мотивированное требование должно быть подписано уполномоченным должностным лицом, содержать указание цели и правового основания затребования коммерческой тайны и срок предоставления этой информации, если иное не установлено законами государства-участника.

2. В случае отказа обладателя коммерческой тайны предоставить ее органу государственной власти, иному государственному органу, органу местного самоуправления данные органы вправе затребовать эту информацию в судебном порядке.

3. Обладатель коммерческой тайны, а также органы государственной власти, иные государственные органы, органы местного самоуправления, получившие эту информацию в соответствии с пунктом 1 настоящей статьи, обязаны предоставить такую информацию по запросу судов, органов прокуратуры, органов предварительного следствия, органов дознания по делам, находящимся в их производстве, в порядке и на основаниях, которые предусмотрены законодательством государства-участника.

4. На документах, предоставляемых указанным в пунктах 1 и 3 настоящей статьи органам и содержащих коммерческую тайну, должен быть нанесен гриф «Коммерческая тайна» с указанием ее обладателя (для юридических лиц – полное наименование и место нахождения, для индивидуальных предпринимателей – фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

Комментарий к статье 18

1. Пункт 1 комментируемой статьи устанавливает обязанность государственных органов и органов местного самоуправления создать условия, обеспечивающие охрану конфиденциальности информации, предоставленной им юридическими лицами или индивидуальными предпринимателями.

Помимо данной обязанности государство выполняет также и другие функции по регулированию и обеспечению информационных отношений, предусмотренные иными нормативными правовыми актами. Основными направлениями государственной политики в сфере информатизации являются: обеспечение условий для развития и защиты всех форм собственности на информационные ресурсы; создание и совершенствование системы привлечения инвестиций и механизма стимулирования разработки и реализации проектов

информатизации; развитие законодательства в сфере информационных процессов, информатизации и защиты информации.

Таким образом, государство призвано создавать условия для деятельности субъектов информационных отношений, во-первых, посредством юридических мер – создания необходимой нормативной базы (разработка и принятие законодательных актов, стандартов, инструкций, классификаторов и т. д.). Во-вторых, посредством мер организационного характера и инвестирования. Последнее подразумевает как привлечение инвестиций в рассматриваемую сферу, так и вливание в нее бюджетных средств. Государство может выступать инициатором конкурсов на выполнение научно-исследовательских и опытно-конструкторских работ, предметом которых могут быть в том числе исследования в области безопасности информации, создание новых технических и иных преград для негласного получения конфиденциальной информации и т. д.

Законодательство государств-участников о защите информации устанавливает для органов государственной власти следующие обязанности (функции):

осуществлять контроль за соблюдением требований к превентивным мерам, принимаемым в отношении информации;

контролировать эксплуатацию специальных программно-технических средств, направленных на сохранение конфиденциальности информации;

обеспечивать организационные меры «защиты» информационных систем, обрабатывающих информацию с ограниченным доступом в негосударственных структурах.

Согласно законодательству государств-участников лицензированию подлежат некоторые виды деятельности, связанные с обеспечением конфиденциальности информации и разработкой для этих целей специальных средств. К таковым видам деятельности относятся:

деятельность по распространению шифровальных (криптографических) средств;

деятельность по техническому обслуживанию шифровальных (криптографических) средств;

предоставление услуг в области шифрования информации;

разработка, производство шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных систем, телекоммуникационных систем;

деятельность по выдаче сертификатов ключей электронных цифровых подписей, регистрации владельцев электронных цифровых подписей, оказанию услуг, связанных с использованием электронных цифровых подписей, и подтверждению подлинности электронных цифровых подписей;

деятельность по выявлению электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя);

деятельность по разработке и (или) производству средств защиты конфиденциальной информации;

деятельность по технической защите конфиденциальной информации;

разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации, индивидуальными предпринимателями и юридическими лицами, осуществляющими предпринимательскую деятельность.

Представляется, что для достижения указанных целей необходимо проведение целого ряда мероприятий по обеспечению безопасности конфиденциальной информации, прежде всего имеющей коммерческую ценность, в масштабе всего государства. Причем эти мероприятия должны быть разработаны не только для государственных нужд.

2. Пункт 2 комментируемой статьи устанавливает принципиально важное условие обеспечения конфиденциальности информации, составляющей коммерческую тайну, при ее предоставлении государственным органам и органам местного самоуправления: должностные лица, государственные или муниципальные служащие указанных органов не вправе разглашать или передавать полученную информацию другим лицам, в том числе другим органам государственной власти и местного самоуправления, без разрешения обладателя указанной информации.

3. Должностные лица, государственные и муниципальные служащие несут ответственность за разглашение и несанкционированное использование информации, составляющей коммерческую тайну, в соответствии с законодательством государства-участника.

Статья 19. Способы получения коммерческой тайны

1. Информация, самостоятельно полученная лицом при осуществлении исследований, систематических наблюдений или иной деятельности, считается полученной законным способом несмотря на то, что содержание указанной информации может совпадать с содержанием коммерческой тайны, обладателем которой является другое лицо.

2. Коммерческая тайна, полученная от ее обладателя на основании договора или другом законном основании, считается полученной законным способом.

3. Коммерческая тайна, обладателем которой является другое лицо, считается полученной незаконно, если ее получение осуществлялось методами промышленного шпионажа, с умышленным преодолением принятых обладателем коммерческой тайны мер по охране конфиденциальности этой информации, а также если получающее эту информацию лицо знало или имело достаточные основания полагать, что эта информация составляет коммерческую тайну, обладателем которой является другое лицо, и что осуществляющее передачу этой информации лицо не имеет на передачу этой информации законного основания.

Комментарий к статье 19

Коммерческая тайна неразрывно связана с понятием конкуренции, так как именно конкуренция является одним из важнейших факторов эффективного

развития рыночной экономики. Конкурентная борьба неизбежно предполагает обеспечение сохранения в тайне сведений, овладение которыми посторонними лицами могло бы ослабить экономические позиции предприятия (фирмы) или нанести невосполнимый ущерб.

Типичными каналами утечки сведений, содержащих коммерческую тайну, для любого научного учреждения или предприятия являются:

– публикации в отечественных и иностранных изданиях;

– договоры о выполнении НИР, включая хоздоговорные работы, договоры подряда и т. п.;

– деятельность совместных и малых предприятий, акционерных обществ, кооперативов, центров и т. д., создаваемых с участием сотрудников, которые были или являются работниками учреждения;

– аренда помещений и другие взаимоотношения, в связи с которыми сотрудники сторонних организаций получают потенциальную возможность доступа к сведениям о сущности интеллектуальной собственности учреждения (совместные или самостоятельные исследования по тематике, тождественной или аналогичной исследованиям учреждения, установление трудовых отношений с сотрудниками учреждения, общие территория и научные интересы);

– любые формы международного сотрудничества;

– экспонирование на отечественных и иностранных выставках и иные формы рекламы;

– передача документации и образцов устройств, веществ, программ для ЭВМ, ноу-хау, результатов НИР представителям отечественных и иностранных предприятий и фирм;

– участие в конференциях, конгрессах, семинарах в своей стране и за рубежом;

– участие в конкурсах на получение грантов от иностранных и отечественных фондов;

– деятельность сотрудников учреждения в качестве сотрудников или консультантов иностранных и отечественных исследовательских центров, фирм, предприятий;

– пребывание в лабораториях учреждения специалистов иностранных фирм и отечественных организаций, в том числе командированных, стажеров, аспирантов и студентов;

– предоставление сведений о лучших разработках учреждения по запросам различных министерств, ведомств, агентств, ассоциаций, фирм, предприятий, фондов и т. п.

Перечисление потенциальных каналов утечки коммерчески ценной информации, конечно, не является предложением к прекращению публикаций или свертыванию сотрудничества. Просто жизнь настоятельно требует надежной защиты коммерческой тайны конкретного предприятия с учетом специфических особенностей его деятельности. Научные учреждения и промышленные предприятия, которые располагают достаточным интеллектуальным потенциалом и рассчитывают на коммерческий успех в условиях конкуренции, должны позаботиться о создании эффективной системы сохранения коммерческой тай-

ны на основе гибкого сочетания организационных мер и ответственности (административной и имущественной) должностных лиц и каждого сотрудника.

Определенный интерес могут представлять исследования немецких ученых в области сохранения коммерческой тайны фирм. Они отмечают следующие тенденции:

1) возрастает доля научно-технических результатов, не обеспечиваемых патентной защитой и сохраняемых только на основе коммерческой тайны;

2) в качестве предмета экспорта все чаще выступает комплексная информация, которая включает объекты, охраняемые как патентами и авторским правом, так и в режиме конфиденциальности;

3) даже при сохранении коммерческой тайны патентная защита играет основную роль;

4) в условиях жесткой конкурентной борьбы и сокращения жизненного цикла научно-технических новшеств успех на рынке напрямую зависит от квалифицированного сохранения коммерческой тайны;

5) наиболее ценной для принятия решения об экспорте и импорте является информация о патенто- и конкурентоспособности объекта, основанная на результатах патентного поиска и маркетинговых исследований;

6) все более важной составной частью стратегического маркетинга становятся комплексные данные об объектах промышленной собственности, ноу-хау и коммерческой тайне.

Специалисты к числу наиболее вероятных каналов утечки классифицированной информации относят:

– совместную с другими фирмами деятельность, участие в переговорах;

– фиктивные запросы со стороны о возможности работать в фирме на различных должностях;

– экскурсии и посещения фирмы;

– сообщения торговых представителей фирмы о характеристиках изделия;

– чрезмерную рекламу;

– поставки смежников;

– консультации специалистов со стороны, которые вследствие этого получают доступ к оборудованию и документам фирмы;

– публикации в печати и выступления;

– совещания, конференции, симпозиумы и т. п.;

– разговоры в нерабочих помещениях;

– обиженных сотрудников фирм.

Следует учитывать также возможные методы и способы сбора информации: а) опрос при личной встрече; б) навязывание дискуссий по интересующим проблемам; в) рассылка в адреса предприятий и отдельных специалистов вопросников и анкет; г) ведение частной переписки научных центров и ученых со специалистами.

В целях сбора сведений в ряде случаев используются переговоры, проводимые для определения перспектив сотрудничества, создания совместных предприятий.

Наличие такой формы сотрудничества, как выполнение совместных программ, предусматривающих непосредственное участие представителей других организаций в работе с документами, посещение рабочих мест, расширяет возможности для снятия копий документов, сбора различных образцов материалов, проб и т. д. Наиболее вероятно могут быть использованы следующие способы получения информации: а) визуальное наблюдение; б) подслушивание; в) техническое наблюдение; г) прямой опрос, выведывание; д) ознакомление с материалами, документами, изделиями и т. д.; е) сбор открытых документов и других источников информации; ж) хищение документов и других источников информации; з) изучение множества источников информации, содержащих по частям необходимые сведения.

Статья 20. Ответственность за несанкционированное разглашение коммерческой тайны

1. Под несанкционированным разглашением коммерческой тайны понимаются умышленные или неосторожные действия работников хозяйствующего субъекта, располагающих сведениями, составляющими коммерческую тайну, или других физических и юридических лиц, имеющих доступ к коммерческой тайне либо незаконно получивших сведения, составляющие коммерческую тайну, повлекшие за собой их преждевременное раскрытие и бесконтрольное использование или распространение, в результате чего нанесен или может быть нанесен ущерб интересам хозяйствующего субъекта.

2. За нарушение настоящего Закона и иных нормативных актов о коммерческой тайне физические и юридические лица привлекаются к ответственности в соответствии с законодательством государства-участника.

3. Работники хозяйствующего субъекта, государственных органов, а также лица, незаконно получившие сведения, составляющие коммерческую тайну, или завладевшие ими, обязаны также возместить ущерб, причиненный хозяйствующему субъекту или субъекту предпринимательства.

Комментарий к статье 20

В настоящее время за нарушение прав владельца коммерческой тайны законодательством государств-участников установлены следующие виды ответственности: 1) ответственность в рамках трудовых отношений; 2) гражданско-правовая ответственность; 3) административная ответственность; 4) уголовная ответственность.

1. Ответственность в рамках трудовых отношений. За несоблюдение режима работы с информацией, составляющей коммерческую тайну, к работникам субъекта предпринимательской деятельности может быть применена материальная и дисциплинарная ответственность. Привлечение к материальной и дисциплинарной ответственности осуществляется на общих основаниях, с учетом особенностей правового статуса «коммерческой тайны». Для законного применения санкций за правонарушения, связанные с коммерческой тайной в рамках трудовых отношений, предпринимателю необходимо иметь некоторые

документы, а именно:

а) документ, устанавливающий перечень сведений, составляющих коммерческую тайну. Это может быть утвержденное предпринимателем (компетентным органом управления субъекта предпринимательской деятельности) положение о коммерческой тайне, в котором четко оговаривалось бы, какие сведения являются коммерческой тайной, порядок отнесения их к таковым, условия хранения, а также кто из работников предпринимателя может передавать указанные сведения представителям государственных органов и организаций;

б) должностные инструкции, которыми должны определяться круг полномочий работников предпринимателя, сведения, содержащие коммерческую тайну, и порядок работы с ними;

С документами, указанными в пункте «а» и «б», работник должен быть ознакомлен перед началом своей трудовой деятельности у данного предпринимателя. Факт ознакомления должен фиксироваться письменно, с указанием даты ознакомления;

в) трудовой договор (контракт), в котором должны быть указаны обязанность работника соблюдать коммерческую тайну и последствия несоблюдения этой обязанности. Условия материальной ответственности работника за разглашение коммерческой тайны могут быть предусмотрены как трудовым договором, так и отдельным соглашением о материальной ответственности.

За нарушение режима коммерческой тайны работником к нему могут быть применены следующие дисциплинарные санкции: выговор, увольнение. Если было заключено соглашение о материальной ответственности за разглашение сведений, составляющих коммерческую тайну, работник также отвечает и материально, в предусмотренных соглашением сторон размерах.

В рамках трудовых отношений в первую очередь интерес представляют особенности привлечения лица к дисциплинарной ответственности за такого вида проступок.

Например, в соответствии со статьей 81 Трудового кодекса Российской Федерации при разглашении сведений, составляющих коммерческую тайну, работник может быть уволен по односторонней инициативе работодателя. Здесь следует заметить, что уволить сотрудника за разглашение тайны не так просто и подходить к этой процедуре работодателю следует очень аккуратно, поскольку любая ошибка может привести к признанию увольнения незаконным и оплате вынужденного прогула. Так, в Постановлении Пленума Верховного Суда Российской Федерации от 17 марта 2004 года № 2 «О применении судами Российской Федерации Трудового кодекса Российской Федерации» обращается внимание на то, что в случае оспаривания работником увольнения по подпункту «в» пункта 6 части 1 статьи 81 Трудового кодекса Российской Федерации «работодатель обязан представить доказательства, свидетельствующие о том, что сведения, которые работник разгласил, в соответствии с действующим законодательством относятся к государственной, служебной, коммерческой или иной охраняемой законом тайне либо к персональным данным другого работника, эти сведения стали известны работнику в связи с исполнением им трудо-

вых обязанностей и он обязывался не разглашать такие сведения». То есть доказывать в суде, что информация действительно носит характер коммерческой тайны, придется именно работодателю.

Судебная практика по данному поводу небогата. Примеры из нее свидетельствуют о том, что решения выносятся в основном в пользу работников. Однако следует отметить и положительные для работодателей решения, принятые судами. Так, в 2008 году информационные агентства широко освещали случай, когда сотрудница туристической фирмы в течение года отправляла конфиденциальную информацию в другую туристическую компанию, как со своего компьютера, так и с компьютеров других сотрудниц. В частности, она передавала информацию о готовящихся сделках компании своему бывшему работодателю. За информацию она просила вознаграждение. Сотрудницу уволили по подпункту «в» пункта 6 статьи 81 Трудового кодекса Российской Федерации – разглашение коммерческой тайны. При этом в компании существовал режим обеспечения коммерческой тайны, девушка подписала все документы о неразглашении. Несмотря на то что факт шпионажа был доказан, бывшая сотрудница подала в суд на компанию. В своем иске она требовала заменить увольнение по статье 81 на статью 77, пункт 3 (по собственному желанию), однако суд ее иск отклонил. В свою очередь руководство организации подало документы в прокуратуру с целью возбуждения уголовного дела. При этом в условиях скудной правоприменительной практики туристическая компания, по словам директора, хотела в основном создать прецедент, «чтобы туристическая общественность, а также правоохранительные органы обратили на это внимание».

Журнал «Трудовое право» (№ 5, 2009 год) в интервью с генеральным директором компании Energy Consulting/Business Service группы Energy Consulting привел пример выигранного компанией в суде трудового спора по увольнению сотрудника за разглашение коммерческой тайны, которая стала ему известна в процессе исполнения трудовых обязанностей (пункт 6 части 1 статьи 81 Трудового кодекса Российской Федерации). Этот сотрудник имел допуск к информации, составляющей коммерческую тайну. Как выяснилось, он передал ее третьему лицу. Факт нарушения корпоративной инструкции по обеспечению сохранности коммерческой тайны был установлен, и компания приняла решение уволить сотрудника. Он попытался оспорить решение в судебном порядке. Суд, изучив дело, признал действия компании правомерными и оставил принятое решение без изменений.

В феврале 2008 года мировой судья судебного участка № 4 Красногорского района Каменска-Уральского признал, что ведущий специалист страховой компании «Гамма», ранее работавшая в «Росгосстрахе», использовала сведения, составляющие коммерческую тайну ОАО «Росгосстрах» (клиентскую базу) без согласия владельца (часть 2 статьи 183 УК), и, учитывая возраст (57 лет) и отсутствие судимостей, приговорил ее к шести месяцам лишения свободы условно. Суд нисколько не сомневался в охраноспособности этих сведений, безусловно, являющихся одновременно и персональными данными, и встал на сторону пострадавшей от нарушения своих исключительных прав страховой компании.

Следует отметить, что в секторах экономики, работающих с физическими лицами, где конкуренция весьма высока, практика привлечения к ответственности бывших работников, прихвативших с собой клиентскую базу или сливающих сведения о клиентах конкурентам, становится все более обыденной. Так, главный экономист кредитного отдела саратовского филиала банка «Петрокоммерц», был уволен по статье 81 Трудового кодекса Российской Федерации за «разглашение охраняемой законом коммерческой тайны, ставшей известной работнику в связи с исполнением им трудовых обязанностей», которое выразилось в передаче клиентской базы в конкурирующий банк, где ему был обещан оклад на 40% больше. Иск о незаконности увольнения судом Октябрьского района г. Саратова был отклонен. Причем на аргумент уволенного менеджера о возможности использования его компьютера другими лицами для его компрометации суд неожиданно предложил ему самому найти того человека, кто это сделал.

2. Гражданско-правовая ответственность. Согласно нормам гражданского права причиненный вред должен быть возмещен в полном объеме. При этом возмещение морального вреда не связано с возмещением материального, а размер возмещения определяется судом.

Моральный ущерб возмещается в денежной или иной материальной форме. В любом случае размер возмещения не может быть менее пяти минимальных размеров заработной платы.

Законодательство государств-участников не содержит исчерпывающего перечня обстоятельств, с наступлением которых предприниматель может связывать причинение ему морального ущерба. В исковом заявлении по делам, связанным с разглашением коммерческой тайны, необходимо указывать, какой именно вред был причинен разглашением, в чем именно состоит причиненный моральный ущерб, какими противоправными действиями ответчика был причинен ущерб. Основанием для возмещения ущерба является решение суда (хозяйственного суда).

По вопросу возмещения работодателю убытков при разглашении коммерческой тайны существует довольно скудная практика. В литературе встречается мнение, что после прекращения трудовых отношений отношения между сторонами перестают регулироваться нормами трудового права и переходят в гражданско-правовую плоскость. Однако следует помнить, что, несмотря на то что вопрос использования и разглашения коммерческой тайны бывшим работником как будто бы относится к гражданско-правовому регулированию, эти права и обязанности возникли из трудовых отношений, которые закончились увольнением работника. Этим объясняется сложность урегулирования данного вопроса.

Законодательство Российской Федерации предусматривает возможность взыскать убытки, причиненные работником, и в рамках трудовых отношений. Какова процедура взыскания убытков и как рассчитывается их размер?

В соответствии с пунктом 7 части 1 статьи 243 Трудового кодекса Российской Федерации при разглашении сведений, составляющих охраняемую законом тайну (государственную, служебную, коммерческую или иную), в случа-

ях, предусмотренных федеральными законами, на работника возлагается материальная ответственность в полном размере причиненного ущерба.

Согласно статье 238 Трудового кодекса Российской Федерации работник обязан возместить работодателю причиненный ему прямой действительный ущерб. Под прямым действительным ущербом понимается реальное уменьшение наличного имущества работодателя или ухудшение состояния указанного имущества (в том числе имущества третьих лиц, находящегося у работодателя, если работодатель несет ответственность за сохранность этого имущества), а также необходимость для работодателя произвести затраты либо излишние выплаты на приобретение, восстановление имущества либо на возмещение ущерба, причиненного работником третьим лицам.

Неполученные доходы (упущенная выгода) взысканию с работника не подлежат. До принятия решения о взыскании ущерба работодатель обязан провести проверку для установления размера причиненного ущерба и причин его возникновения. Как правило, для этого создается комиссия с участием соответствующих специалистов. У работника следует истребовать письменное объяснение для установления причин ущерба. В случае отказа или уклонения работника от предоставления указанного объяснения составляется соответствующий акт (статья 247 ТК РФ). Причиненный работниками ущерб возмещается в порядке, установленном статьей 248 Трудового кодекса Российской Федерации.

Если размер причиненного ущерба не превышает среднемесячного заработка работника (независимо от вида материальной ответственности), его взыскание осуществляется на основании письменного приказа (распоряжения) работодателя. Такой акт должен быть издан не позднее месячного срока со дня установления размера причиненного работником ущерба.

Если месячный срок истек, взыскание ущерба может быть произведено только с согласия самого работника или в судебном порядке. Ущерб, размер которого превышает среднемесячный заработок работника, также может быть взыскан только с согласия работника или в судебном порядке. Добровольное возмещение (полное или частичное) ущерба работником допускается путем внесения соответствующих денежных сумм в кассу организации. В соответствии со статьей 138 Трудового кодекса Российской Федерации удержания ущерба из заработной платы могут производиться в размере не свыше 20% заработка, причитающегося к выплате работнику.

В случае разглашения коммерческой тайны затруднение при расчете причиненного ущерба заключается в определении суммы ущерба. В настоящее время отсутствуют точные критерии определения данной суммы. Убытки от разглашения коммерческой тайны выражаются главным образом именно в упущенной выгоде, т. е. в доходах, которые могла бы получить организация в случае сохранения тайны, однако, как уже упоминалось, упущенная выгода взысканию с работника не подлежит.

По общему правилу размер ущерба, причиненного работодателю при утрате и порче имущества, определяется по фактическим потерям, исчисляемым исходя из рыночных цен, действующих в данной местности на день при-

чинения ущерба, но не ниже стоимости имущества по данным бухгалтерского учета с учетом степени износа этого имущества (статья 246 ТК РФ).

Итак, в соответствии с нормами трудового права работник может нести лишь «ограниченную» материальную ответственность в форме возмещения материального ущерба (а не убытков, в том числе упущенной выгоды).

В то же время статья 1472 Гражданского кодекса Российской Федерации устанавливая ответственность за нарушение исключительного права на секрет производства, предусматривает, что нарушитель исключительного права на секрет производства, в том числе лицо, которое неправомерно получило сведения, составляющие секрет производства, и разгласило или использовало эти сведения, а также лицо, обязанное сохранять конфиденциальность секрета производства в соответствии с пунктом 2 статьи 1468, пунктом 3 статьи 1469 или пунктом 2 статьи 1470 Гражданского кодекса, обязано возместить убытки, причиненные нарушением исключительного права на секрет производства, если иная ответственность не предусмотрена законом или договором с этим лицом.

Вопрос о том, какая же ответственность применима к работнику – нарушителю режима коммерческой тайны: в форме возмещения материального ущерба или в форме возмещения убытков, может решаться с учетом нормы статьи 15 Гражданского кодекса Российской Федерации, в пункте 1 которой указано, что лицо, право которого нарушено, может требовать полного возмещения причиненных убытков, если законом не предусмотрено возмещение убытков в меньшем размере. Уменьшенный размер ответственности должен быть установлен законом. Таким предусмотренным законом уменьшением размера гражданско-правовой ответственности является ограничение или уменьшение размера ответственности, закрепленное в статье 238 Трудового кодекса Российской Федерации, обязывающей работника возместить работодателю лишь прямой действительный ущерб.

3. Административная ответственность. Административная ответственность за нарушения, связанные с коммерческой тайной, устанавливается за получение, использование, разглашение коммерческой тайны нормами кодекса об административных правонарушениях. Так, Законом Украины «О защите от недобросовестной конкуренции» предусмотрена ответственность за неправомерный сбор коммерческой информации (статья 16), разглашение коммерческой тайны (статья 17), склонение к разглашению коммерческой тайны (статья 18.), неправомерное использование коммерческой тайны (статья 19). Этим же законом регулируется порядок подачи и рассмотрения заявлений по указанным правонарушениям. Установленное для нарушителя наказание – штраф в размере от 10 до 20 минимальных размеров заработной платы.

4. Уголовная ответственность. Во многих экономически развитых странах мира уже длительное время предусмотрена уголовная ответственность за разглашение коммерческой тайны, а в уголовном праве Франции такая ответственность фигурирует еще с 1844 года.

Общественная опасность незаконного получения, разглашения сведений, составляющих коммерческую тайну, заключается в том, что лица, совершившие такие деяния, или недобросовестные предприниматели, использующие

«чужую коммерческую тайну», лишают своих соперников тех преимуществ (по отношению к своим конкурентам), которые дает им обладание конфиденциальной информацией. Поэтому в пункте 5 части 1 статьи 14 Федерального закона от 26 июля 2006 года № 135-ФЗ «О защите конкуренции» в числе запретов на недобросовестную конкуренцию упоминается «незаконное получение, использование, разглашение информации, составляющей коммерческую, служебную или иную охраняемую законом тайну».

В части 1 статьи 183 Уголовного кодекса Российской Федерации предусмотрена уголовная ответственность за незаконное получение и разглашение сведений, составляющих коммерческую, налоговую и банковскую тайну. В части 1 данной статьи объективная сторона преступления характеризуется собиранием сведений, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, подкупа или угроз. Перечень способов не является исчерпывающим, поскольку в статье указывается на возможность существования иных незаконных способов. Необходимое условие для квалификации деяния правонарушителя по данной статье – к информации, составляющей коммерческую тайну, не должно быть свободного доступа и ее владелец принял для этого все соответствующие меры. Часть 2 анализируемой статьи Уголовного кодекса предусматривает ответственность за незаконное разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе. Так, объективная сторона этого состава предполагает не только разглашение соответствующих сведений, но и их использование. Последнее означает распоряжение преступником этими сведениями, в том числе и в предпринимательских целях. В части 3 статьи 183 предусмотрена ответственность за «те же деяния, причинившие крупный ущерб или совершенные из корыстной заинтересованности». Это могут быть большие материальные убытки, понесенные хозяйствующим субъектом в конкурентной борьбе, вызванные спадом производства, необходимостью его переориентации, уменьшением клиентуры, потерей рынков сбыта и т. д. Крупный ущерб определен в законе в сумме, превышающей 250 000 рублей.

Предусмотренные частью 4 статьи 183 Уголовного кодекса Российской Федерации тяжкие последствия преступления понимаются более широко, чем причинение материальных убытков. Это может быть банкротство и ликвидация организации, банкротство индивидуального предпринимателя, причинение серьезного вреда здоровью людей, самоубийство потерпевшего и др., если такие последствия находятся в причинной и виновной связи с незаконным разглашением или использованием соответствующих сведений.

Статья 200 Уголовного кодекса Республики Казахстан устанавливает уголовную ответственность за незаконные получение и разглашение сведений, составляющих коммерческую или банковскую тайну. Так собирание сведений, составляющих коммерческую или банковскую тайну, путем похищения документов, подкупа или угроз в отношении лиц, владеющих коммерческой или банковской тайной, или их близких, перехвата в средствах связи, незаконного проникновения в компьютерную систему или сеть, использования специальных

технических средств, а равно иным незаконным способом в целях разглашения либо незаконного использования этих сведений – наказывается штрафом в размере от 100 до 200 месячных расчетных показателей или в размере заработной платы или иного дохода осужденного за период до двух месяцев, либо исправительными работами на срок до 2-х лет, либо арестом на срок до 6-ти месяцев, либо лишением свободы на срок до 1 года.

Незаконные разглашение или использование сведений, составляющих коммерческую или банковскую тайну, без согласия их владельца лицом, которому она была доверена по службе или работе, совершенные из корыстной или иной личной заинтересованности и причинившие крупный ущерб, наказываются штрафом в размере от 200 до 500 месячных расчетных показателей или в размере заработной платы или иного дохода осужденного за период от 2-х до 5 месяцев, либо арестом на срок от 4 до 6 месяцев, либо исправительными работами на срок от 1 года до 2 лет, либо лишением свободы на срок до 3-х лет со штрафом в размере до 100 месячных расчетных показателей или в размере заработной платы или иного дохода осужденного за период до 1 месяца либо без такового.

Уголовный кодекс Республики Беларусь, по сравнению с Уголовным кодексом Республики Казахстан, имеет значительно больше отличительных особенностей от Уголовного кодекса Российской Федерации. Особенности заключаются в конструкции статей, предусматривающих ответственность за посягательство на тайну, их расположении в главах, наименовании. Так, в главе 25 «Преступления против порядка осуществления экономической деятельности» включены статья 254 «Коммерческий шпионаж» и статья 255 «Разглашение коммерческой тайны». Коммерческая и банковская тайны по Уголовному кодексу Республики Беларусь защищается двумя статьями – статьей 254 «Коммерческий шпионаж» и статьей 255 «Разглашение коммерческой тайны». Руководствуясь названием статей, логично сделать вывод, что понятие предмета в данных составах включает в себя сведения, составляющие коммерческую и банковскую тайну, т. е. банковская тайна есть разновидность коммерческой тайны.

Санкции статьи 254 «Коммерческий шпионаж» предусматривают, что похищение либо собирание незаконным способом сведений, составляющих коммерческую или банковскую тайну, с целью их разглашения либо незаконного использования (коммерческий шпионаж) наказываются штрафом, или арестом на срок до 6-ти месяцев, или ограничением свободы на срок до 3-х лет, или лишением свободы на тот же срок. Коммерческий шпионаж, повлекший причинение ущерба в особо крупном размере, наказывается арестом на срок от 2-х до 6-ти месяцев, или ограничением свободы на срок от 2-х до 5-ти лет, или лишением свободы на срок от 1-го года до 5-ти лет.

Статьей 255 «Разглашение коммерческой тайны» предусмотрено, что умышленное разглашение коммерческой или банковской тайны без согласия ее владельца при отсутствии признаков преступлений, предусмотренных статьями 226-1 и 254 настоящего Кодекса, лицом, которому такая коммерческая или банковская тайна известна в связи с его профессиональной или служебной дея-

тельностью, повлекшее причинение ущерба в крупном размере, наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом на срок до 6-ти месяцев, или ограничением свободы на срок до 3-х лет, или лишением свободы на тот же срок. То же действие, совершенное из корыстной или иной личной заинтересованности, наказывается ограничением свободы на срок до 4-х лет или лишением свободы на срок до 5-ти лет.

В Уголовном кодексе Украины предусмотрена ответственность за следующие виды преступлений:

– незаконный сбор с целью использования или использование сведений, составляющих коммерческую или банковскую тайну (статья 231);

– разглашение коммерческой или банковской тайны (статья 232).

Проанализируем данные статьи.

1. Незаконный сбор с целью использования или использование сведений, составляющих коммерческую или банковскую тайну.

Умышленные действия, направленные на получение сведений, которые составляют коммерческую тайну, с целью разглашения или другого использования этих сведений (коммерческий шпионаж), а также незаконное использование таких сведений, если это нанесло существенный вред субъекту хозяйственной деятельности, наказываются штрафом от двухсот до тысячи не облагаемых минимумов доходов граждан или ограничением свободы сроком до пяти лет или лишением свободы сроком до трех лет.

Данная статья содержит два состава преступления: 1) незаконный сбор с целью использования сведений, которые составляют коммерческую тайну; 2) незаконное использование сведений, которые содержат коммерческую тайну, если это нанесло предприятию существенный экономический ущерб.

Научно-практический комментарий к Уголовному кодексу Украины трактует первый состав преступления как активные действия, направленные на добывание (получение) таких сведений любым способом: исключение, в том числе похищение документов, которые содержат коммерческую тайну, незаконное ознакомление с такими документами или предметами любым способом, прослушивание телефонных разговоров, подслушивание устных бесед, опрос сотрудников предприятия, получение таких сведений от лиц, которые владеют ими, путем подкупа, угроз.

Преступление в этой форме считается законченным с момента осуществления действий, направленных на незаконный сбор сведений, которые составляют коммерческую тайну, независимо от их последующего использования.

Субъективная сторона данного деяния характеризуется лишь прямым намерением.

Обязательным признаком субъективной стороны является цель – последующее использование незаконно собранных сведений, которые составляют коммерческую тайну:

– для собственных потребностей, например для внедрения в производство;

– продажа или безоплатная передача другим субъектам предпринимательской деятельности;

– разглашение с целью причинения материального или другого вреда субъекту предпринимательской деятельности;

– требование вознаграждения или осуществление определенных действий за возвращение или неразглашение собранных сведений, которые содержат коммерческую тайну.

Мотивы незаконного сбора сведений, которые содержат коммерческую тайну, персоналом предприятия, как правило, корыстные.

Второй состав преступления трактуется как внедрение «технических» секретов в собственное производство, учет полученных сведений, при планировании собственной предпринимательской деятельности, продажа сведений, которые составляют коммерческую тайну, и т. п.

Обязательным признаком объективной стороны данного преступления является наличие значительного материального убытка, который превышает в 50 раз и более установленный законодательством минимальный размер заработной платы.

При определении убытка учитываются:

– прямой материальный ущерб;

– расходы на ликвидацию последствий от использования сведений другими субъектами предпринимательской деятельности;

– убытки от снижения реализации продукции (товаров, услуг);

– расходы, связанные с вынужденным перепрофилированием;

– убытки от падения цен.

Моральный убыток, нанесенный предприятию использованием сведений, которые составляют коммерческую тайну, на квалификацию преступления не влияет, но учитывается при определении меры наказания.

Субъективная сторона преступления предусматривает обязательное наличие намерения. Виновное лицо должно осознавать, что незаконно использует сведения, которые составляют коммерческую тайну.

Для квалификации данного состава преступления не суть важно, кем были собраны незаконно используемые сведения, которые представляют собой коммерческую тайну.

2. Разглашение коммерческой тайны.

Умышленное разглашение коммерческой тайны без согласия ее владельца лицом, которому эта тайна стала известна в связи с профессиональной или служебной деятельностью, если оно осуществлено из корыстных или других личных побуждений и нанесло существенный вред субъекту хозяйственной деятельности, наказывается штрафом от двухсот до пятисот не облагаемых налогом минимумов доходов граждан, с лишением права занимать определенные должности или заниматься определенной деятельностью сроком до трех лет или исправительными работами сроком до двух лет, или лишением свободы на тот же срок.

Разглашение коммерческой тайны являет собой незаконное ознакомление других лиц со сведениями конфиденциального характера, отнесенными пред-

приятием к коммерческой тайне, а также преднамеренное создание условий, направленных на ознакомление с ними посторонних лиц, совершенное лицом, которому такие сведения стали известны в связи с профессиональной или служебной деятельностью и которое обязано такие сведения хранить в секрете.

Способы разглашения сведений, которые составляют коммерческую тайну, могут быть самыми разнообразными, например:

– сообщение таких сведений третьим лицам, в частности конкурентам;

– предоставление для ознакомления третьим лицам документов и других носителей информации, которые содержат коммерческую тайну;

– опубликование в средствах массовой информации сведений, которые содержат коммерческую тайну.

Обязательным признаком объективной стороны преступления является наличие существенного материального убытка – в размере 50 и более установленных законодательством минимальных заработных плат.

Нанесение предприятию морального убытка в результате разглашения коммерческой тайны, например ухудшение деловой репутации, данный состав преступления не образует.

Субъективная сторона преступления характеризуется прямым намерением и специальными мотивами – корыстным или другими личными мотивами.

Субъектами данного преступления наряду с сотрудниками предприятия могут быть представители правоохранительных, контролирующих и других государственных органов, банковских структур и т. п., которым такие сведения стали известны в процессе выполнения служебных обязанностей и которые обязаны хранить в секрете полученную информацию.

Возбуждать уголовные дела по факту разглашения коммерческой тайны в соответствии со статьей 4 Уголовно-процессуального кодекса Украины имеют право: суд, прокуратура и органы дознания на основании заявления потерпевшей стороны.

Говоря о практике применения уголовного законодательства, следует отметить, что случаи обращения с заявлениями в правоохранительные органы довольно редки. Как правило, если кто-то из предпринимателей и знает о существовании статьи 183 Уголовного кодекса Российской Федерации, то считают, что данная статья закона «не работает» и, следовательно, никто никого привлекать к уголовной ответственности не будет.

Однако практика расследования таких дел существует. Правоохранительные органы в последние годы стали расследовать подобные преступления. Так, в Свердловской области были случаи возбуждения уголовных дел по статье 183 Уголовного кодекса Российской Федерации. Рассмотрим некоторые из них.

Первое уголовное дело по факту хищения коммерческой информации было возбужденно УФСБ по Свердловской области в 2003 году. Тогда контрразведчики выявили факт несанкционированного копирования документов на «Уралмашзаводе» – якобы в интересах коммерческих фирм. В офисе этих компаний провели обыски, две сотрудницы «Уралмашзавода» написали явку с повинной. К следствию были привлечены спецслужбы других регионов России и зарубежных государств. Однако вскоре руководство «Уралмашзавода» офици-

ально заявило, что правонарушение было обнаружено сотрудниками «Уралмашзавода», нанесенный ущерб составляет незначительную сумму. Уголовное дело закрыли.

В декабре 2007 года был осужден к штрафу менеджер по сбыту Череповецкого металлургического комбината ОАО «Северсталь», который по электронной почте направил закрытые сведения о ценах на продукцию «Северстали» своему знакомому предпринимателю, получив за это 250 тысяч рублей.

Интересное уголовное дело по статье 183 Уголовного кодекса Российской Федерации было рассмотрено в одном из районных судов Екатеринбурга. В феврале 2007 года из одной организации уволились два менеджера по продажам. При их увольнении из офиса пропали бумажные документы, которые содержали сведения, составляющие коммерческую тайну («клиентская база»), а из компьютеров исчезли соответствующие файлы. Выяснилось, что, еще работая в этой организации, правонарушители учредили свою компанию с аналогичной сферой деятельности. При этом они значительно завышали цены на продукцию, выставляемую в счетах потенциальным клиентам (с помощью программы 1С) от имени компании, где они работали по трудовому договору, после чего взамен таких счетов (с умышленно завышенной ценой товара) предлагали по заниженным ценам товар в счетах учрежденной ими организации. Таким образом, они заключали договоры с заказчиками в интересах своей организации, незаконно используя сведения, составляющие коммерческую тайну, в ущерб интересам обладателя коммерческой тайны, с корыстной целью, что отрицательно влияло на нормальную работу организации, подрывало конкурентоспособность предоставляемого ими товара на рынке. Уволившись, бывшие менеджеры, вопреки подписанным обязательствам о неразглашении коммерческой тайны, активно использовали сведения, составляющие коммерческую тайну, которые им стали известны на прежней работе. Представителям потерпевшей организации пришлось обратиться с заявлением в районное управление внутренних дел.

Ответственность за утрату конфиденциальной информации (через неправомерные действия работников) может наступить и для работодателя, если эта информация относится к какому-либо виду служебной тайны. Если, допустив раскрытие коммерческой тайны, работодатель рискует лишь своим бизнесом, то при незаконном распространении персональных данных, тайны банковского вклада, врачебных данных и других охраняемых законом сведений последствиями для фирмы может быть возмещение убытков и морального вреда пострадавшим лицам, а для ее должностных лиц (не исключая и руководителя) – административная или уголовная ответственность.

Арбитражные суды в такой же ситуации порой занимают противоположную позицию. Интересно в этом отношении постановление Тринадцатого арбитражного апелляционного суда по иску Управления ФАС и ЗАО «А.Д.Д.» к ООО «АЕГЭ», основанному бывшими менеджерами «А.Д.Д.». Суть дела аналогична – работники, уйдя из «А.Д.Д.», создали свою компанию, занимающуюся тем же, что и бывший работодатель, предлагая ту же продукцию клиентам «А.Д.Д.». В доказательство хищения коммерческих секретов были представле-

ны логи, свидетельствующие об отправке работником с электронного адреса, расположенного на сервере ЗАО «А.Д.Д.», сообщений с прикрепленными файлами на иной внешний адрес, принадлежащий ему же. Однако суд решил, что истцы не представили доказательств передачи именно информации, составляющей коммерческую тайну, а также отправки сообщений именно бывшим работником, так как доступ к электронному адресу, названному судом «спорным» и расположенному на сервере ЗАО «А.Д.Д.», имели и иные лица в частности, системный администратор и сотрудники службы безопасности ЗАО «А.Д.Д.». Более того, суд посчитал, что, поскольку в иске речь шла о поставщиках и потребителях продукции ЗАО «А.Д.Д.», сведения о которых включены в Единый государственный реестр юридических лиц, ООО «АЕГЭ» вполне могло и самостоятельно получить эту информацию из отрытых источников, и в соответствии с Федеральным законом «О коммерческой тайне» она считается полученной законным способом, несмотря на то что ее содержание может совпадать с содержанием сведений, составляющих коммерческую тайну, обладателем которой является другое лицо.

Постановлением Тринадцатого арбитражного апелляционного суда было отменено предписание Управления ФАС о прекращении ООО «АЕГЭ» нарушения антимонопольного законодательства (в форме недобросовестной конкуренции). Суд отметил, что при вынесении решения Управлением ФАС не исследовался вопрос о соблюдении третьими лицами режима коммерческой тайны, а именно об обеспечении сохранности конфиденциальности коммерческой тайны, а в оспоренном решении антимонопольного органа не нашло отражения то обстоятельство, что третьими лицами в целях охраны коммерческой тайны были соблюдены все требования законодательства Российской Федерации.

В совершенно аналогичной ситуации Октябрьский районный суд Новосибирска в 2011 году осудил бывших менеджеров ООО «Сибпластком-1» за незаконное использование сведений, составляющих коммерческую тайну (часть 3 статьи 183 УК РФ), которые при увольнении скопировали клиентскую базу ритейлера (состоящую из юридических лиц) и открыли фирму подобного профиля, «переманив» часть деловых партнеров конкурента. Возможность самостоятельного создания такой базы подозреваемыми судом не рассматривалась.

Арбитражные суды довольно строго подходят к полноте реализации предписанных законом режимных мер. Так, рассматривая иск ОАО «Уралвагонзавод» к конкурентам, воспользовавшимся его технологической документацией, арбитражный суд Волго-Вятского округа согласился с выводами предыдущих судов о непринятии истцом, пострадавшим от хищения чертежей своей продукции, всех необходимых мер для охраны конфиденциальности информации. В ходе слушаний было установлено, что «Уралвагонзавод» не смог представить доказательств нанесения грифа «Коммерческая тайна» на документы, содержащие информацию, составляющую коммерческую тайну, и это свидетельствует о неполноте принятия предусмотренных законом охранных мер. Режим коммерческой тайны считается установленным после выполнения ее обладателем всех требований, прописанных в части 1 статьи 10 Федерального закона «О коммерческой тайне». И нанесение ограничительного грифа с указанием

обладателя информации, составляющей коммерческую тайну, и его места нахождения является таким же обязательным, как наличие перечня информации, составляющей коммерческую тайну, или трудовых договоров с работниками, допущенными к секретам.

Статья 21. Ответственность за непредоставление органам государственной власти, иным государственным органам, органам местного самоуправления информации, составляющей коммерческую тайну

Невыполнение обладателем информации, составляющей коммерческую тайну, законных требований органов государственной власти, иных государственных органов, органов местного самоуправления о предоставлении им информации, составляющей коммерческую тайну, а равно воспрепятствование получению должностными лицами этих органов указанной информации влечет за собой ответственность в соответствии с законодательством государства-участника.

Комментарий к статье 21

Ответственность за невыполнение обладателем информации, составляющей коммерческую тайну, требований государственных органов, органов местного самоуправления о предоставлении данной информации и (или) за воспрепятствование ее получению должностными лицами указанных органов может наступить лишь в том случае, если такие требования (соответственно, и действия должностных лиц, направленные на получение информации, составляющей коммерческую тайну) законны, т. е. они должны быть обоснованны и аргументированны, а главное – должны полностью основываться на законе, а не на ином, в том числе ведомственном, нормативном правовом акте.

Обратимся к судебной практике.

В ходе проверки сотрудники Управления Федеральной антимонопольной службы по Псковской области направили письмо-запрос в ЗАО «Псковпищепром» с требованием представить информацию об объеме реализации алкогольной продукции за 2006 год в натуральном выражении и перечень хозяйствующих субъектов, приобретающих продукцию у общества, с указанием их наименования и места нахождения. ЗАО «Псковпищепром» проигнорировало данный запрос и не предъявило необходимые документы, сославшись на то, что данная информация относится к разряду коммерческих тайн. Федеральная антимонопольная служба оштрафовала закрытое акционерное общество на 50 тысяч рублей. ЗАО «Псковпищепром» обратилось в суд.

Федеральный арбитражный суд Северо-Западного округа в постановлении от 11 октября 2007 года № А52-594/2007 вынес решение, что компании обязаны представлять Федеральной антимонопольной службе информацию по требованию, даже если она относится к коммерческой тайне. Вынося решение по данному делу, судьи указали, что запрос ведомства был подписан уполномоченным должностным лицом управления, содержит цель, правовое основание затребования информации и срок ее представления. Также отмечено, что на антимонопольный орган возложена обязанность по соблюдению коммерческой,

служебной, иной охраняемой законом тайны. Таким образом, арбитры встали на сторону антимонопольной службы.

Приняты на тридцать девятом
пленарном заседании
Межпарламентской Ассамблеи
государств – участников СНГ
(постановление № 39-15 от 29 ноября 2013 года)