



К.В. Прохин

Защита коммерческой тайны

- Особенности коммерческой тайны
- Порядок признания информации коммерческой тайной
- Способы защиты информации от несанкционированного разглашения
- Ответственность за нарушение коммерческой тайны



ГРОС
2010

ИНСТРУКЦИЯ ПО ВЫЖИВАНИЮ

Пронин К.В.

Защита коммерческой тайны (инструкция по выживанию)

Издательство ГроссМедиа
Год выпуска 2006 ISBN
5476003096

Описание книги

Что такое коммерческая тайна? Это право предприятия на сохранение в тайне своих производственных, торговых и финансовых операций, а также соответствующей документации. Но зачастую многие бизнесмены, предприниматели и другие хозяйствующие субъекты не знают, как правильно трактовать то или иное понятие из закона "О коммерческой тайне", какие именно сведения относятся к коммерческой тайне, насколько можно приоткрывать занавес для партнеров, конкурентов, государственных органов, чтобы не повлечь негативных последствий для своего предприятия. В этой книге дается определение коммерческой тайны и других видов конфиденциальной информации, рассказывается о методике, в соответствии с которой информация может быть отнесена к коммерческой тайне, о ситуациях, в которых государственные органы власти могут потребовать информацию, составляющую коммерческую тайну, и об охране конфиденциальности при этом, освещаются способы защиты такой информации от утечки, промышленного шпионажа, разглашения и несанкционированного доступа. Особенностью этой книги является то, что в ней описаны методы работы с персоналом, имеющим доступ к коммерческой информации, о правах и обязанностях работника и работодателя в случае возникновения спорных ситуаций. В конце книги приведен краткий словарь терминов и перечень основных законодательных актов и документов, актуальных при работе с коммерческой тайной. Для руководителей всех уровней, бизнесменов, предпринимателей и других обладателей информации, составляющей коммерческую тайну, участников предпринимательской деятельности, а также студентов, аспирантов и преподавателей профессиональных юридических и экономических образовательных учреждений.

Защита коммерческой тайны (инструкция по выживанию)

Введение

Успех любой коммерческой деятельности во многом зависит от грамотного обращения с информационными потоками. В условиях рыночной экономики информация является товаром, и ее получение, хранение, передача и использование подчиняются законам товарно-денежных отношений. Каждый субъект предпринимательской деятельности имеет право охранять свои интересы и защищать ценную для него информацию, получая при этом определенную свободу предпринимательства. Одним из старейших методов охраны такой информации является правовой институт коммерческой тайны. Задолго до возникновения понятия интеллектуальной собственности ремесленники во всем мире хранили в тайне секреты своего мастерства. Такие секреты передавались в устной форме из поколения в поколение, от отца к сыну. Патриархальный характер семьи гарантировал сохранность древних "ноу-хау". С наступлением эры научно-технической революции ситуация резко изменилась. Сложные производственные процессы и система деловых отношений, быстрое внедрение новых технологий требовали введения письменной документации и обусловили рост количества наемных работников, которые могли свободно менять работодателя. Все это привело к возникновению серьезной угрозы для секретов производства. Такая угроза исходила, во-первых, от "нелояльных" работников, осведомленных по роду своей деятельности с секретными сведениями, а, во-вторых, от несанкционированной утечки документации. Все это привело к необходимости установления правовых основ защиты коммерческой тайны, имеющей коммерческую ценность в рамках законодательства о борьбе с недобросовестной конкуренцией.

В нашей стране, где на протяжении 70 лет господствовала планово-административная экономика, данный вид регулирования не был востребован и практически отсутствовал. Впервые право на сохранение коммерческой тайны хозяйствующими субъектами было установлено Законом СССР от 4 июня 1990 г. "О предприятиях в СССР". В статье 33 указанного Закона вводилось понятие коммерческой тайны, как не являющихся государственными секретами сведений, связанных с производством, технологической информацией, управлением, финансами и другой деятельностью предприятий, разглашение (передача, утечка) которых может нанести ущерб их интересам. В настоящее время российское законодательство об охране коммерческой тайны представляет собой совокупность норм, которые содержатся в различных правовых актах и обеспечивают правовую защиту предпринимательских секретов во всех сферах общественных отношений.

Вопросам защиты коммерческой тайны в настоящее время уделяется все больше внимания. Статистика свидетельствует о значительном росте за последние годы экономических преступлений, в том числе, связанных с незаконным получением и оборотом информации, составляющей коммерческую тайну. И это не удивительно - получение незначительной информации о конкуренте может сэкономить фирме огромные средства, что является достаточно сильным стимулом для нарушения законов, регулирующих отношения в области информации. Поэтому большинство коммерческих компаний придают огромное значение таким категориям, как "коммерческая тайна", "ноу-хау". Обеспечение сохранности информации о деятельности компании является условием ее выживания в рыночной конкурентной среде. По оценкам экспертов, потеря лишь четверти информации, относимой к категории коммерческой тайны, обеспечивает весомые преимущества конкурентам и в течение нескольких месяцев приводит к банкротству половины фирм, допустивших утечку сведений. О необходимости создания надежного механизма защиты коммерческой тайны говорит и тот факт, что в развитых странах коммерческие компании, по данным экспертов, выделяют на борьбу с экономическим шпионажем до 20 процентов получаемой чистой прибыли.

Однако практика показывает, что зачастую многие отечественные предприниматели не совсем четко ориентируются в законодательстве по данному вопросу, не знают, какие именно сведения относятся к коммерческой тайне, в какой мере возможен допуск к ней партнеров, конкурентов, государственных органов. Чтобы не повлечь негативных последствий для своего предприятия, и всем правовым, организационным и техническим мерам защиты их руководители нередко предпочитают старый добрый сейф. В этой книге дается определение коммерческой тайны и других видов конфиденциальной информации, рассказывается о методике, в соответствии с которой информация может быть отнесена к коммерческой тайне, о ситуациях, в которых государственные органы власти могут потребовать информацию, составляющую коммерческую тайну, и об охране конфиденциальности. При этом освещаются способы защиты такой информации от утечки, промышленного шпионажа и разглашения. Особенностью этой книги является то, что в ней описаны методы работы с персоналом,

имеющим доступ к коммерческой информации, права и обязанности работника и работодателя в случае возникновения спорных ситуаций. В конце книги приведен перечень основных законодательных актов, регламентирующих вопросы организации работы со сведениями, составляющими коммерческую тайну.

Глава 1. Что такое коммерческая тайна?

1.1. Конфиденциальная информация

Для того чтобы ответить на вопрос, что же такое коммерческая тайна, прежде всего необходимо разобраться с теми основополагающими понятиями, на которых она базируется.

Начнем рассмотрение с такой правовой категории, как "информация". Слово "информация" имеет латинское происхождение и в переводе означает "знакомиться", "излагать", "разъяснять". В связи с тем, что данный термин в настоящее время используется в самых разных отраслях человеческой деятельности, единого толкования термина "информация" не существует. Для того чтобы избежать разночтений при его использовании, необходимо четкое законодательное определение. Согласно статье 2 Федерального закона от 20 февраля 1995 г. N 24-ФЗ "Об информации, информатизации и защите информации", информация представляет собой разнообразные сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

В законодательстве Российской Федерации имеется и другая формулировка для определения термина "информация". Она вытекает из приведенного в Законе РФ от 27 декабря 1991 г. N 2124-1 "О средствах массовой информации" (далее - Закон о СМИ) содержания понятия "массовая информация" - это предназначенные для неопределенного круга лиц печатные, аудио-, аудиовизуальные и иные сообщения и материалы. Если исходить из того, что специализированное понятие "массовая информация" образуется от более общей категории "информация" посредством уточняющей формулировки "предназначенные для неопределенного круга лиц", то можно сделать следующий вывод: информация - это печатные, аудио-, аудиовизуальные, иные сообщения и материалы. Таким образом, как мы видим, один закон понимает под информацией сведения, другой - сообщения и материалы. С точки зрения лингвистики, понятия "сведения" и "сообщения" являются синонимами, так как определяются друг через друга (следует заметить, что, по мнению ряда ученых-цивилистов, "сведения" составляют содержание "сообщений"). Однако нельзя не заметить, что в Законе о СМИ термин "сообщения" используется законодателем неотрывно от термина "материалы". Две приведенные формулировки отражают различные подходы к пониманию сущности информации. Принципиальное отличие второго подхода - представление информации исключительно в "овеществленном" виде, т.е. на каком-либо материальном носителе.

Все это можно было бы воспринять как отвлеченные научные теории, если бы в ряде случаев от применения той или иной концепции при толковании правовых норм мы не получали бы юридически значимые последствия, существенным образом отличающиеся друг от друга. Так, согласно статье 3 Федерального закона от 29 июля 2004 г. N 98-ФЗ "О коммерческой тайне", под "передачей информации, составляющей коммерческую тайну" понимается передача информации, зафиксированной на материальном носителе. Вместе с тем, при определении там же термина "разглашение" законодатель подчеркивает, что несанкционированное получение информации третьими лицами может осуществляться "в любой возможной форме" (например, устной).

По категориям доступа всю информацию можно условно разделить на две основные категории: открытую (общедоступную) и с ограниченным доступом. В свою очередь, информация с ограниченным доступом по своей правовой природе также подразделяется на два вида: сведения, составляющие государственную тайну; конфиденциальная информация.

Если информация не подпадает ни под один из двух вышеназванных видов, то она является открытой.

Термин "конфиденциальная информация" определяется статьей 2 Закона "Об информации, информатизации и защите информации", как "документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ". Порядок отнесения информации к конфиденциальной и виды конфиденциальной информации установлены Указом Президента РФ N 188 от 6 марта 1997 г. "Об утверждении перечня сведений конфиденциального характера", в соответствии с которым к конфиденциальной информации относятся:

- 1) сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в СМИ в установленных федеральными законами случаях;
- 2) сведения, составляющие тайну следствия и судопроизводства;

-
- 3) служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом РФ и федеральными законами (служебная тайна);
 - 4) сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее);
 - 5) сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом РФ и федеральными законами;
 - 6) сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них и некоторые другие.

Вернемся к рассмотрению понятия "информация, составляющая коммерческую тайну". Как мы видим, коммерческая тайна является одним из видов конфиденциальной информации. Указ определяет ее как "сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом РФ и федеральными законами". Данное определение носит отсылочный характер. Центральное место среди правовых источников, определяющих статус коммерческой тайны, занимает Гражданский кодекс Российской Федерации (ст. 139), в соответствии с которым "информация составляет 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".

В законе "О коммерческой тайне" используется несколько иной подход: законодатель разделяет понятия "коммерческая тайна" и "информация, составляющая коммерческую тайну". Согласно пункту 1 вышеназванного закона коммерческая тайна - это "конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду". В статье 139 Гражданского кодекса РФ закон использует термин "информация, составляющая коммерческую тайну", под которой понимается "научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе, составляющая секреты производства (ноу-хау), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании, и в отношении которой обладателем такой информации введен режим коммерческой тайны". В свою очередь, под режимом коммерческой тайны понимаются введенные правообладателем меры по охране конфиденциальности такой информации. Представляется, что разделение понятий "коммерческая тайна" и "информация, составляющая коммерческую тайну" носит искусственный характер и не может считаться полезным с точки зрения практического применения. Кроме того, такой подход противоречит статье 139 Гражданского кодекса РФ. В литературе по данному вопросу в подавляющем большинстве используется именно термин "коммерческая тайна", поэтому в дальнейшем мы будем использовать эти два термина как синонимы.

Перейдем к анализу установленных законодателем условий, которые позволяют говорить о принадлежности информации к категории "коммерческая тайна".

1.2. Понятие коммерческой тайны и его правовая природа

1.2.1. Коммерческая ценность

Итак, во-первых, коммерческая тайна - это информация, обладающая коммерческой ценностью. Ценность информации - комплексный показатель ее качества, мера пригодности для принятия решений в конкретной сфере. Таким образом, под коммерческой ценностью информации понимается ее пригодность (полезность) для выработки тех или иных решений в сфере коммерческой деятельности. Приведенная интерпретация коммерческой ценности в основном справедлива для "внешней" информации. В качестве примера можно привести результаты маркетинговых исследований, проводимых фирмой, с целью изучения приоритетных направлений развития производства. Практика показывает, что степень полезности определяется тремя компонентами:

- 1) достоверность
- 2) актуальность
- 3) полнота информации*(1).

Вся информация, поступающая извне, характеризуется определенной степенью достоверности. Владение достоверной информацией и рациональное ее использование создают условия оптимального

управления бизнесом. Напротив, искаженные сведения, сведения о несуществующих фактах и событиях, особенно в случае целенаправленной дезинформации, априори не могут быть отнесены к коммерческой тайне - принятые на их основе решения могут повлечь значительные убытки, коммерческая ценность такой информации является "отрицательной" величиной. Степень достоверности информации зависит, прежде всего, от уровня надежности источника. С целью оптимального использования полученных сведений полезно их классифицировать в зависимости от предоставившего их источника: А - абсолютно надежный и компетентный; В - обычно надежный; С - не всегда надежный; D - ненадежный; Е - неопределенный. Однако полагаются только на уровень достоверности источника при оценке полученной информации не следует. Бывают ситуации, когда от источника класса "А" может поступить явная дезинформация. Наиболее достоверная информация - это информация, которая подтверждается другими фактами.

Актуальность применительно к информации определяется такими ее характеристиками, как "своевременность" и "относимость". Коммерческая ценность даже самой достоверной информации может быть сведена к нулю, если она поступила в распоряжение фирмы, когда момент для принятия коммерчески значимого решения уже упущен. То же можно сказать и об информации, по всем признакам подпадающей под категорию коммерчески ценной, но весьма далекой от сферы деятельности компании. Вряд ли фирма, занимающаяся изготовлением пластиковых окон, сможет извлечь пользу из информации, касающейся технологии производства пятирезонаторных пролетных клистронов.

Последним компонентом, определяющим "степень полезности" коммерческой информации, является ее полнота. Иногда вовсе не обязательно обладать всеми знаниями по конкретному вопросу, достаточно иметь представление о наиболее значимых элементах всего информационного массива. С другой стороны, отдельный незначительный компонент коммерческой информации не позволяет найти его эффективное применение. Таким образом, под "полнотой" понимается достаточность информации для принятия соответствующего решения. Аналогичный подход к определению информации, составляющей коммерческую тайну, применяется и в Соглашении по торговым аспектам прав интеллектуальной собственности - ТРИПС (Agreement on Trade-Related Aspects of Intellectual Property Rights - TRIPS). Этот международный договор является эталоном для законодательства стран-участниц Всемирной Торговой Организации в области защиты интеллектуальной собственности, включая коммерческую тайну. Согласно пункту 2 статьи 39 Соглашения, "секретной" (в отечественной терминологии - "конфиденциальной") может являться информация, которая в целом или в определенной конфигурации и подборе ее компонентов не является общеизвестной или легко доступной. То есть, в рамках института коммерческой тайны правовое значение может иметь подбор компонентов информации ("конфигурация").

Законодатель в статье 139 Гражданского кодекса РФ обращает внимание на то, что коммерческой ценностью обладает не только информация, позволяющая получить определенную выгоду в данный момент времени (действительная ценность), но и сведения, которые могут обрести ценность в будущем (потенциальная ценность).

Критерий неизвестности коммерчески значимой информации третьим лицам является ключевым критерием. Если в какой-либо из отраслей производства подавляющее количество предприятий используют одни и те же технологии для изготовления определенной продукции, такой технологический процесс нужно рассматривать как общеизвестный прием производства, но ни в качестве информации, составляющей коммерческую тайну. Ни у кого не вызывает сомнения абсурдность требований редакции какой-либо массовой газеты с многотысячными тиражами запретить своим читателям "разглашать" напечатанные материалы из колонки новостей*(2). Поэтому ситуации, когда потребители услуг пользуются ресурсами одного поставщика информации (например, агентства, транслирующего биржевую информацию) и при этом называются потребителями информации, "составляющей коммерческую тайну", и, следовательно, принимают на себя обязательства по сохранению ее в тайне, лишены правовой основы. Ведь зачастую число таких потребителей может превышать тиражи многих массовых СМИ. Для обладателя коммерческой тайны ее коммерческая ценность проявляется в наличии определенных экономических преимуществ по сравнению с третьими лицами, не располагающими данной информацией. В российском законодательстве о коммерческой тайне отсутствуют четкие критерии для придания тому или иному лицу статуса "третьего". В данном вопросе подход зарубежных законодателей, понимающих под третьими лицами тех, для кого эти сведения составляют коммерческий интерес, представляется весьма обоснованным. Так, ТРИПС сужает круг третьих лиц до профессионалов, к числу которых могут относиться другие субъекты предпринимательской деятельности, конкурирующие с обладателем коммерческой тайны, его контрагенты по хозяйственным обязательствам, потребители его продукции, работ и услуг. Согласно положениям ТРИПС, если коммерческая информация легко доступна достаточно широкому кругу профессионалов, на нее не может быть распространена правовая режима коммерческой тайны. При этом такая информация может оставаться недоступной простому обывателю в силу объективных причин (например, отсутствие

специальных познаний или навыков работы в определенной сфере, аккредитации на осуществление какой-либо деятельности и т.д.).

Далеко не всем известно, какие акции пользуются повышенным спросом сегодня, но эта информация не является коммерческой тайной, так как широко доступна биржевым брокерам, которые входят "в круг лиц, имеющих дело сданной информацией".

1.2.2. Недоступность на законном основании

Вторым признаком информации, составляющей коммерческую тайну, согласно статье 139 Гражданского кодекса РФ, является ее недоступность на законном основании. Если соответствующие сведения могут быть без труда получены законным образом любым заинтересованным лицом, например, путем изучения открытых данных, знакомства с публикациями и тому подобного, такая информация коммерческой тайной не признается (не следует путать получение информации, составляющей коммерческую тайну, с помощью специальных методов, например, "деконструирования", или "обратного инжиниринга", которые мы рассмотрим ниже, с получением открытой информации из различных источников).

Все способы получения информации, составляющей коммерческую тайну, от ее обладателя могут быть разделены на две группы - законные и незаконные. Причем, наличие согласия обладателя такой информации на передачу ее другому лицу еще не обеспечивает стопроцентной гарантии, что такая передача осуществляется на законном основании. Данное утверждение справедливо для случаев, когда режим коммерческой тайны императивно распространяется на определенный вид информации на основании требований законодательных актов. Например, статья 15 Федерального закона от 7 мая 1998 г. N 75-ФЗ "О негосударственных пенсионных фондах" относит к коммерческой тайне сведения о состоянии пенсионных счетов и о производимых выплатах негосударственных пенсий. Передача такой информации фондом другому лицу (кроме оговоренных законом случаев) будет признана незаконной.

Критерием определения законности или незаконности получения информации конкретным способом является часть 4 статьи 4 Закона "О коммерческой тайне", устанавливающая, что "информация, составляющая коммерческую тайну, обладателем которой является другое лицо, считается полученной незаконно, если ее получение осуществлялось с умышленным преодолением принятых обладателем информации, составляющей коммерческую тайну, 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".

Из этой дефиниции следует определение "добросовестного приобретателя". Применение каких-либо санкций к третьему лицу, получившему информацию, составляющую коммерческую тайну, у лица, не имевшего права на ее передачу, исключается, если выполнены следующие условия: добросовестный приобретатель не знал и не должен был знать о том, что лицо, от которого получены эти сведения, не имело права на их распространение. В силу презумпции добросовестности участников гражданского оборота, закрепленной в пункте 3 статьи 10 Гражданского кодекса РФ, бремя доказывания неосторожности приобретателя информации возлагается на ее первоначального обладателя. Поэтому, если такие доказательства отсутствуют, добросовестный приобретатель вправе свободно использовать эти сведения в своей предпринимательской деятельности. Кроме того, законом на него не возлагаются никакие дополнительные обязательства перед первоначальным обладателем права на коммерческую тайну, кроме как принимать меры к обеспечению конфиденциальности полученных сведений. Однако приобретателю информации, составляющей коммерческую тайну, следует иметь полный пакет соответствующей документации, свидетельствующей о том, что эти сведения были получены на законных основаниях.

Своеобразным "способом" получения информации, составляющей коммерческую тайну, который, без сомнения, никак нельзя назвать противозаконным, является ее получение в результате небрежности обладателя тайны. Вопрос о правах и обязанностях "жертвы случая" определен в Законе "О коммерческой тайне" весьма неоднозначно. Так, согласно пункту 6 части 2 статьи 7 указанного Закона, обладатель информации, составляющей коммерческую тайну, имеет право "требовать от лиц, получивших доступ к информации, составляющей коммерческую тайну, в результате действий, осуществленных случайно или по ошибке, охраны конфиденциальности этой информации". При отказе в принятии таких мер обладатель имеет право требовать защиты своих прав в судебном порядке (ч. 5 ст. 14). Во-первых, из текста Закона не ясно, что подразумевается под "действиями, осуществленными случайно или по ошибке": кто действовал "случайно" или допустил ошибку. Если ошибку допустил обладатель информации, составляющей коммерческую тайну, то на каком основании закон накладывает

обязанность на "одаренного" принимать меры к охране конфиденциальности этой информации? А такие меры зачастую требуют определенных материальных затрат. Закон ничего не говорит о возможности "жертвы ошибки" переложить бремя заботы о чужих секретах на рассеянного обладателя. Еще одним пробелом в законе является вопрос - вправе ли лицо, получившее доступ к информации в результате случайности или ошибки, использовать полученные сведения для получения прибыли в своей предпринимательской деятельности наравне с первоначальным обладателем информации. Закон не содержит прямого запрета и, следуя принципу "что не запрещено - то разрешено", можно сделать вывод о правомочности нового обладателя информации на ее использование.

Согласно части 3 статьи 4 Закона "О коммерческой тайне" информация, составляющая коммерческую тайну, полученная от ее обладателя на основании договора или другом законном основании, считается полученной законным способом. Получение информации, составляющей коммерческую тайну, в рамках гражданско-правовых отношений на основании различных видов договоров, правовые основы обеспечения конфиденциальности информации, права и обязанности сторон будут подробно рассмотрены ниже, в [главе 5](#).

Еще одним способом получения коммерческой тайны, на который не распространяются запретительные положения, является так называемое "независимое открытие". Законность данного метода, вытекающая из самой правовой природы коммерческой тайны, закреплена в национальных законодательствах практически всех зарубежных стран и в нормах международного права (в том числе, соглашением ТРИПС). Такое единодушие не случайно. В противном случае были бы подорваны основы патентной системы, гарантирующей защиту от независимого открытия прав патентообладателя в обмен на обнародование им закрытой информации и передачу ее в общее пользование после окончания срока действия патента. Россия в этом вопросе не является исключением - согласно части 2 статьи 4 Закона "О коммерческой тайне", 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 информации, составляющей коммерческую тайну, обладателем которой является другое лицо. Лицо, сделавшее независимое открытие, также может придать ему статус коммерческой тайны. Таким образом, возникают два обладателя одного и того же секрета, которые даже не догадываются, что являются не единственными его "пользователями". Возможна совершенно законная ситуация, когда обладатель коммерческой тайны может наткнуться на подробное описание своего секрета в каком-нибудь общедоступном научном журнале. Ничего не мешает "независимому открывателю" опубликовать свои изыскания или выступить с ними на открытой конференции и т.д.

Очень часто приходится сталкиваться с такой практикой: коммерческая компания целенаправленно и скрупулезно собирает сведения о фирме-конкуренте (или партнере по бизнесу). Специалисты относят такой сбор информации о конкурентах и других субъектах предпринимательской деятельности к обычному маркетингу и выделяют следующие основные направления, по которым производится сбор информации:

- 1) информация о рынке (цена, условия договоров, скидки, доля на рынке и тенденции ее изменения, рыночная политика и планы, численность и расстановка торговых агентов и так далее);
- 2) информация о производстве продукции (номенклатура изделий, оценка качества и эффективности, технология и оборудование, уровень издержек и так далее);
- 3) информация об организационных особенностях и финансах (выявление лиц, принимающих ключевые решения, и их философии, главных проблем, программ проведения научно-исследовательских работ и т.д.)*(3).

Собранная таким образом информация с помощью системного анализа позволяет получить полное представление о наиболее уязвимых местах другой компании, что значительно укрепляет собственные позиции в конкурентной борьбе. Однако методы сбора информации могут быть признаны противозаконными только в том случае, если обладатель коммерческой тайны сможет доказать не только то, что эта информация отвечала всем установленным законом критериям охраноспособности, но и что конкретное лицо получило доступ к ней, используя незаконные способы (то есть фактически необходимо доказать наличие обстоятельств, указанных в ч. 4 ст. 4 Закона "О коммерческой тайне"). Если правообладатель не сможет доказать эти обстоятельства, он не может рассчитывать на правовую защиту и возмещение понесенных убытков. Как показывает практика, при отсутствии прямых свидетельств использования оппонентом неправомερных способов получения коммерческой тайны практически невозможно доказать, что конкурент скопировал ваши ресурсы, а не получил информацию самостоятельно ("независимое открытие"). К сожалению, Закон "О коммерческой тайне" не расшифровывает понятия "неправомερные способы получения коммерческой тайны", хотя в редакции законопроекта, внесенного в Госдуму, такая дефиниция была: "неправомερные способы получения коммерческой тайны - сбор информации, составляющей коммерческую тайну, посредством похищения документов, подкупа или угрозы, дачи взятки, введения в заблуждение, нарушения или

подстрекательства (принуждения) к нарушению обязательств о соблюдении режима коммерческой тайны, а равно иным незаконным способом без согласия обладателя коммерческой тайны на передачу коммерческой тайны третьим лицам". Непонятно, какими соображениями руководствовались законодатели, изъяв из текста Закона эту норму, которая, кстати, соответствовала нормам Соглашения ТРИПС. Правоприменителю остается руководствоваться частью 1 статьи 183 Уголовного кодекса РФ, устанавливающей уголовную ответственность за соби́рание сведений, составляющих коммерческую, налоговую или банковскую тайну, путем "похищения документов, подкупа или угроз, а равно иным незаконным способом". Если информация является внутренней разработкой, сделанной работниками компании в ходе проведения различных исследований, чтобы избежать возможных осложнений в дальнейшем и снять все вопросы относительно законности ее получения, необходимо соответствующим образом фиксировать весь ход работ (например, в специальном журнале лабораторных работ). Целесообразно осуществлять видеозапись проводимых экспериментов и соответствующих комментариев разработчиков.

Близким по своей природе к "независимому открытию" способом получения сведений, составляющих коммерческую тайну, является так называемый обратный технический анализ или "обратный инжиниринг". Суть этого метода заключается в исследовании имеющегося в широкой продаже продукта с целью обнаружения секретов его работы или того, как он сделан. Так как источником информации при обратном инжиниринге выступает продукт, находящийся в широкой продаже, приобретаемый на законных основаниях ("законный источник"), такой способ получения информации, составляющей коммерческую тайну, по формальным признакам не может быть признан противозаконным. Методы борьбы с обратным техническим анализом можно разделить на технические (различные технические ухищрения, приводящие, например, к саморазрушению "секретных" структур продукта при попытке нарушить его целостность или произвести копирование) и юридические. Некоторые производители включают в договоры купли-продажи пункт о запрещении в отношении приобретаемого товара проведения обратного инжиниринга, но при массовых продажах это вызывает большие затруднения.

Массовый характер в международном масштабе приобрела проблема использования обратного инжиниринга в сфере информационных технологий. Производители компьютерных программных продуктов несут колоссальные убытки от его применения нечестными на руку конкурентами. Для того чтобы обуздать поборников этого метода, крупные компании в настоящее время во всем мире пытаются пролоббировать введение правовых мер защиты сразу по трем направлениям: они хотят ввести договорное использование своей продукции, обеспечить соблюдение авторских прав и исполнение условий международных договоров.

Первое направление, связанное с договорным использованием компьютерных программ, исходит из того, что право на это использование должно предоставляться на основании лицензии, а не продаваться. Во времена зарождения эры массовой компьютеризации число пользователей компьютеров было так мало, что компании - производители программных продуктов имели возможность вести переговоры о лицензионных соглашениях с каждым пользователем программ. При заключении таких соглашений производители включали в них положения, согласно которым пользователям было запрещено заниматься "обратным инжинирингом". Эти положения, в соответствии с общими принципами договорного права, надежно обеспечивали соблюдение договорных обязательств. С развитием компьютерной индустрии, когда количество персональных пользователей стало исчисляться сотнями миллионов, заключать персональные лицензионные соглашения с каждым из них стало практически нереальным. Чтобы хоть как-то обезопасить себя и свою продукцию от "взлома", производители программного обеспечения применяют так называемые "оберточные договоры". Они печатают текст лицензионного соглашения, запрещающего "обратный инжиниринг", на упаковке каждого продаваемого продукта (отсюда и название). Однако для полноценного использования "оберточных договоров" и придания им юридической силы требуется пересмотр отдельных принципов договорного права. Это связано с тем, что, в соответствии с действующими принципами договорного права, при заключении договора требуется обоюдное согласие заключающих его сторон.

Компании - производители компьютерных программ также применяют специальную функцию, не позволяющую произвести запуск программного продукта, пока пользователь не выразит свое согласие нажатием на специальную панель, которая высвечивается на экране всякий раз при запуске программы и содержит аналогичный текст лицензионного соглашения. Запуская программу, пользователь тем самым выражает свое согласие, что соответствует требованию договорного права о взаимном согласии сторон договора, но следует учитывать, что такая процедура, строго говоря, урезает права покупателя программы. Он платит за товар, а потом, уже после заключения договора купли-продажи, чтобы иметь возможность пользоваться покупкой, вынужден отказываться от части своих прав. По сути, это является нарушением со стороны продавца добросовестного намерения соблюдать договор купли-продажи. Решение этой проблемы - совместное использование "оберточных договоров" (дабы заранее уведомить

покупателя об определенных ограничениях его прав) и описанных выше специальных программных функций (с целью обеспечить "согласие" сторон на заключение соглашения).

Еще более эффективным методом борьбы с "обратным инжинирингом" является применение Интернета для заключения лицензионных соглашений с минимальными затратами (переговоры с миллионами клиентов ведет сервер компании-производителя). Использование интернет-технологий позволяет осуществлять выведение лицензионных требований на мониторе у потенциального покупателя программы и получать его выражение согласия на условия дополнительного соглашения до начала передачи ему программного продукта по сети. Хотя такая форма сделки не противоречит общим принципам договорного права, поскольку согласие на получение товара дается в момент уведомления о запрете проведения обратного инжиниринга, для ее "юридической чистоты" необходима четкая регламентация на законодательном уровне.

Еще одним подходом в борьбе с обратным техническим анализом компьютерных программ является использование правового института интеллектуальной собственности. Для проведения "обратного инжиниринга" программы, как правило, необходимы адаптация и копирование оригинального программного продукта, защищенного авторским правом. Согласно законодательству, исключительное право на копирование и адаптацию своих произведений имеет только обладатель авторского права. Но это общее правило в законодательстве по авторскому праву многих стран имеет ряд ограничений. В России согласно статье 15 Закона РФ от 23 сентября 1992 г. N 3523-1 "О правовой охране программ для электронных вычислительных машин и баз данных" пользователь программного продукта или базы данных имеет право осуществлять их адаптацию, то есть вносить в них изменения, осуществляемые исключительно в целях обеспечения функционирования программы для ЭВМ или базы данных на конкретных технических средствах пользователя или под управлением конкретных программ пользователя. Производимые изменения должны быть вызваны исключительно техническими причинами. Если компьютерная программа (или база данных) может бесперебойно функционировать на технических средствах пользователя и взаимодействовать с его программами, внесение в них каких-либо изменений запрещается. Безусловно, за автором программного продукта или базы данных сохраняется право на их модификацию. Кроме того, допускается изготовление копии программы для ЭВМ или базы данных при условии, что эта копия предназначена для архивных целей и для замены правомерно приобретенного экземпляра в случаях, когда оригинал программы для ЭВМ или базы данных утерян, уничтожен или стал непригоден для использования. Созданная пользователем копия программы или базы данных не может быть использована для иных целей и должна быть уничтожена в случае, если дальнейшее использование этих программных средств перестает быть правомерным.

При определенных условиях, согласно рассматриваемому закону, пользователь программного продукта может даже декомпилировать охраняемую законом программу как самостоятельно, так и с помощью других лиц. Декомпилирование заключается в преобразовании программного кода в исходный текст в целях изучения структуры и кодирования компьютерной программы. Однако это не означает, что пользователь может осуществлять "обратный инжиниринг". Законом установлено, что использование декомпилирования считается допустимым тогда, когда это необходимо для достижения способности к взаимодействию самостоятельно разработанной пользователем программы с другими программами, которые могут взаимодействовать с декомпилированной программой. При этом оговариваются три обязательных условия для осуществления декомпилирования:

- 1) информация, необходимая для достижения способности к взаимодействию, ранее не была доступна этому лицу из других источников;
- 2) указанные действия осуществляются в отношении только тех частей декомпилируемой программы для ЭВМ, которые необходимы для достижения способности к взаимодействию;
- 3) информация, полученная в результате декомпилирования, может использоваться лишь для достижения способности к взаимодействию независимо разработанной программы для ЭВМ с другими программами, не может передаваться иным лицам, за исключением случаев, если это необходимо для достижения способности к взаимодействию независимо разработанной программы для ЭВМ с другими программами, а также не может использоваться для разработки программы для ЭВМ, по своему виду существенно схожей с декомпилируемой программой для ЭВМ, или для осуществления любого другого действия, нарушающего авторское право (п. 2 ст. 25 Закона РФ от 9 июля 1993 г. N 5351-1 "Об авторском праве и смежных правах").

В ряде случаев возможность доступа определенной категории лиц к информации, составляющей коммерческую тайну, может быть обусловлена прямым требованием различных законодательных актов. Речь, прежде всего, идет о возможности затребования такой информации различными государственными органами в ходе выполнения возложенных на них функций. Вопросы, связанные с предоставлением информации, составляющей коммерческую тайну, будут подробнее рассмотрены ниже, в [главе 4](#). Здесь же отметим только, что возможность получения госорганами и их должностными лицами конфиденциальных сведений не означает утрату этими сведениями статуса коммерческой

тайны, поскольку доступ к информации имеют только конкретные лица в конкретных объемах, в обязанность которых входит обеспечение ее нераспространения.

Но правовыми актами законность доступа к определенной информации, даже если обладателем она отнесена к разряду коммерческой тайны, может быть установлена не только для государственных органов, но и для других субъектов. В качестве примера можно привести следующий прецедент из судебной практики. АО "Армейские инвестиции" подало в суд иск с целью обязать некоммерческое партнерство "Первая судоходная депозитарно-клиринговая компания" предоставить данные из реестра АО "Союз" о наименовании зарегистрированных в реестре владельцев и о количестве, категории и номинальной стоимости принадлежащих им ценных бумаг. Архангельский областной арбитражный суд иск "Армейских инвестиций" удовлетворил, признав, что "Первая судоходная депозитарно-клиринговая компания", которая является реестродержателем АО "Союз", согласно требованиям Федерального закона от 22 апреля 1996 г. N 39-ФЗ "О рынке ценных бумаг", обязана предоставлять требуемые сведения всем зарегистрированным лицам, владеющим одним процентом и более обыкновенных акций общества. "Армейские инвестиции" являются владельцем 1,2 процента от общего числа обыкновенных акций.

Но держатель реестра не собирался так просто расставаться с "секретной" информацией. Им была направлена кассационная жалоба в Федеральный арбитражный суд Северо-Западного округа. В жалобе ответчик приводил новый аргумент: запрос АО "Армейские инвестиции" о предоставлении сведений подписан председателем совета директоров без удостоверения его полномочий, кроме того, он не заверен печатью. Следовательно, передавать конфиденциальную информацию держателям акций нет оснований, кроме того, они могут использовать эту информацию во вред акционерам. Федеральный арбитражный суд с опасениями заявителя жалобы не согласился. Из первоначального ответа "Первой судоходной компании" на запрос "Армейских инвестиций" следует, что этот запрос был расценен, как исходящий от надлежущего лица. А отказ был мотивирован исключительно тем, что информация содержит коммерческую тайну и является конфиденциальной. Вопрос о предполагаемых действиях номинальных держателей акций, сказано в постановлении суда, не имеет отношения к предмету иска. Таким образом, как "Армейские инвестиции" могут распорядиться полученными сведениями - значения для данного спора не имеет. Лица, добровольно вступившие в сферу отношений, регулируемых Законом "О рынке ценных бумаг", тем самым обязались следовать тем нормам поведения, которые им установлены.

1.2.3. Меры по конфиденциальности

Третьим обязательным признаком информации, составляющей коммерческую тайну, согласно статье 139 Гражданского кодекса РФ является принятие мер обладателем к охране ее конфиденциальности. Спектр этих мер весьма обширен. Следует отметить, что при значимости всех названных выше условий охраноспособности коммерческой тайны последнее из них является, пожалуй, решающим. Вопросам организации многоуровневой системы защиты конфиденциальной информации в коммерческой компании посвящена [глава 6](#).

1.2.4. Правовая природа

Анализ юридической конструкции статьи 128 Гражданского кодекса РФ позволяет прийти к заключению, что информация, в том числе коммерческая тайна, является самостоятельным объектом гражданских прав. Гражданский кодекс РФ выделяет 5 групп объектов гражданских прав:

- 1) вещи, включая деньги и ценные бумаги, иное имущество, в том числе имущественные права;
- 2) работы и услуги;
- 3) информация;
- 4) результаты интеллектуальной деятельности, в том числе исключительные права на них (интеллектуальная собственность);
- 5) нематериальные блага.

Как мы можем видеть, информация, составляющая коммерческую тайну, не относится к имуществу, и, следовательно, на нее не может быть распространен режим права собственности. Статья 128 Гражданского кодекса РФ однозначно разделяет на отдельные классы информацию и объекты интеллектуальной собственности. Под объектами интеллектуальной собственности закон понимает творческие, нематериальные объекты, охраняемые особыми гражданско-правовыми законами. На эти объекты возникают исключительные права: на некоторые права появляются сразу после их создания, на другие - после государственной регистрации. До осуществления регистрации закон

называет такие объекты "способными к правовой охране". Первоначальные права на объекты интеллектуальной собственности принадлежат их авторам. К таким объектам относятся авторские произведения науки, литературы и искусства (включая компьютерные программы и базы данных), исполнения артистов-исполнителей, изобретения, полезные модели, промышленные образцы, топологии интегральных микросхем, селекционные достижения. Однако формулировки ряда норм Гражданского кодекса РФ, федеральных законов и международных договоров дают основание полагать о существовании исключительных прав и на информацию. В частности, Соглашение ТРИПС распространяет термин "интеллектуальная собственность" на все правовые категории, рассматриваемые в разделах 1-7 части II Соглашения (то есть и на информацию, составляющую коммерческую тайну). Такое смешение вызвано некоторым сходством правовой природы: объекты интеллектуальной собственности, как и коммерческая тайна, имеют нематериальный характер и являются результатом интеллектуальной деятельности. Но есть и принципиальное различие: в основе исключительного права (интеллектуальной собственности) лежит легальная монополия, подтверждаемая выдачей государственного документа (свидетельства или патента), а право на коммерческую тайну представляет собой фактическую монополию, которая весьма уязвима от целого ряда опасностей (промышленный шпионаж, возможность утечки по неосторожности и т.д.). Как отмечается в литературе, если обладатель новых знаний (ноу-хау) не хочет делиться ими с обществом, то и государство предоставляет их обладателю не исключительные права, а лишь охрану от несанкционированного заимствования этой информации третьими лицами, т.е., упрощая до аналогии с частной собственностью, охрану от воровства⁽⁴⁾. Право на защиту не носит срочного характера. Это вытекает из самой системы охраны ее конфиденциальности. Срок охраны ограничивается действием мер защиты от разглашения и утечки. Если же информация, составляющая коммерческую тайну, потеряла признак неизвестности третьим лицам и стала общедоступной, причем, не важно на законных или незаконных основаниях, она теряет охраноспособность и на нее перестает распространяться режим коммерческой тайны. Все это позволяет говорить о коммерческой тайне только как об объекте, примыкающем к объектам интеллектуальной собственности.

Появление двух сходных институтов, направленных на защиту коммерчески значимой информации, не случайно. Законодательство о коммерческой тайне призвано стимулировать развитие тех областей производства, где применение патентной защиты малоэффективно. Правовой институт коммерческой тайны может обеспечивать охрану секретов производства (ноу-хау), представляющих собой различные новаторские предложения, каждое из которых относительно мало, чтобы стать объектом патентования. Многие виды таких предложений, в принципе, непатентоспособны, поскольку не отвечают признакам новизны изобретения, но их совокупность становится уже весьма ценной. Поэтому возникает необходимость защитить их от конкурентов, желающих их тайно заимствовать и использовать. Для этого и нужен правовой институт ноу-хау (секретов производства), как один из видов коммерческой тайны.

Но этот институт применяется не только к непатентоспособным объектам. Сведения о патентоспособных объектах (до их официальной публикации) можно считать разновидностью как конфиденциальной информации в широком смысле⁽⁵⁾, так и информации, составляющей секреты производства (ноу-хау), но только при наличии трех обязательных признаков коммерческой тайны. С момента официального опубликования данных сведений изменяется их правовой режим - они переходят в ряд объектов интеллектуальной собственности.

Кроме этого, многие коммерческие компании зачастую предпочитают не патентовать изобретение, а отнести его к секретам производства. Следует подчеркнуть, что решение не подавать заявку на изобретение на патентоспособное техническое решение возможно только по письменной договоренности с автором, так как, по существующему правилу, если работодатель в течение трех месяцев с момента уведомления его автором о сделанном изобретении не подаст заявку на него, автор вправе сам подать заявку и получить патент.

Что же лучше: патентовать или сохранять информацию в режиме ноу-хау? Получение патента - процесс дорогостоящий и довольно длительный. Поэтому патентовать любое рационализаторское предложение или нововведение для компании может быть весьма накладно. Патент, без сомнений, хорош тем, что есть закон, который защищает его, устанавливая исключительные права патентообладателя. С другой стороны, обладатель патента сам должен отслеживать все нарушения его исключительных прав. У патента установлен срок и территориальные границы его действия. За пределами этих временных и территориальных границ он доступен любому лицу. Кроме того, возникает необходимость в уплате годовых пошлин за поддержание патента в силе. У ноу-хау нет срока и территории действия. С другой стороны, обеспечение режима конфиденциальности может потребовать гораздо больших материальных затрат. На ноу-хау может быть несколько собственников (вспомним про "независимые открытия", "обратный инжиниринг" и прочие головные боли обладателя коммерческой тайны). Прибегать к ноу-хау имеет смысл, когда нет денег на зарубежное патентование (ведь

информация о патентах попадает в Интернет и становится доступной для ознакомления во всех странах мира, где российский патент не обеспечивает никакой защиты). На практике особенно эффективным следует признать сочетание двух этих моделей защиты: изобретения или полезные модели патентуют, но информацию о технической сущности полностью не раскрывают. Таким образом, выполняя требования патентного ведомства, можно не раскрыть суть изобретения.

В качестве примера удачного сочетания ноу-хау и патентной защиты можно привести курьезный случай, имевший место на одном из заводов в городе Новочеркасске. Там провели сокращение штатов, под которое, как это всегда бывает, в первую очередь попали пенсионеры. Вскоре после этого пришел крупный заказ на изготовление колес с зубчатой конусоидальной передачей. Запустили заказ в производство - идет брак. И тут кто-то вспомнил, что был до сокращения на заводе специалист именно по этим колесам с зубчатой передачей. Обратились к "сокращенному" пенсионеру, который, естественно, не питал особо теплых чувств к администрации родного завода. А он говорит: у меня патент на изобретение. Нашли его патент и сделали все по описанной технологии - все равно один брак идет. Снова пришлось обращаться к автору-пенсионеру, а он говорит: у меня там было ноу-хау заложено. Могу отдать только за отдельную плату. Пришлось раскошелиться и за патент, и за "коммерческую тайну".

1.3. Охрана коммерческой тайны за рубежом

Большинство экономически развитых зарубежных стран имеют весьма развитый нормативный массив, регулирующий правовой институт коммерческой тайны, в основе которого лежат как национальные правовые традиции, так и современные стандарты международной предпринимательской деятельности. Мы рассмотрим зарубежную практику защиты коммерческой тайны на основе законодательства США, Украины и Китая.

Соединенные Штаты Америки. В США, где существует двухуровневая система законодательства, защита коммерческой тайны регулируется, в основном, законодательствами штатов (в отличие от таких правовых институтов, как промышленная собственность и авторское право, которые устанавливаются на федеральном уровне). Однако большинство штатов в этом вопросе опираются на единый рамочный законодательный акт (Uniform Trade Secret Act), согласно которому коммерческая тайна определяется как информация (включая формулы, модели, программы, механизмы, способы, технологии), которая обладает самостоятельной экономической ценностью (действительной или потенциальной) и недоступна для других лиц, которые могли бы извлечь экономическую выгоду из ее использования или разглашения, и в отношении которой приняты меры по защите ее секретности. В отличие от объектов патентного права, к коммерческой тайне предъявляются лишь минимальные требования новизны ее содержания. Кроме того, коммерческую тайну может составлять информация, отдельные элементы которой являются общеизвестными, но в совокупности они представляют собой определенную коммерческую ценность.

Отличительной чертой американского законодательства о защите коммерческой тайны является акцент на мерах уголовной ответственности, как наиболее эффективного средства обеспечения прав и интересов обладателя коммерческой тайны. Это объясняется тем, что предусмотренная законом гражданская ответственность (возмещение убытков) не носит достаточного превентивного характера для предотвращения преступлений в этой области. В 1996 году был принят федеральный Закон об экономическом шпионаже (The Economic Espionage Act), согласно которому предусматривается уголовная ответственность за присвоение лицом коммерческой тайны в своих интересах или в интересах третьих лиц, если данное лицо было осведомлено о том, что его действия наносят ущерб обладателю коммерческой тайны, и за приобретение, покупку или владение коммерческой тайной другого лица, переданной или присвоенной без ведома ее обладателя. Под "присвоением" понимается любое незаконное действие (кража, мошенничество, несанкционированное копирование, изготовление чертежей, схем, фотографий, передача файлов и иные виды несанкционированной передачи коммерческой тайны). За посягательства на законные права обладателя коммерческой тайны закон устанавливает наказание в виде лишения свободы сроком до десяти лет и штрафа в размере до полумиллиона долларов США. Если субъектом преступления является юридическое лицо, штраф может достигать до пяти миллионов долларов (в США к уголовной ответственности могут привлекаться юридические лица).

Повышенные наказания предусмотрены также, если кража коммерческих секретов осуществляется в интересах иностранных граждан и организаций. Это объясняется тем, что обеспечение конкурентоспособности национальной экономики является одной из целей защиты коммерческой тайны. Законом также предусматривается конфискация собственности, приобретенной с нарушением прав обладателя коммерческой тайны и, кроме того, использованной для совершения

соответствующих правонарушений. Предоставленные федеральным органам власти полномочия по конфискации собственности позволяют им в необходимых случаях производить демонтаж компьютерных сетей, принтеров и другой техники, использованных для совершения преступлений. По закону министр юстиции наделен правом обращаться в суд с гражданским иском о получении судебного запрета в целях защиты законных интересов обладателя коммерческой тайны. Подача таких исков может осуществляться как в рамках уголовного преследования, так и отдельно.

Важным признаком коммерческой тайны в соответствии с Uniform Trade Secret Act является условие о необходимости принятия разумных усилий в целях обеспечения конфиденциальности информации ее обладателем. На практике под "разумными усилиями" понимаются, например: сообщение работникам о необходимости соблюдения режима конфиденциальности определенных сведений, заключение с ними соглашений о неразглашении коммерческой тайны, оборудование помещений для хранения конфиденциальных документов охранной сигнализацией и т.д. При увольнении работника руководитель компании обычно ставит в известность нового работодателя об осведомленности работника в области коммерческих секретов. Это делается для того, чтобы в дальнейшем иметь возможность требовать возмещения ущерба от компании-нанимателя в случае использования чужих секретов - ведь теперь правонарушителю нельзя сослаться на незнание и неосторожность.

Согласно сложившейся судебной практике, суды не всегда относят к коммерческой тайне информацию, которая, по мнению компании, является коммерчески ценной для осуществления предпринимательской деятельности (даже если это действительно так). Например, клиентская база компании может быть признана коммерческой тайной только тогда, когда внесенные в нее клиенты не известны в соответствующей отрасли предпринимательства и могут быть установлены только с применением значительных организационных и финансовых ресурсов, кроме того, необходимым для признания условием являются большие затраты времени на создание базы. В этом случае возможно доказать коммерческую ценность клиентской базы на основании отсутствия аналогичной информации у конкурентов.

Специфической чертой является широкое применение в частном секторе и в ходе судебных разбирательств полиграфных проверок (с использованием "детектора лжи"). Это позволяет службам безопасности коммерческих компаний эффективно бороться с экономическим шпионажем и предотвращать значительное количество утечек конфиденциальной информации. После принятия в 1985 году закона, сильно ограничившего применение полиграфов, как в частном, так и государственном секторе, потери коммерческих компаний от экономического шпионажа выросли практически в два раза. Это вынудило правительство в 1988 году отменить свой запрет и в настоящее время количество полиграфных проверок превышает 4 миллиона в год.

Украина. В соответствии со статьей 505 Гражданского кодекса Украины, коммерческой тайной является информация, являющаяся секретной в том понимании, что она в целом или в определенной форме и совокупности ее составляющих является неизвестной и не является легкодоступной для лиц, обычно имеющих дело с видом информации, к которому она принадлежит, в связи с этим имеет коммерческую ценность и была предметом адекватных существующим обстоятельствам мер по сохранению ее секретности, примененных лицом, законно контролирующим эту информацию. Следует особо подчеркнуть, что в то же время Гражданский кодекс Украины относит коммерческую тайну к объектам интеллектуальной собственности. Эта же позиция закреплена в статье 155 Хозяйственного кодекса (ХК) Украины и определяет одним из прав интеллектуальной собственности в сфере хозяйствования коммерческую тайну. В части 1 статьи 162 ХК Украины определены полномочия субъектов хозяйствования по отношению к коммерческой тайне. Согласно указанной статье, владелец технической, организационной или другой коммерческой информации имеет право на защиту от незаконного использования такой информации третьими лицами при условии, что эта информация имеет коммерческую ценность, в связи с тем, что она неизвестна третьим лицам, и к ней нет свободного доступа других лиц на законных основаниях, а владелец информации применяет меры по охране ее конфиденциальности. Упомянутые выше акты регламентируют коммерческую тайну, в той или иной степени определяют ее понятие и устанавливают ее защиту. Но многие нормы этих актов имеют отсылочный характер - и отсылают они к специальному закону, которого на Украине пока не существует.

Китай. В соответствии с законодательством Китая понятие коммерческой тайны определяется как техническая и управленческая информация закрытого характера, обладающая признаком экономической или практической ценности, и в отношении которой приняты разумные меры по защите секретности. Юридическая защита устанавливается в отношении промышленных "ноу-хау", содержащихся в любых документах, дизайнерских проектах, схемах и чертежах. Закон запрещает совершение действий, связанных с получением коммерческой тайны путем хищения, незаконного принуждения или другими неправомерными способами. Также закон устанавливает запрет на разглашение и использование информации, составляющей коммерческую тайну, полученную

незаконными способами и с нарушением условий использования сведений, предусмотренных соглашением между сторонами. Владелец коммерческой тайны, законные интересы которого были нарушены, имеет право обратиться в суд с иском о возмещении причиненных убытков. В случае если точно определить размер убытков представляется весьма затруднительным, компенсация рассчитывается исходя из размеров полученной правонарушителем прибыли.

Глава 2. Коммерческая тайна и другие виды конфиденциальной информации

Как уже было сказано в [главе 1](#), к конфиденциальной информации относятся сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные); сведения, составляющие тайну следствия и судопроизводства; служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с требованиями законодательства (служебная тайна); сведения с ограниченным доступом, связанные с профессиональной деятельностью (врачебная, нотариальная, адвокатская тайна и так далее); коммерческая тайна. Особняком стоит государственная тайна - ее статус существенно отличается от всех вышеперечисленных. Правоотношения, связанные с каждым из названных видов тайн, регламентируются соответствующим законодательством, которое определяет права и обязанности субъектов таких правоотношений, а также устанавливает ответственность за нарушение режима конфиденциальности или секретности (в случае государственной тайны). Нередко перечисленные категории конфиденциальных сведений смешиваются. Для их отграничения необходимо выделить ряд критериев. Для разных видов тайн отдельные критерии могут совпадать, однако их совокупность должна быть индивидуальной. Такими критериями выступают: кто является обладателем информации, к какой сфере общественной жизни относится информация, составляющая тайну, на кого возложена ее защита, чем определяется состав информации того или иного вида тайны.

На основании указанных критериев выделяют следующие виды тайн.

Государственная тайна - защищаемые государством сведения в области его внешнеполитической, военной, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. Перечень сведений, составляющих государственную тайну, устанавливается федеральным законодательством. Защита государственной тайны возлагается на уполномоченные государственные органы. Особо следует отметить, что в ряде случаев возможен определенный "дуализм" - одни и те же сведения (в основном, экономического характера), отнесенные к государственной тайне, могут одновременно выступать, как коммерческая тайна для хозяйствующих субъектов (различного рода технологии и производственные секреты).

Личная (семейная) тайна - вид тайны, включающий сведения о фактах, событиях и обстоятельствах частной жизни гражданина. Согласно части 2 статьи 23 Конституции РФ, 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.

Для целей Трудового кодекса РФ персональные данные работника определены как информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника. Порядок получения и использования персональных данных в процессе трудовых отношений регламентируется главой 14 "Защита персональных данных работника".

В некоторых случаях незаконное использование персональных данных руководителей, сотрудников и деловых партнеров может причинить значительный ущерб коммерческой компании. Разглашение информации личного характера о неблагоприятных поступках частного предпринимателя или руководителя фирмы негативно сказывается на их деловой репутации и в целом на имидже фирмы. Пожалуй, еще большую опасность представляют личные секреты даже рядовых сотрудников в руках шантажистов. Однако коммерческая тайна и персональные данные (личная тайна) имеют различную правовую природу. Обеспечение охраны от разглашения, получения и незаконного использования осуществляется за счет норм о неприкосновенности частной жизни.

2.1. Коммерческая и служебная тайны

Вопрос о соотношении служебной и коммерческой тайны представляет определенную сложность, поскольку Гражданский кодекс РФ в статье 139 оперирует этими двумя понятиями, не раскрывая, в чем их отличие. Несмотря на то, что служебная и коммерческая тайны обладают, согласно

указанной статье, тремя аналогичными признаками, синонимами они не являются. Это разноплановые понятия. Во-первых, основания, по которым сведения, относящиеся к служебной тайне, и сведения, составляющие коммерческую тайну, признаются конфиденциальными, существенно различаются между собой. Сохранение в тайне служебной информации, в отличие от коммерческой тайны, не обусловлено ее коммерческой ценностью. Служебная тайна не может быть объектом гражданского оборота. Запрещение ее разглашать устанавливается императивно законодательством, регламентирующим отдельные виды деятельности государственных органов.

Итак, служебную тайну можно определить как вид тайны, включающий устанавливаемую и защищаемую федеральными и муниципальными органами власти и их предприятиями информацию любой области деятельности, доступ к которой ограничивается служебной необходимостью. В целях осуществления своих функций и в рамках установленных полномочий все государственные органы в той или иной степени аккумулируют у себя массивы самой разнообразной информации, в том числе составляющей личную (семейную), коммерческую и другие виды тайн. Мы будем рассматривать случаи, когда информация, составляющая коммерческую тайну, приобретает статус служебной. В основном, это касается государственных органов, для осуществления деятельности которых необходима информация экономической направленности. В качестве характерных примеров могут выступать таможенные и налоговые органы (соотношение коммерческой и налоговой тайны будет более подробно рассмотрено в [параграфе 3](#) настоящей главы).

Так, согласно пункту 1 статьи 10 Таможенного кодекса РФ, таможенные органы по своему статусу наделены полномочиями на получение любой информации (включая коммерческую), необходимой для обеспечения соблюдения таможенного законодательства. Например, для целей таможенной статистики используются документы и сведения, представляемые лицами в соответствии с Таможенным кодексом РФ, такие как грузовая таможенная декларация. Сведения, содержащиеся в ней, в ряде случаев могут составлять коммерческую тайну, поскольку дают представление о товарообороте коммерческой компании, объеме поставок и так далее. Такая информация, в соответствии с пунктом 3 статьи 10 Таможенного кодекса РФ, имеет специальный режим хранения и доступа.

Статья 33 Закона РФ от 27 ноября 1992 г. N4015-1 "Об организации страхового дела в Российской Федерации" устанавливает обязанность должностных лиц федерального органа исполнительной власти по надзору за страховой деятельностью не разглашать служебную информацию, составляющую коммерческую тайну страховщика.

Как видно из приведенных примеров, законодатель обязал лиц, имеющих доступ к служебной тайне, соблюдать ее конфиденциальность под угрозой применения наказания, в том числе и уголовного. Однако следует отметить, что судебная практика по делам о разглашении и незаконном использовании коммерческой информации, находящейся в режиме служебной тайны, государственными служащими, мягко говоря, не велика. Это объясняется не высокими моральными качествами чиновников, а сложностью доказывания наличия состава преступления за указанные деяния. Какую информацию и в каком объеме предприниматели обязаны предоставлять в различные государственные органы, мы рассмотрим в [главе 4](#).

2.2. Коммерческая и банковская тайны

Основные принципиальные положения о составе сведений, составляющих банковскую тайну, и о режиме этой тайны изложены в статье 857 Гражданского кодекса РФ и в статье 26 ФЗ "О банках и банковской деятельности" от 2 декабря 1990 г. N395-1. Статья 857 Гражданского кодекса РФ устанавливает, что банк гарантирует тайну банковского счета и банковского вклада, операций по счету и сведений о клиенте. 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 в порядке, предусмотренном законом. Несколько иначе это положение сформулировано в статье 26 Закона РФ N395-1, согласно которой кредитные организации, Банк России гарантируют тайну об операциях, о счетах и вкладах своих клиентов и корреспондентов. Все служащие кредитной организации обязаны хранить тайну об операциях, счетах и вкладах ее клиентов и корреспондентов, а также об иных сведениях, устанавливаемых кредитной организацией, если это не противоречит указанному Федеральному закону.

Как видим, между Гражданским кодексом и Законом "О банках и банковской деятельности" имеются определенные противоречия. Гражданский кодекс в качестве субъекта, в обязанности которого вменяется хранить тайну, определяет банк, а Закон - кредитную организацию (таким образом, из сферы регулирования Гражданского кодекса выпадают небанковские кредитные организации У(б), в Гражданском кодексе объектом защиты названы сведения об операциях по вкладу, а в Законе - вообще об операциях. В Законе, в отличие от Гражданского кодекса, перечень сведений, подпадающих под

правовой институт банковской тайны, является открытым (в перечень входят "иные сведения").

С принятием Федерального закона от 30 декабря 2004 г. №218-ФЗ "О кредитных историях" прибавился еще один вид обладателей банковской тайны. Согласно указанному закону предусмотрено создание бюро кредитных историй, основная цель которых состоит в накоплении определенного перечня информации, характеризующей платежную дисциплину заемщика по исполнению договора займа (кредита) и в совокупности составляющей кредитные истории физических и юридических лиц. В частности, в кредитные истории вносятся следующие сведения:

- 1) указание суммы обязательства заемщика на дату заключения договора займа (кредита);
- 2) указание срока исполнения обязательства заемщика в полном размере в соответствии с договором займа (кредита);
- 3) указание срока уплаты процентов;
- 4) о внесении изменений или дополнений к договору займа (кредита), в том числе, касающихся сроков исполнения обязательств;
- 5) о дате и сумме фактического исполнения обязательств заемщика в полном или неполном размерах;
- 6) о погашении займа (кредита) за счет обеспечения в случае неисполнения заемщиком своих обязательств по договору;
- 7) о фактах рассмотрения арбитражным или третейским судом споров по договору займа (кредита) и содержании резолютивных частей судебных актов, вступивших в законную силу;
- 8) иная информация, официально полученная из государственных органов.

Поскольку аккумулируемая в бюро кредитных историй информация может иметь значительную ценность при конкурентной борьбе, возникает необходимость в обеспечении защиты коммерческой тайны юридических лиц и частных предпринимателей. Закон "О кредитных историях" уделяет большое внимание порядку хранения и передачи кредитных историй, а также надзору за деятельностью бюро. Информация может поступить в бюро только при наличии согласия заемщика. Предусмотрен особый механизм передачи на основании договора оказания информационных услуг, исключающий возможность утечки сведений. Бюро кредитных историй обязаны иметь лицензию на осуществление деятельности по технической защите конфиденциальной информации и обеспечивать защиту информации сертифицированными средствами¹⁴. Пункт 14 статьи 6 рассматриваемого закона устанавливает для пользователей кредитных историй и иных лиц, имеющих доступ на законных основаниях к такой информации, обязанность не разглашать ее третьим лицам под угрозой привлечения к ответственности в соответствии с действующим законодательством.

Для нормального функционирования экономики институт банковской тайны не менее важен, чем институт коммерческой тайны. Не следует путать коммерческую тайну самих банков, как коммерческих организаций, и банковскую тайну. Принципиальное отличие между ними заключается в способе отнесения тех или иных сведений к категории конфиденциальной информации. Владелец коммерческой тайны сам определяет, какая информация подпадает под эту категорию (за исключением случаев, установленных законом). Перечень сведений, являющихся банковской тайной, определен законом и одинаков для всех банков и других кредитных организаций. Сами кредитные организации не имеют права по собственному желанию его ни расширить, ни сузить. Подводя итог, можно сказать, что банковская тайна представляет собой компромисс между частными интересами кредитных организаций и их клиентов - с одной стороны, и публичной необходимостью обеспечения прозрачности банковской деятельности - с другой.

В мировой практике существуют два принципиально отличных подхода в решении этого вопроса. Законодательство целого ряда стран (Германия, Люксембург) исходит из принципа так называемой абсолютной банковской тайны, согласно которому предоставление банком государственным (в том числе правоохранительным) органам сведений о банковских операциях своих клиентов недопустимо. В большинстве государств (США, Норвегия, Великобритания) специализированные органы (в основном, налоговые) имеют доступ к банковской информации, в том числе (при выполнении ряда условий), к информации, составляющей банковскую тайну. Такой подход имеет гораздо больше сторонников, особенно в последнее время. Это связано, в первую очередь, с необходимостью борьбы с финансированием международного терроризма и транснациональных преступных организаций, а также контролем за своевременностью и полнотой налоговых выплат.

2.3. Коммерческая и налоговая тайны

Примером служебной тайны можно считать налоговую тайну, предусмотренную статьей 102 Налогового кодекса Российской Федерации (далее - НК РФ). Согласно указанной статье, любые сведения, кроме случаев, установленных НК РФ, полученные налоговыми органами о

налогоплательщике в процессе реализации своих полномочий, признаны конфиденциальной информацией и составляют налоговую тайну. Налоговая тайна не подлежит разглашению налоговыми органами (их должностными лицами), за исключением сведений, предусмотренных федеральным законом. К таким сведениям относятся: разглашенные налогоплательщиком самостоятельно или с его согласия об идентификационном номере налогоплательщика, об уставном фонде (уставном капитале) налогоплательщика, о нарушениях законодательства о налогах и сборах и мерах ответственности за эти нарушения, предоставляемых налоговым или правоохранительным органам других государств.

Для сведений, составляющих налоговую тайну, установлен специальный режим хранения и доступа. За неправомерное разглашение, использование и утрату налоговой тайны налоговые органы несут гражданско-правовую имущественную ответственность за причинение вреда налогоплательщику или его имуществу с возмещением в полном объеме убытков, включая упущенную выгоду, за счет средств федерального бюджета на основании статьи 35 и 103 НК РФ. В соответствии со статьей 12 Закона РФ от 21 марта 1991 г. №943-1 "О налоговых органах Российской Федерации", за нарушение обязанности по соблюдению налоговой тайны на должностных лиц налоговых органов может быть возложена дисциплинарная и уголовная ответственность. Уголовная ответственность должностных лиц наступает в зависимости от вида разглашенных сведений, составляющих налоговую тайну. В случае разглашения сведений о частной жизни лица, составляющих его личную или семейную тайну, применяется статья 137 Уголовного кодекса РФ. Если коммерческая компания представляет в налоговый орган сведения, составляющие ее коммерческую тайну, то после передачи такая информация приобретает статус налоговой тайны (ст. 102 НК РФ). В этом случае ее правовой режим будет регулироваться совместно нормами налогового законодательства и нормами законодательства о коммерческой тайне.

Таким образом, если в результате незаконного разглашения, использования или утраты сведений, составляющих налоговую тайну, нарушена коммерческая тайна, то компания вправе использовать способы защиты своего субъективного права, предусмотренные как НК РФ (для налоговой тайны), так и законодательством о коммерческой тайне. В том числе, привлечение виновных к уголовной ответственности по части 2 статьи 183 Уголовного кодекса РФ. Так, бывший руководитель УМНС по Тульской области, разгласивший сведения, составляющие коммерческую тайну, предоставленные организацией в налоговую инспекцию (получившую, таким образом, статус налоговой тайны), признан виновным в совершении преступлений, предусмотренных частью 4 статьи 290 Уголовного кодекса РФ (получении взятки в крупном размере - 40 тысяч долларов) и частью 3 статьи 183 Уголовного кодекса РФ.

В соответствии со статьями 21, 24 и 102 НК РФ, правом требовать соблюдения налоговой тайны обладают организации и физические лица, признаваемые налогоплательщиками, плательщиками сборов и налоговыми агентами. Выступая в качестве обладателей информации, предоставляемой в соответствии с НК РФ в налоговые органы, они вправе по своему усмотрению реализовывать правомочия владения, пользования и распоряжения этой информацией, в том числе, придавать ее огласке и давать согласие налоговым органам на ее разглашение. Налоговый орган выступает лишь "пользователем" информации, составляющей налоговую тайну, и обязан принимать необходимые меры для соблюдения режима конфиденциальности. Поэтому он не вправе распоряжаться ею по своему усмотрению, в частности, устанавливать срок, в течение которого такая информация является налоговой тайной. К сожалению, в НК РФ не урегулирован вопрос о времени и обстоятельствах прекращения обязанности налоговых органов (должностных лиц) по соблюдению налоговой тайны. Исходя из ее двойственной природы и руководствуясь нормами законодательства о коммерческой тайне, можно сделать вывод - пока информация обладает свойствами коммерческой ценности, неизвестности третьим лицам, и ее обладатель принимает меры к охране конфиденциальности, налоговые органы обязаны соблюдать в отношении такой информации режим налоговой тайны.

Институт налоговой тайны направлен, прежде всего, на защиту законных интересов коммерческих компаний, предоставляющих в соответствии с требованиями законодательства коммерчески значимую информацию государству, которое, в свою очередь, обязуется хранить ее в тайне. Приводимый ниже судебный прецедент*(8) интересен тем, что, помимо чисто практического значения, показывает - бывают ситуации, когда правовой институт, признанный охранять законные интересы хозяйствующих субъектов, может обернуться препятствием для добросовестных предпринимателей.

Высший Арбитражный Суд Российской Федерации, рассмотрев в судебном заседании дело по заявлению ЗАО "Управление и финансы" о признании недействующим пункта 3 Порядка предоставления налоговыми органами информации взыскателю, утвержденного приказом Министерства Российской Федерации по налогам и сборам от 23 января 2003 г. № БГ-3-28/23, в части предоставления взыскателю информации о факте наличия у должника-организации открытых счетов и вкладов в банках и иных кредитных организациях, как не соответствующего пункту 1 статьи 6, пункту 1 статьи 31, пункту 3

статьи 46 Федерального закона от 21 июля 1997 г. Ы119-ФЗ "Об исполнительном производстве", пункту 1 статьи 12 Федерального закона от 21 июля 1997 г. N 118-ФЗ "О судебных приставах", пункту 1 статьи 139, пунктам 1, 2 статьи 874, пункту 1 статьи 875 Гражданского кодекса Российской Федерации, пунктам 1, 2 статьи 102 Налогового кодекса Российской Федерации, пункту 3 статьи 10 Федерального закона от 20 февраля 1995 г. N 24-ФЗ "Об информации, информатизации и защите информации" в их взаимосвязи, установил следующее.

Приказом МНС РФ N БГ-3-28/23 утвержден Порядок предоставления налоговыми органами информации взыскателю (далее - Порядок), пункт 3 которого определяет, что при наличии счетов и вкладов у должника-организации в банках и иных кредитных учреждениях взыскателю предоставляется "информация о факте наличия у должника-организации открытых счетов".

Заявитель полагает, что предоставление сведений только о наличии расчетных счетов должника ограничивает право взыскателя по исполнительному листу на списание со счета должника денежных средств по решению арбитражного суда, предоставленное ему Федеральным законом "Об исполнительном производстве". Такое право взыскатель может реализовать при условии оформления инкассового поручения, в котором, в соответствии с требованиями Положения "О безналичных расчетах Российской Федерации", утвержденного Центральным банком РФ 3 октября 2002 г. N 2-П, должен быть указан номер счета.

МНС России считает, что содержащееся во втором предложении пункта 3 Порядка ограничение направляемой взыскателю информации сведениями лишь о наличии или отсутствии счета должника в кредитном учреждении вызвано невозможностью предоставить взыскателю данные о номере счета должника, поскольку такие сведения относятся к налоговой тайне, которая в силу статьи 102 Налогового кодекса РФ не подлежит разглашению. Объем информации, подлежащей предоставлению взыскателю, статьей 46 Федерального закона "Об исполнительном производстве" не конкретизирован. По мнению министерства, оспариваемое положение Порядка не нарушает законных прав заявителя. При отсутствии сведений об имеющихся у должника счетах в кредитных учреждениях взыскатель, в соответствии со статьей 6 этого Федерального закона, вправе направить исполнительный лист судебному приставу-исполнителю.

Изучив материалы дела, заслушав объяснения лиц, участвующих в споре, исследовав представленные по делу доказательства, суд посчитал заявление ЗАО "Управление и финансы" подлежащим удовлетворению по следующим основаниям.

В пункте 1 Порядка указано, что настоящий нормативный акт разработан на основании п. 3 ст. 46 Федерального закона "Об исполнительном производстве". При этом, как заявляет министерство, из положений, содержащихся в данной статье Закона, следует обязанность налогового органа предоставить взыскателю сведения лишь о наличии или отсутствии у должника счетов в банках и иных кредитных организациях, обязанность налогового органа сообщить взыскателю номер счета названной выше нормой не предусмотрена.

Между тем, как следует из абзацев третьего и четвертого пункта 3 статьи 46 Закона, информация, предоставляемая взыскателю, должна быть такой же, как предоставляемая судебному приставу-исполнителю информация, необходимая для обращения взыскания по исполнительным листам на денежные средства, находящиеся на счетах в банках и иных кредитных организациях.

Списание денежных средств, находящихся на счете, без распоряжения клиента, согласно статье 854 Гражданского кодекса РФ, допускается по решению суда, а также в случаях, предусмотренных законом.

Статьей 874 Кодекса предусмотрено, что порядок осуществления расчетов по инкассо регулируется законом, установленными в соответствии с ним банковскими правилами и применяемыми в банковской практике обычаями делового оборота.

Органом, регулирующим организацию расчетных систем в Российской Федерации, является согласно статье 80 Федерального закона от 10 июля 2002 г. N 86-ФЗ "О Центральном банке Российской Федерации" Центральный банк РФ.

В соответствии с Положением "О безналичных расчетах в Российской Федерации" Центрального банка, списание денежных средств по исполнительным листам осуществляется по инкассовым поручениям, которые, являясь расчетными документами, должны содержать в числе необходимых реквизитов номер счета плательщика. Расчетные документы, оформленные с нарушением установленных требований, приему не подлежат (п. 2.10, 2.16, 12.1, 12.2 Положения).

Следовательно, не имея данных о номере счета должника, взыскатель, так же как и судебный пристав-исполнитель, не сможет реализовать предусмотренное статьей 6 Федерального закона "Об исполнительном производстве" право на взыскание присужденных судом денежных средств непосредственно через кредитное учреждение.

Согласно Порядку взаимодействия налоговых органов Российской Федерации и служб судебных приставов органов юстиции субъектов Российской Федерации по принудительному исполнению

постановлений налоговых органов и иных исполнительных документов, утвержденному приказом МНС России от 25 июля 2000 г. N ВГ-3-10/265/215, налоговый орган направляет судебному приставу-исполнителю по его запросу информацию, необходимую для принудительного взыскания по исполнительным документам, в числе которой названы сведения о номерах расчетных счетов, наименовании и месте нахождения банков и иных кредитных учреждений, в которых открыты счета должников.

Следовательно, если под необходимой информацией для судебного пристава-исполнителя, указанной в пункте 3 статьи 46 Федерального закона "Об исполнительном производстве", МНС России понимает, в том числе, и сведения о номерах счетов в кредитных учреждениях должника, то, как следует из абзаца четвертого пункта 3 статьи 46 этого Закона, такие же сведения могут быть предоставлены взыскателю по его заявлению при наличии у него исполнительного листа с неистекшим сроком давности. При этом нельзя согласиться с позицией МНС России, что из содержания пункта 3 статьи 46 данного Закона вытекает лишь право налогового органа предоставить взыскателю необходимую информацию, а не его обязанность. Формулировка "может быть предоставлена" неразрывна с содержащимся далее текстом: "при наличии у него исполнительного листа с неистекшим сроком давности".

Иными словами, законодатель указал на возможность предоставления взыскателю необходимой информации при условии, что он располагает исполнительным листом, давность взыскания по которому не истекла, а не на возможность налогового органа по своему усмотрению решать вопрос о предоставлении необходимых сведений. МНС России, определяя порядок предоставления информации, не вправе устанавливать иные, кроме установленных законом, ограничения к получению информации, необходимой для взыскания задолженности через банк.

По смыслу, содержащемуся в пункте 1 статьи 102 Налогового кодекса РФ, сведения о счетах организаций, находящихся в кредитных учреждениях, действительно относятся к налоговой тайне.

По своей природе и назначению институт налоговой тайны имеет публично-правовой характер и означает защиту налоговым органом сведений, разглашение которых может нарушить права граждан и организаций.

Вместе с тем, как следует из пункта 2 статьи 102 Кодекса, налоговая тайна не подлежит разглашению, за исключением случаев, предусмотренных федеральным законом. Закрепление в законе отступлений необходимо для защиты прав и законных интересов других лиц.

Специального закона, посвященного налоговой тайне и, следовательно, вопросам ее разглашения, не имеется. Однако Федеральный закон "Об исполнительном производстве" предусматривает возможность передачи налоговым органом взыскателю в случае, оговоренном в пункте 3 статьи 46 этого Закона, необходимой информации о банковском счете должника, к которой, как указано выше судом, относится и информация о номере такого счета.

Кроме того, по смыслу, содержащемуся в статье 10 Федерального закона "Об информации, информатизации и защите информации", не подлежит ограничению доступ к информации, необходимой для реализации законных прав и обязанностей граждан, а равно и организаций.

Федеральный конституционный закон от 31 декабря 1996 г. "О судебной системе Российской Федерации" определяет, что вступившие в законную силу постановления федеральных судов, мировых судей и судов Российской Федерации обязательны для всех без исключения органов государственной власти, органов местного самоуправления, должностных лиц, других физических и юридических лиц и подлежат неукоснительному исполнению.

Защита нарушенных прав должна обеспечиваться эффективным механизмом реализации судебных решений.

Названные выше принципы не могут не учитываться при применении положений, содержащихся в статье 46 Закона "Об исполнительном производстве", в их взаимосвязи с положениями других статей этого же Закона, в частности, статьей 6, предусматривающей право взыскателя направить исполнительный лист непосредственно в кредитное учреждение, и статьей 31, указывающей на право доступа взыскателя ко всем материалам исполнительного производства, а также с другими правовыми актами, приведенными выше.

С учетом изложенного, суд пришел к выводу о наличии оснований к признанию положения, содержащегося во втором предложении пункта 3 оспариваемого нормативного акта, недействующим.

2.4. Коммерческая и профессиональная тайны

Профессиональная тайна - обобщенное понятие, включающее различные виды тайн других юридических или физических лиц, которые получены лицом в результате осуществления им своей профессиональной деятельности (тайна связи, банковская, врачебная, кредитная, журналистская, адвокатская, тайна усыновления, исповеди, голосования). Таким образом, профессиональная тайна, как

и служебная, является производной от первичных видов. Защита профессиональной тайны и ответственность за ее неправомерное использование осуществляется посредством правовых норм, охраняющих соответствующие виды конфиденциальных сведений. Так, ранее статьей 128.1 Уголовного кодекса РСФСР 1960 года была предусмотрена уголовная ответственность за разглашение сведений, составляющих врачебную тайну. В настоящее время такое деяние квалифицируется по части 2 статьи 137 Уголовного кодекса РФ как нарушение неприкосновенности частной жизни. Использование лицом своего служебного положения выступает в качестве квалифицирующего признака. Существует множество видов профессиональной тайны, в частности: адвокатская, врачебная, аудиторская, журналистская тайны, тайна связи, записей актов гражданского состояния и так далее. Здесь мы рассмотрим только некоторые из них.

Согласно статье 8 Федерального закона от 7 августа 2001г. Ы119-ФЗ "Об аудиторской деятельности", аудиторы обязаны хранить тайну об операциях аудируемых и лиц, которым оказывались сопутствующие аудиту услуги. Аудиторская тайна не может быть сведена исключительно к сведениям по операциям. Согласно пункту 2 статьи 8 вышеуказанного закона, на аудиторов возложена обязанность обеспечивать сохранность сведений и документов, полученных или составляемых ими при осуществлении аудиторской деятельности - они не могут передавать указанные сведения и документы третьим лицам, либо разглашать их без письменного согласия аудируемых организаций или индивидуальных предпринимателей, кроме установленных законодательством случаев. К таким случаям относятся: прямое указание законодательных актов или на основании судебного решения; получение разрешения проверяемого лица, при условии соблюдения интересов всех заинтересованных лиц; при защите профессиональных интересов аудитора в ходе официального расследования или частного разбирательства, проводимого руководителями или уполномоченными представителями проверяемых лиц; при намеренном и незаконном вовлечении аудитора проверяемым лицом в действия, противоречащие законодательным и профессиональным нормам. Аудиторская тайна, согласно статье 8 Федерального закона "Об аудиторской деятельности", должна соблюдаться в отношении всех сведений и документов, полученных от клиентов аудиторской фирмы.

В соответствии со статьей 8 Федерального закона от 31 мая 2002 г. N 63-ФЗ "Об адвокатской деятельности и адвокатуре в Российской Федерации", 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.

Статья 5 Основ законодательства Российской Федерации о нотариате от 11 февраля 1993 г. N 4462-1 регламентирует тайну нотариальных действий: "Нотариусу при исполнении служебных обязанностей, а также лицам, работающим в нотариальной конторе, запрещается разглашать сведения, оглашать документы, которые стали им известны в связи с совершением нотариальных действий, в том числе и после сложения полномочий или увольнения, за исключением случаев, предусмотренных настоящими Основами".

Статья 41 Закона РФ "О средствах массовой информации" вводит понятие журналистской тайны. Так, согласно требованиям указанной статьи, 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.

Глава 3. Сведения, не являющиеся коммерческой тайной

В соответствии с частью 1 статьи 4 Федерального закона "О коммерческой тайне", право на отнесение информации к информации, составляющей коммерческую тайну, и на определение перечня и состава такой информации принадлежит обладателю такой информации за исключением случаев, установленных законом. Каким критериям должна отвечать информация для распространения на нее правового режима коммерческой тайны, мы определили в [главе 1](#). Теперь рассмотрим, какие сведения не могут составлять коммерческую тайну. Прежде всего, это, конечно, та информация, которая не обладает хотя бы одним из трех критериев (коммерческая ценность в силу неизвестности третьим лицам, отсутствие свободного доступа на законных основаниях, обладателем приняты меры к охране ее конфиденциальности).

Следующее ограничение вытекает из формы выражения информации вовне. Особенностью российского законодательства является требование о материальном носителе сведений, претендующих на высокое звание коммерческой тайны. То есть, информация должна быть зафиксирована на любом материальном носителе - документах, изделиях или даже физических полях. На идеи, замыслы,

сведения и иные данные, независимо от их коммерческой ценности для их обладателя, если они не облачены в какой-либо материальной форме, правовой режим охраны коммерческой тайны не распространяется. Такой подход на первый взгляд выглядит нелогичным - ведь для информации главным является не форма, в которой она существует, а то, какова ценность содержащихся в ней сведений. Однако при таком подходе практически невозможно было бы ни доказать, ни опровергнуть факт несанкционированного доступа или хищения информации у ее обладателя.

Еще одно ограничение вытекает из установленного законодательством субъектного состава обладателей коммерческой тайны.

Обладателем может выступать юридическое лицо (в том числе, иностранная коммерческая компания) либо индивидуальный предприниматель. Граждане, выступающие в гражданском обороте в качестве потребителей, а также занимающиеся предпринимательской деятельностью без регистрации в качестве индивидуальных предпринимателей, не могут выступать в качестве обладателей коммерческой тайны. Судебная практика придерживается аналогичного подхода.

В качестве примера можно привести решение Верховного Суда РФ от 19 июня 2003 г. N КАСОЗ-236 по вопросу применения норм о регулировании вопросов, связанных с коммерческой тайной, на физических лиц, не зарегистрированных в качестве частных предпринимателей в установленном порядке.

Рассмотрев гражданское дело по заявлению А. к Правительству Российской Федерации и Министерству Финансов Российской Федерации о взыскании материального ущерба, компенсации морального вреда, а также о признании недействующим Постановления Правительства РСФСР от 5 декабря 1991 г. N35 "О перечне сведений, которые не могут составлять коммерческую тайну", суд установил: согласно пункту 1 части 1 статьи 134 ГПК РФ, судья отказывает в принятии искового заявления, если заявление не подлежит рассмотрению и разрешению в порядке гражданского судопроизводства, поскольку в заявлении оспариваются акты, которые не затрагивают права, свободы или законные интересы заявителя. Как следует из заявления, поданного на первую инстанцию, А. оспаривает Постановление Правительства РСФСР от 5 декабря 1991 г. N35 "О перечне сведений, которые не могут составлять коммерческую тайну". Акт в оспоренной части распространяется на юридических лиц и индивидуальных предпринимателей и непосредственно каких-либо прав, свобод или законных интересов заявителя не затрагивает. При таких обстоятельствах основания для рассмотрения заявления в указанной части по существу в Верховном Суде РФ, как и в любом другом федеральном суде, отсутствуют, и судья Верховного Суда РФ правомерно отказал в принятии заявления на основании пункта 1 части 1 статьи 134 ГПК РФ.

И, наконец, статья 5 Закона "О коммерческой тайне" содержит перечень сведений, которые не могут составлять коммерческую тайну. К ним относятся сведения:

- 1) содержащиеся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;
- 2) содержащиеся в документах, дающих право на осуществление предпринимательской деятельности;
- 3) о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения;
- 4) о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других негативных факторах;
- 5) о численности и составе работников, о системе оплаты труда, об условиях труда, о показателях производственного травматизма и профессиональной заболеваемости, о наличии свободных рабочих мест;
- 6) о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;
- 7) о нарушениях законодательства РФ и фактах привлечения к ответственности за совершение этих нарушений;
- 8) об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;
- 9) 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 своей деятельности;
- 10) о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;
- 11) обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами.

С принятием Закона "О коммерческой тайне" следует считать утратившим силу Постановление

Правительства РСФСР от 5 декабря 1991 г. N35 "О перечне сведений, которые не могут составлять коммерческую тайну" (с изменениями и дополнениями от 3 октября 2002 г.). По сравнению с перечнем образца 1991 г. новый перечень уточнен, по ряду позиций расширен. Однако основное принципиальное отличие заключается в следующем: из нового перечня исключены сведения, относящиеся к отчетности о финансово-хозяйственной деятельности, иные сведения, необходимые для проверки правильности исчисления и уплаты налогов и других обязательных платежей, документы о платежеспособности, документы об уплате налогов и других обязательных платежей. Исключение этой категории из перечня сведений, которые не могут составлять коммерческую тайну, является вполне закономерным.

Как уже ранее отмечалось, возможность получения госорганами и их должностными лицами конфиденциальных сведений не означает утрату этими сведениями статуса коммерческой тайны, поскольку доступ к информации имеют только конкретные лица в конкретных объемах, в обязанность которых входит обеспечение ее нераспространения. Как показывает практика, зачастую происходит смешение двух категорий сведений - тех, которые не могут составлять коммерческую тайну, и тех, которые отнесены к коммерческой тайне на законном основании, однако в силу требований различных нормативных актов обязаны предоставляться определенным лицам.

В качестве примера можно привести постановление Федерального арбитражного суда Уральского округа от 7 сентября 2000 г. по делу N Ф09-1246/2000-ГК. Акционер обратился в суд, обжалуя отказ администрации акционерного общества предоставить ему копии документов бухгалтерского учета. Администрация АО мотивировала свой отказ тем, что истребуемые истцом документы содержали сведения, составляющие коммерческую тайну. Суд, рассмотрев материалы дела, в удовлетворении иска отказал, признал действия администрации АО правомерными и указал, что в предоставлении информации, составляющей коммерческую тайну, есть ограничения. Они установлены статьей 139 Гражданского кодекса РФ и пунктом 4 статьи 10 Федерального закона от 21 ноября 1996 г. N 129-ФЗ "О бухгалтерском учете". И закон ограничивает доступ к сведениям, содержащимся в документах (регистры бухгалтерского учета и внутренней бухгалтерской отчетности), которые истребовал акционер.

Такой подход суда, по всей видимости, нельзя назвать бесспорным. Да, истребуемая информация не подпадает под перечень сведений, которые не могут составлять коммерческую тайну и, следовательно, обладатель имеет право ее "засекретить". Однако, согласно гражданскому законодательству, акционеры являются собственниками АО и имеют право участвовать в распределении прибыли и в решении вопросов управления АО, отнесенных к компетенции общего собрания акционеров. Не имея доступа к бухгалтерским документам, акционеры не имеют возможности оценить экономическое положение компании и, соответственно, принимать адекватные управленческие решения и контролировать деятельность администрации. Не применим к владельцам акций (уточним - акций с правом голоса) термин "третье лицо", для которых и ограничивается доступ к сведениям, составляющим коммерческую тайну. Акционеры являются собственниками акционерной компании, которая, в свою очередь, является обладателем коммерческой тайны. Да, имея доступ к конфиденциальной информации, обладающей значительной коммерческой ценностью, владелец небольшого пакета акций может посчитать, что ему выгоднее продать такую информацию конкурентам. Однако так же может поступить и любой наемный работник в любой организации, по роду служебной деятельности имеющий доступ к секретам работодателя, коммерческая ценность которых может превышать размер его зарплаты в сотни раз. Для таких случаев и предусмотрены различные виды ответственности (гражданско-правовой, уголовной, административной).

Ссылка на иные федеральные законы делает перечень сведений, которые не могут составлять коммерческую тайну, открытым. С практической точки зрения более целесообразным следует признать подход, в соответствии с которым при необходимости установить недопустимость ограничений еще на какую-то группу сведений, эти ограничения вводились не отраслевыми законами, а путем внесения изменений в статью 5 Закона "О коммерческой тайне". В настоящее время целый ряд федеральных законов, регулирующих самые разные сферы деятельности, вводит дополнительные ограничения. Например, согласно статье 9 Федерального закона от 22 апреля 1996 г. N 39-ФЗ "О рынке ценных бумаг", организатор торговли на рынке ценных бумаг (то есть профессиональный участник рынка ценных бумаг, осуществляющий деятельность по организации торговли на рынке ценных бумаг) обязан предоставить любому заинтересованному лицу следующие сведения: 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.

Подход законодателя об отнесении тех или иных категорий сведений к перечню сведений, которые не могут составлять коммерческую тайну, находит отражение и в судебной практике по данному вопросу. В качестве примера можно привести решение Верховного Суда РФ от 13 ноября 2003 г.

№ ГКПИОЗ-1188, вынесенное по заявлению Федерального государственного унитарного предприятия "Кировторф" о признании недействующим и не подлежащим применению пункта 2 Постановления Правительства РСФСР от 5 декабря 1991 г. №35 "О перечне сведений, которые не могут составлять коммерческую тайну" в части слов "до и".

Как было установлено Верховным Судом РФ в ходе рассмотрения данного дела, пункт 2 вышеуказанного Постановления Правительства содержит запрет государственным и муниципальным предприятиям до и в процессе их приватизации относить к сведениям, составляющим коммерческую тайну, следующие данные: о размерах имущества предприятия и его денежных средствах; о вложении средств в доходные активы (ценные бумаги) других предприятий, в процентных облигации и займы, в уставные фонды совместных предприятий; о кредитных, торговых и иных обязательствах предприятия, вытекающих из законодательства РСФСР и заключенных им договоров; о договорах с кооперативами, иными негосударственными предприятиями, творческими и временными трудовыми коллективами, а также отдельными гражданами. ФГУП "Кировторф" обратилось с заявлением, полагая нарушенными свои права оспариваемым нормативным правовым актом, установившим запрет отнесения сведений к коммерческой тайне до приватизации, и просило признать этот правовой акт недействующим из-за его противоречия статье 8 Конституции РФ и пункту 2 статьи 1 Гражданского кодекса РФ.

Как следует из представленных заявителем учредительных документов, ФГУП "Кировторф" является государственным унитарным предприятием. Заявитель полагает, что сообщение сведений о финансовом состоянии предприятия причинило ему существенный ущерб, и в связи с этим неоднократно обращался в различные судебные инстанции и правоохранительные органы. В удовлетворении заявлений было отказано со ссылкой на оспариваемый нормативный правовой акт, поскольку указанные ФГУП "Кировторф" сведения не относятся к коммерческой тайне. Полагая нарушенными свои права принятием оспариваемого нормативного правового акта Правительством РСФСР, ФГУП "Кировторф" просило признать этот акт недействующим.

Правительство осуществляет исполнительную власть в Российской Федерации, возложенную на него Конституцией РФ, федеральными конституционными законами, федеральными законами и указами Президента РФ.

Согласно статье 114 Конституции РФ, а также действующей на момент вынесения рассматриваемого решения Верховным Судом РФ редакции статьи 14 Федерального конституционного закона от 17 декабря 1997 г. № 2-ФКЗ "О Правительстве Российской Федерации" Правительство РФ управляет федеральной собственностью^{^^}.

Как посчитал ВС РФ, из положений статьи 139 Гражданского кодекса РФ следует, что определение сведений, которые не могут составлять коммерческую тайну, в процессе деятельности государственных унитарных предприятий находится в компетенции Правительства РФ, наделенного правом принятия правовых актов.

Кроме того, указанные в оспариваемом Постановлении Правительства РФ сведения не могут составлять коммерческую тайну, так как руководители федеральных государственных унитарных предприятий обязаны в порядке отчетности представлять эти сведения в Минимущество России и федеральные органы исполнительной власти, осуществляющие регулирование деятельности в соответствующей отрасли, а поэтому к ним имеется свободный доступ со стороны третьих лиц на законном основании.

Обязанности по представлению такой отчетности возлагается статьей 13 Федерального закона от 21 ноября 1996 г. № 129-ФЗ "О бухгалтерском учете" и Положением по ведению бухгалтерского учета и бухгалтерской отчетности в РФ, утвержденным Приказом Министерства финансов РФ от 29 июля 1998 г. №34н.

Таким образом, Правительство РФ при определении перечня сведений, которые не могут составлять коммерческую тайну, действовало как собственник имущества федеральных унитарных предприятий в пределах предоставленных ему вышеуказанными нормативными актами полномочий, а поэтому доводы заявителя о нарушении статьи 8 Конституции РФ и статьи 1 Гражданского кодекса РФ о нарушении равенства участников гражданских правоотношений и ущемлении прав государственной собственности, находящейся у государственных унитарных предприятий, являются несостоятельными.

В связи с этим основания к удовлетворению заявления, по мнению ВС РФ, отсутствуют, поскольку оспариваемые положения нормативного правового акта приняты полномочным органом в полном соответствии с действующим законодательством и не противоречат указанным в заявлении нормам действующего законодательства.

На основании изложенного Верховный Суд РФ оставил заявление ФГУП "Кировторф" без удовлетворения.

Несмотря на то, что Постановление Правительства РСФСР от 5 декабря 1991 г. № 35 "О перечне сведений, которые не могут составлять коммерческую тайну" больше не действует в связи с принятием Закона "О коммерческой тайне", данное судебное решение не утратило актуальности. Это связано с тем,

что статья 5 Закона "О коммерческой тайне" содержит положение, согласно которому к коммерческой тайне не могут быть отнесены сведения о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения.

Глава 4. Предоставление информации, составляющей коммерческую тайну, органам государственной власти

4.1. Права органов власти на истребование информации, составляющей коммерческую тайну

Существование цивилизованных рыночных отношений невозможно без института коммерческой тайны, которому должны быть обеспечены надежные правовые гарантии со стороны государства. В то же время, в интересах борьбы с преступностью, осуществления правосудия, соблюдения налогового, антимонопольного и таможенного законодательства государство должно иметь возможность контролировать деятельность частного бизнеса. Поэтому рядом нормативных актов определен круг государственных органов и должностных лиц, которые в строго определенных случаях имеют право на получение финансово-хозяйственной информации, в том числе и составляющей коммерческую тайну. Очень важно найти оптимальный баланс публичных и частных интересов. Перекос, как в одну, так и в другую сторону, крайне негативно отражается на состоянии экономики страны. Наделение государственных органов излишними полномочиями ведет к росту коррупции и злоупотреблений со стороны чиновников и, как следствие, увеличению сектора теневой экономики. С другой стороны, согласно статье 28 действовавшего ранее Закона от 25 декабря 1990 г. N445-1 "О предприятиях и предпринимательской деятельности", предприятие имело право не представлять информацию, составляющую коммерческую тайну, причем, в силу отсутствия в российском праве легального определения коммерческой тайны, на основании указанного закона можно было отказывать в предоставлении государственным органам любых сведений. Такое положение вынуждало госструктуры использовать неправовые методы давления на частный бизнес. В настоящее время эти отношения переведены в цивилизованное русло.

В общем виде обязанность представления зафиксированной на материальном носителе информации с реквизитами, позволяющими ее идентифицировать (документированной информации), для формирования государственных информационных ресурсов предусмотрена Федеральным законом от 20 февраля 1995 г. N 24-ФЗ "Об информации, информатизации и защите информации". Согласно статье 8 указанного Закона, граждане, органы государственной власти, органы местного самоуправления, организации и общественные объединения обязаны представлять документированную информацию органам и организациям, ответственным за формирование и использование государственных информационных ресурсов. Перечни представляемой в обязательном порядке документированной информации и перечни органов и организаций, ответственных за сбор и обработку федеральных информационных ресурсов, утверждает Правительство РФ. При регистрации юридических лиц регистрационные органы обеспечивают их перечнями представляемых в обязательном порядке документов и адресами их представления. Перечень представляемой в обязательном порядке документированной информации прилагается к уставу каждого юридического лица (положению о нем).

Согласно пункту 8 статьи 3 Закона "О коммерческой тайне", предоставление информации, составляющей коммерческую тайну - это передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций. Особо следует обратить внимание, что, помимо государственных органов, информация, составляющая коммерческую тайну, может быть затребована и органами местного самоуправления. Однако далеко не каждый государственный орган или орган местного самоуправления может затребовать сведения конфиденциального характера - такое право должно предоставляться соответствующим органам только федеральными законами, либо нормативно-правовыми актами, определяющими статус таких органов, их компетенцию, основные права и обязанности.

Кроме того, согласно части 3 статьи 6 Закона "О коммерческой тайне", обладатели информации, составляющей коммерческую тайну, а также органы государственной власти, иные государственные органы, органы местного самоуправления, получившие такую информацию, обязаны предоставить эту 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 Российской Федерации.

Так, например, контролируя исполнение обязанности по уплате налогов, в соответствии со статьей 11 Закона РФ от 18 апреля 1991 г. N1026-1 "О милиции", органы внутренних дел вправе

получать от граждан и должностных лиц организаций сведения, документы и копии с них. В соответствии со статьей 31 НК РФ, налоговые органы, в частности, имеют право: требовать от налогоплательщика или налогового агента документы по формам, установленным государственными органами и органами местного самоуправления, служащие основаниями для исчисления и уплаты (удержания и перечисления) налогов, а также пояснения и документы, подтверждающие правильность исчисления и своевременность уплаты (удержания и перечисления) налогов; производить выемку документов при проведении налоговых проверок у налогоплательщика или налогового агента, свидетельствующих о совершении налоговых правонарушений, в случаях, когда есть достаточные основания полагать, что эти документы будут уничтожены, сокрыты, изменены или заменены; осматривать (обследовать) любые используемые налогоплательщиком для извлечения дохода либо связанные с содержанием объектов налогообложения независимо от места их нахождения производственные, складские, торговые и иные помещения и территории, проводить инвентаризацию принадлежащего налогоплательщику имущества. Порядок проведения инвентаризации имущества налогоплательщика при налоговой проверке утверждается Министерством финансов Российской Федерации. В целях исполнения функций, возложенных на органы регулирования естественных монополий, согласно статье 13 Федерального закона от 17 августа 1995 г. N 147-ФЗ "О естественных монополиях", их работники имеют право беспрепятственного доступа к информации о деятельности субъектов естественных монополий, имеющейся у органов исполнительной власти и органов местного самоуправления, а также у субъектов естественных монополий. Сведения, которые составляют коммерческую тайну и получены органом регулирования естественной монополии на основании статьи 13, разглашению не подлежат. Аналогичные положения содержатся еще в целом ряде федеральных законов, регламентирующих деятельность различных государственных органов.

4.2. Порядок предоставления информации, составляющей коммерческую тайну

Согласно части 1 статьи 6 Закона "О коммерческой тайне", обладатель информации, составляющей коммерческую тайну, обязан предоставлять ее органам государственной власти, иным государственным органам, органам местного самоуправления только по мотивированному требованию. Мотивированное требование должно быть подписано уполномоченным должностным лицом, содержать указание цели и правового основания затребования информации, составляющей коммерческую тайну, и срок предоставления этой информации, если иное не установлено федеральными законами. Поэтому запросы, направляемые хозяйствующим субъектам, должны быть оформлены на официальных бланках того органа, который направил данный запрос, а на самом запросе обязательно должен быть проставлен исходящий номер и указана дата отправления. Следует обратить внимание, что запрос не может быть передан лично в устной форме или по телефону, даже если звонит уполномоченное должностное лицо. Такие требования обладатель коммерческой тайны вправе не выполнять. Также не стоит спешить выполнять и требования о предоставлении коммерчески значимой конфиденциальной информации, если в запросе нет указания, с какой целью и на каких правовых основаниях государственный орган желает получить "секрет фирмы". То есть запрос должен быть мотивированным. Приведем пример.

В коммерческую компанию поступает запрос из органа внутренних дел с требованием представить для проверки первичные документы по учету основных средств за несколько лет. При этом в запросе отсутствуют ссылки на нормы законов, разрешающие милиции запрашивать подобную информацию. В этом случае несмотря на требования пункта 8 статьи 9 Федерального закона от 21 ноября 1996 г. N 129-ФЗ "О бухгалтерском учете", согласно которому "первичные учетные документы могут быть изъяты только органами дознания, предварительного следствия и прокуратуры, судами, налоговыми инспекциями и органами внутренних дел на основании их постановлений в соответствии с законодательством Российской Федерации", запрос можно оставить без ответа. Какова должна быть, если можно так выразиться, "степень мотивированности", законом не установлено. Ясно, что мотивировки такого типа, как "в соответствии с действующим законодательством..." или "на основании страхового законодательства...", нельзя признать достаточными. Представляется наиболее целесообразным в запросе делать ссылку на конкретные статьи нормативно-правовых актов, на основании которых производится этот запрос.

Во всех случаях, когда обладатель коммерческой тайны считает требования государственного органа (органа местного самоуправления) о предоставлении ему тех или иных конфиденциальных сведений незаконными и отказывается исполнить запрос, инициатор запроса, согласно части 2 статьи 6 Закона "О коммерческой тайне", наделяется правом затребовать эту информацию в судебном порядке. Рассмотрение дела в суде дает обеим сторонам спора равные процессуальные возможности для отстаивания своей позиции, что является дополнительной правовой гарантией от злоупотреблений со

стороны чиновников. Кроме того, обладатель коммерческой тайны также наделен правом на обращение в суд - он может подать иск о признании соответствующего предписания государственного органа (органа местного самоуправления) не соответствующим закону, иному нормативному правовому акту. В соответствии со статьей 13 Гражданского кодекса РФ ненормативный акт государственного органа или органа местного самоуправления, а в случаях, предусмотренных законом, также нормативный акт, не соответствующий закону или иным правовым актам, нарушающие гражданские права и охраняемые законом интересы гражданина или юридического лица, могут быть признаны судом недействительными. При обжаловании актов государственных органов или органов местного самоуправления применяется общий срок исковой давности - три года*(10).

Предоставление информации, составляющей коммерческую тайну, органам государственной власти, иным государственным органам, органам местного самоуправления должно осуществляться хозяйствующими субъектами на безвозмездной основе.

Согласно части 4 статьи 6 Закона "О коммерческой тайне", на документах, предоставляемых уполномоченным органам и содержащих информацию, составляющую 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). Это необходимо для правовой охраны поступающей в уполномоченные органы информации, содержащей коммерческую тайну.

4.3. Охрана конфиденциальности информации при ее предоставлении

Создание необходимых условий для предотвращения утечки и разглашения информации, составляющей коммерческую тайну, возлагается на ее обладателя. И чем большую коммерческую ценность информация представляет, тем более совершенной должна быть ее защита. При получении информации с грифом "коммерческая тайна" государственными органами и органами местного самоуправления от ее обладателей, забота о сохранности перекладывается на плечи государства. Согласно статье 13 Закона "О коммерческой тайне", органы государственной власти, иные государственные органы, органы местного самоуправления в соответствии с настоящим Федеральным законом и иными федеральными законами обязаны создать условия, обеспечивающие охрану конфиденциальности информации, предоставленной им юридическими лицами или индивидуальными предпринимателями. Должностные лица органов государственной власти, иных государственных органов, органов местного самоуправления, государственные или муниципальные служащие указанных органов без согласия обладателя информации, составляющей коммерческую тайну, 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 информацию, составляющую коммерческую тайну, за исключением случаев, предусмотренных законодательством, а также не вправе использовать эту информацию в корыстных или иных личных целях. В случае нарушения конфиденциальности информации эти лица несут ответственность в соответствии с законодательством Российской Федерации. Виды и условия ответственности должностных лиц, государственных и муниципальных служащих за разглашение коммерческой тайны мы подробно рассмотрим в [главе 7](#). Здесь же хотелось бы отметить, что конкретные меры по охране конфиденциальности информации при ее предоставлении в Законе "О коммерческой тайне" не оговорены.

Создание надежной системы защиты конфиденциальной информации обходится весьма недешево. Смогут ли государственные органы (не говоря уже об органах местного самоуправления, зачастую не имеющих денег на канцелярские принадлежности) изыскать необходимые финансовые ресурсы - вопрос открытый. Как уже отмечалось, в частном бизнесе существует прямая зависимость: чем ценнее информация и чем большие убытки понесет компания от ее разглашения, тем больше вкладывается сил в ее защиту. Должно ли государство следовать такому подходу? Если да, то как, не имея полного представления о всех аспектах деятельности коммерческой организации, оценить коммерческую ценность предоставленных сведений. Неуверенность предпринимателей в возможности государственных структур сохранить их секреты приводит к попыткам под любыми предлогами уклониться от их предоставления. Именно поэтому законодательством предусмотрена ответственность за невыполнение обладателем информации, составляющей коммерческую тайну, законных требований органов государственной власти (органов местного самоуправления) о предоставлении им такой информации.

4.4. Ответственность за отказ в предоставлении информации

Возможность привлечь к ответственности обладателя информации, составляющей коммерческую тайну, за отказ в ее предоставлении государственным (муниципальным) органам или воспрепятствование в ее получении должностными лицами этих органов предусмотрена статьей 15 Закона "О коммерческой тайне". Ответственность наступает только при условии, что требования инициатора запроса правомерны.

Что же может грозить компании или частному предпринимателю за такой отказ? Согласно статье 19.7 Кодекса РФ об административных правонарушениях, "непредставление или несвоевременное представление в государственный орган (должностному лицу) сведений (информации), представление которых предусмотрено законом и необходимо для осуществления этим органом (должностным лицом) его законной деятельности, а равно представление в государственный орган (должностному лицу) таких сведений (информации) в неполном объеме или в искаженном виде влечет наложение административного штрафа на граждан в размере от одного до трех минимальных размеров оплаты труда; на должностных лиц - от трех до пяти минимальных размеров оплаты труда; на юридических лиц - от тридцати до пятидесяти минимальных размеров оплаты труда. Отметим, что статья 19.7 Кодекса РФ об административных правонарушениях, помимо ответственности за непредставление сведений (информации), предусматривает наказание и за "представление сведений (информации) с нарушением установленных сроков", а также "представление сведений (информации) в неполном объеме либо заведомо недостоверных сведений (информации)". Дела об административных правонарушениях, предусмотренных статьей 19.7 Кодекса РФ об административных правонарушениях, рассматриваются мировыми судьями.

В настоящее время разрешение вопросов в судебном порядке за рассматриваемое правонарушение является скорее исключением, чем правилом. Большинство конфликтов между уполномоченными органами и обладателями информации, составляющей коммерческую тайну, удается разрешить на досудебной стадии. В качестве примера можно вспомнить нашумевший конфликт между управлением специальных технических мероприятий службы криминальной милиции (УСТМ) при ГУВД Самарской области и сотовым оператором ЗАО "Средневожская межрегиональная ассоциация радиотелекоммуникационных систем" ("СМАРТС").

В марте 2004 г. УСТМ обратилось в управление Федеральной службы по надзору в сфере связи ("Россвязьнадзор") по Самарской области с ходатайством о приостановлении действия лицензии сотового оператора. Помимо ходатайства в "Россвязьнадзор" УСТМ направило жалобу на действия оператора связи в суд, намереваясь подвергнуть ЗАО "СМАРТС" административному наказанию. Причиной обращения послужил отказ сотового оператора выполнить требования УСТМ о предоставлении информации. Самарские милиционеры требовали предоставить так называемый частотно-территориальный план сети. Это список базовых станций оператора сточными координатами, частотами и высотой передатчиков. Такая схема расположения передатчиков позволяет точно определить местоположение абонента. В СМАРТСе объяснили свой отказ тем, что требуемая информация отнесена компанией к категории "коммерческая тайна", а УСТМ при формировании своего запроса нарушило порядок получения информации указанной категории, который определен Федеральным законом "О коммерческой тайне". После серии взаимных консультаций стороны пришли к соглашению, тем более что, как выяснилось, сотрудники УСТМ могут получить интересующую их информацию в региональном отделении Радиочастотного центра (государственный орган, занимающийся выделением радиочастот). После этого ГУВД отозвало свой иск в суд и обращение в "Россвязьнадзор".

Глава 5. Охрана коммерческой тайны в рамках гражданско-правовых отношений

5.1. Правовые основы обеспечения конфиденциальности информации в рамках гражданско-правовых отношений

Основное назначение информации, составляющей коммерческую тайну, - получение обладателем такой информации определенных экономических преимуществ перед своими конкурентами и извлечение прибыли из факта ее обладания. Если ваша компания тоже хочет заполучить "секрет фирмы", то есть научно-техническое, технологическое, производственное, финансово-экономическое или иное решение, признанное коммерческой тайной, у вас всего два законных пути.

Первый - нанять в штат фирмы высококвалифицированных специалистов, профинансировать проведение изыскательских работ, иными словами, выработать необходимое "знание" внутри своей

организации.

Второй путь - получение необходимых конфиденциальных сведений по договору со сторонним лицом - первоначальным создателем коммерчески значимой информации. При этом подходе между фирмой (частным предпринимателем), заинтересованной в использовании информации, составляющей коммерческую тайну, и законным обладателем такой информации должен быть заключен гражданско-правовой договор. Такая возможность предусмотрена, в частности, пунктом 4 статьи 7 Закона "О коммерческой тайне", где устанавливается право обладателя коммерческой тайны вводить ее в гражданский оборот на основании договоров. К сожалению, в указанном законе отсутствует четкая регламентация договорных отношений по передаче прав на использование коммерческой информации. Приводятся только некоторые принципиальные требования к условиям их заключения. Основное внимание уделяется обязательствам по сохранению конфиденциальности, которые являются лишь одним из существенных условий таких договоров. Согласно пункту 7 статьи 3 Закона "О коммерческой тайне", передача осуществляется "в объеме и на условиях, которые предусмотрены договором". Такое "емкое" определение не дает никакого ответа на вопрос, какие предусмотрены виды передачи информации, составляющей коммерческую тайну. Можно только предполагать, как это делает большинство цивилистов, что речь идет как об уступке коммерческой тайны, так и о ее предоставлении в целях использования (лицензионном договоре). Однако некоторые правоведы считают, что передача возможна и по другим видам договоров, таким как договор купли-продажи, дарения, подряда, на выполнение научно-исследовательских, опытно-конструкторских и технологических работ. Такая точка зрения выглядит несколько странно с учетом того, что, по действующему законодательству, обладатель коммерческой тайны передает ее контрагенту для использования на определенных условиях, но при этом обладатель остается обладателем коммерческой тайны. Если же согласиться с возможностью передачи секретов по договору купли-продажи, то получается, что "продавец" должен "забыть" всю ту информацию, которую он передал по договору. Зачастую в хозяйственных договорах встречаются формулировки о "передаче прав на ноу-хау". Такая формулировка не совсем точно отражает суть договора. По своей правовой природе договорные отношения, связанные с коммерческой тайной, представляют собой не акт передачи прав на использование конфиденциальной информации. Они строятся на предоставлении контрагенту доступа к сведениям на определенных условиях.

По мере того, как договорные отношения, связанные с коммерческой тайной, перестанут быть экзотикой и прочно войдут в практику делового оборота, проявится еще один существенный пробел законодательства в регулировании рассматриваемых правоотношений. Речь идет о переходе коммерческой тайны (в основном это касается ноу-хау) в общепринятый способ производства. При заключении большого количества договоров о предоставлении доступа к информации, составляющей коммерческую тайну, ее обладатель сталкивается с двумя проблемами. Во-первых, ему все труднее становится осуществлять контроль за своим "секретом", так как это связано с необходимостью отслеживать и пресекать случаи нарушения контрагентами принятых договорных обязательств по соблюдению конфиденциальности. Во-вторых, важно не перешагнуть определенный количественный предел, после которого говорить о неизвестности информации третьим лицам будет уже невозможно. Согласно пункту 2 статьи 39 Соглашения ТРИПС, именно неизвестность информации широкому кругу профессионалов, обычно работающих с подобной информацией, делает ее конфиденциальной. Как уже отмечалось в [главе 1](#), если большинство производителей в каком-либо секторе экономики используют один и тот же "промышленный секрет", то он приобретает статус общепринятого способа производства. В связи с отсутствием в законодательстве четких критериев оценки общезвестности конфиденциальной информации, определять этот количественный предел придется в каждом конкретном случае с участием судебных органов.

Рассмотрим, какие общие требования к договорам, связанным с передачей коммерческой тайны, установлены действующим законодательством. Во-первых, передаваемая информация должна быть обязательно зафиксирована на материальном носителе. Передача коммерческой тайны в устной форме, даже при осуществлении такой передачи на возмездной основе, не может считаться гражданско-правовым договором, и, соответственно, на нее не распространяются меры правовой защиты, предусмотренные законом.

Основным требованием, касающимся договоров о передаче коммерческой тайны, является сохранение конфиденциальности предоставляемой информации. Согласно статье 12 Закона "О коммерческой тайне", в договор в обязательном порядке должны быть включены следующие положения:

1) условия охраны конфиденциальности информации, в том числе, в случае реорганизации или ликвидации одной из сторон договора;

2) обязанность контрагента незамедлительно сообщить обладателю информации, составляющей коммерческую тайну, о допущенном контрагентом либо ставшем ему известным факте разглашения или угрозы разглашения, незаконного получения или незаконного использования коммерческой тайны третьими лицами (даже если такое положение не фигурирует в тексте договора,

эта обязанность контрагента вытекает напрямую из закона);

3) обязанность контрагента по возмещению убытков при разглашении им этой информации вопреки договору.

В указанной статье дважды затрагивается вопрос ответственности контрагента за разглашение полученной по договору информации. Согласно части 2 статьи 12 Закона "О коммерческой тайне", в договоре должна быть установлена обязанность контрагента по возмещению убытков при разглашении им этой информации вопреки договору. Отсюда можно сделать вывод, что, если в тексте договора не будет предусмотрена такая обязанность, контрагент не обязан возмещать убытки. В то же время, в части 6 вышеуказанной статьи закреплено: "сторона, не обеспечившая в соответствии с условиями договора охраны конфиденциальности информации, переданной по договору, обязана возместить другой стороне убытки, если иное не предусмотрено договором", следовательно, обязанность возмещения убытков контрагентом устанавливается законом априори и можно не включать данное положение в договор. Налицо явное противоречие, причем, что называется "не отходя от кассы" - в тексте одной и той же статьи. Предпринимателям остается посоветовать во всех случаях включать данный пункт в договоры во избежание в дальнейшем возможных недоразумений.

В случае если иное не установлено договором между обладателем информации, составляющей коммерческую тайну, и контрагентом, контрагент в соответствии с законодательством Российской Федерации самостоятельно определяет способы защиты коммерческой тайны, переданной ему по договору. Законодательство устанавливает общеобязательный минимальный набор мер по защите конфиденциальности коммерческой информации (эти меры мы рассмотрим в **главе 6**), однако зачастую их может быть явно недостаточно. Поэтому законодатель предусмотрел возможность заранее согласовать перечень охранных мер и включить в договор те из них, на которых настаивает обладатель информации. По смыслу закона можно предположить только одно ограничение на их количественный и качественный состав: обладатель коммерческой тайны может потребовать от контрагента исполнения мер по защите информации только в том объеме, в каком он сам их обеспечил. И это понятно - нет никакого смысла принимать повышенные меры безопасности в одном месте, если интересующие сведения злоумышленник легко может получить в другом.

Законодатель побеспокоился и о защите прав контрагентов. Согласно пункту 5 статьи 12 Закона "О коммерческой тайне", обладатель информации, составляющей коммерческую тайну, переданной им контрагенту, до окончания срока действия договора не может разглашать эту информацию, а также в одностороннем порядке прекращать охрану ее конфиденциальности, если иное не установлено договором. Следует особо еще раз подчеркнуть, что данное требование действует даже в том случае, если компания - первоначальный обладатель реорганизуется или даже ликвидируется. В случае реорганизации обязанность по обеспечению мер информационной безопасности возлагается на компанию-правопреемника в объеме, предусмотренном договором. При ликвидации обладатель обязан принять все возможные меры для предотвращения разглашения переданной контрагенту информации: уничтожить материальные носители (либо по согласованию с контрагентом передать ему все относящиеся к договору конфиденциальные информационные ресурсы), с бывшим персоналом, допущенным к коммерческой тайне, должны быть заключены договоры о ее неразглашении как минимум на период действия договора.

Кроме перечисленных выше обязательных требований в договор по передаче коммерческой тайны, в соответствии с принципом свободы договора, могут быть включены дополнительные условия, касающиеся таких вопросов, как право обладателя информации самому использовать эту информацию и передавать ее другим контрагентам, территория, на которой может быть использована переданная информация и так далее. В частности, определение территории действия договора может быть обусловлено желанием сторон избежать конкуренции при использовании одного и того же ноу-хау контрагентом и первоначальным обладателем коммерческого секрета на одной и той же территории (стороны хотят поделить "зоны влияния").

5.2. Права и обязанности сторон по отдельным видам гражданско-правовых договоров

Как правило, передача информации, составляющей коммерческую тайну, в рамках гражданско-правовых отношений происходит путем передачи права пользования информацией контрагенту на основе лицензионных соглашений, которые могут иметь как исключительный, так и неисключительный характер. Примером может служить лицензионный договор, в рамках которого оформляются отношения между правообладателем (лицензиаром) и пользователем (лицензиатом). Такие лицензионные договоры не имеют законодательного закрепления и обычно рассматриваются цивилистами, как договоры *sui generis*, особого рода, имеющие определенное сходство с договорами купли-продажи, аренды. В настоящее время в международном обороте четко наметилась тенденция существенного

роста объема таких лицензионных договоров. Право на коммерческую информацию может передаваться по договору коммерческой концессии (франчайзинга). Отдельные элементы лицензионного договора могут быть включены в другие гражданско-правовые договоры, такие как договор на передачу готовых научно-технических разработок - технологий, конструкций, содержащих незапатентованные технические решения, договоры подряда, совместной деятельности, о создании акционерного общества. Еще раз подчеркнем, что во всех договорах, в которых предусматривается разрешение на использование сведений, составляющих коммерческую тайну, на контрагента должна быть возложена обязанность по соблюдению ее конфиденциальности. Рассмотрим более подробно наиболее часто используемые виды договоров о передаче коммерческой тайны.

Лицензионный договор. Самым широко распространенным видом договоров, посредством которого информация, составляющая коммерческую тайну, вводится в гражданский оборот, являются так называемые лицензионные договоры. Если быть точным, то такой вид договоров нельзя назвать "лицензионным" в традиционном смысле. Это связано с тем, что его предметом является предоставление самой информации, а не исключительного права на ее использование. Напомним, что коммерческая тайна имеет иную правовую природу, чем объекты интеллектуальной собственности, и, следовательно, у обладателя информации отсутствует на нее исключительное право. Таким образом, лицензионный договор о передаче коммерческой тайны отличается от патентной лицензии по объекту отчуждаемых прав, поэтому часто для его обозначения применяют другое название - "беспатентная лицензия". В последнее время все большее распространение получает комбинированный вид договоров - в лицензионные соглашения об использовании патента включаются отдельным пунктом соглашения о передаче информации, составляющей коммерческую тайну (чаще всего это касается ноу-хау).

Существенными условиями рассматриваемого вида договоров являются условия о предмете договора, порядке и сроке передачи коммерческой тайны, о вознаграждении за передаваемую информацию, о территории и сроке действия договора. Принципиальным является вопрос о сохранении за обладателем права использования передаваемого по договору "секрета", а также о возможности передачи его третьим лицам. По данному критерию договоры подразделяются на исключительные и неисключительные. Возможно и такое условие, по которому информацию, составляющую коммерческую тайну, вправе передавать по договору третьим лицам только лицензиат (получатель).

Коммерческая тайна передается в виде описания, которое оформляется в виде приложения к договору (даже если описание невелико по объему, включать его в текст договора не рекомендуется). В качестве такого приложения может выступать не только бумажный носитель, но и любой другой (например, магнитный носитель). Ряд авторов придерживается мнения о возможности передачи "коммерческого опыта" в нематериальной форме (в виде оказания технической помощи, обучения, управленческих услуг), однако такой подход противоречит пункту 7 статьи 3 Закона "О коммерческой тайне". Более того, чаще всего в договор включается обязанность лицензиара без дополнительной оплаты оказать получателю помощь в уяснении содержания передаваемой информации путем дачи необходимых консультаций. Поэтому даже в том случае, если стороны соглашения договорились о проведении обучения персонала, то передачу коммерческой тайны необходимо все же закрепить путем оформления соответствующих протоколов.

Передача осуществляется после выплаты лицензиатом вознаграждения в полном объеме или паушального взноса по акту, подписываемому сторонами договора*(11).

Вознаграждение выплачивается обычно в виде роялти и определяется в процентах от прибыли (дохода) получателя от использования коммерческой тайны. Кроме того, на размер роялти обычно влияют следующие факторы:

- 1) при передаче информации на исключительной основе ставка значительно повышается;
- 2) предоставление права лицензиату передавать по сублицензионным договорам информацию третьим лицам также увеличивает размер вознаграждения;
- 3) срок действия лицензионного договора (обычно ставка роялти тем ниже, чем больше срок).

Если срок действия договора не установлен, считается, что он заключен на неопределенный срок, так как предметом договора является не патент, срок действия которого определен и по истечении которого договор прекращает свое действие, а коммерческая тайна. Если по тем или иным причинам информация, положенная в основу соглашения, стала общедоступной, договор прекращает свое действие;

4) в какой отрасли экономической деятельности коммерческая тайна предназначена для использования.

В договоре может предусматриваться ежегодная выплата лицензиатом обладателю коммерческой тайны минимальных жестко установленных платежей в случае неиспользования им полученной по договору информации для извлечения прибыли. Ясно, что при такой системе оплаты существенным условием договора становится вопрос о механизме контроля лицензиара за промышленно-финансовой деятельностью приобретателя информации. Обычно механизм контроля

предусматривает ежеквартальный отчет об объемах производства и ценах на продукцию, выпускаемую лицензиатом с использованием "секрета производства", и ежегодную проверку бухгалтерской отчетности контрагента представителями лицензиара с целью удостовериться в подлинности предоставленных в течение года данных.

С целью защиты законных интересов получателя информации, составляющей коммерческую тайну, договор должен предусматривать ответственность лицензиара за несовпадение переданной информации и той, которая была продекларирована при заключении договора (иными словами, передали ноу-хау, а оно не работает, как было заявлено). В этом случае обладатель обязан возместить все полученные по договору платежи, включая паушальный взнос и оплатить неустойку. Следует отметить, что согласно пункту 3 статьи 10 Гражданского кодекса РФ, презюмируется добросовестность лицензиара, поэтому бремя доказывания возлагается на получателя.

Кроме всего вышеперечисленного, рекомендуется предусмотреть в договоре обязанность получателя коммерческой тайны после прекращения действия договора передать обладателю информации все материальные носители, включая созданные в период действия договора самим лицензиатом, которые могут раскрывать конфиденциальные сведения третьим лицам.

Договор коммерческой концессии. Остановимся более подробно на договоре коммерческой концессии, как наиболее универсальном инструменте. Этот относительно новый для российского законодательства договорный институт близок по своей правовой природе к "франчайзингу" - широко распространенной в странах "развитого капитализма" системе коммерческих отношений, применяемой в различных областях экономического оборота. Согласно статье 1027 Гражданского кодекса РФ, "по договору коммерческой концессии одна сторона (правообладатель) обязуется предоставить другой стороне (пользователю) за вознаграждение на срок или без указания срока право использовать в предпринимательской деятельности пользователя комплекс исключительных прав, принадлежащих правообладателю, в том числе право на фирменное наименование и (или) коммерческое обозначение правообладателя, на охраняемую коммерческую информацию, а также на другие предусмотренные договором объекты исключительных прав - товарный знак, знак обслуживания и так далее".

Следует отметить, что, с точки зрения юридической техники, указанная статья имеет ряд неточностей. В законодательстве о коммерческой тайне отсутствует термин "охраняемая коммерческая информация". Ясно, что речь идет об информации, составляющей коммерческую тайну, однако коммерческая тайна не относится к объектам исключительных прав. Договор коммерческой концессии предусматривает использование комплекса исключительных прав, деловой репутации и коммерческого опыта правообладателя в определенном объеме (в частности, с установлением минимального и (или) максимального объема использования), с указанием или без указания территории использования применительно к определенной сфере предпринимательской деятельности (продаже товаров, полученных от правообладателя или произведенных пользователем, осуществлению иной торговой деятельности, выполнению работ, оказанию услуг). В соответствии с частью 3 статьи 1027 Гражданского кодекса РФ, сторонами по договору коммерческой концессии могут быть коммерческие организации и граждане, зарегистрированные в качестве индивидуальных предпринимателей.

Договор коммерческой концессии должен быть в обязательном порядке заключен в письменной форме. В противном случае договор считается ничтожным (ч. 1 ст. 1028 Гражданского кодекса РФ). Помимо этого, он подлежит регистрации в том федеральном органе исполнительной власти, где зарегистрирован правообладатель (если правообладатель зарегистрирован за рубежом, то допускается регистрация договора по месту регистрации пользователя). Если по договору коммерческой концессии предоставляются права на использование объектов промышленной собственности (товарных знаков, полезных моделей, изобретений, охраняемых свидетельством или патентом) и объекты патентного права, то договор подлежит также регистрации в Патентном ведомстве.

Согласно статье 1032 Гражданского кодекса РФ в обязанности пользователя договора коммерческой концессии входит требование о неразглашении секретов производства правообладателя и другой полученной от правообладателя конфиденциальной коммерческой информации (хотя, как мы уже отмечали, такая обязанность возлагается на контрагента по всем договорам, в которых предусмотрена передача информации, составляющей коммерческую тайну).

Следует различать договор коммерческой концессии и лицензионный договор на право пользования информацией, составляющей коммерческую тайну. В отличие от лицензионного договора, при котором права передаются контрагенту только на отдельные объекты интеллектуальной собственности и коммерческой тайны, по договору коммерческой концессии предоставляется право использовать весь комплекс исключительных прав (фирменное наименование, товарный знак, знак обслуживания, ноу-хау и т.д.), принадлежащих правообладателю. Можно сказать, что передача "комплекса прав" контрагенту выступает в качестве существенного условия, необходимого для признания заключенного договора "коммерческой концессией". Несмотря на то, что между двумя рассматриваемыми видами договоров имеются существенные различия, зачастую приходится

сталкиваться с тем, что в судебной практике возникают споры, связанные с квалификацией договоров на передачу информации, составляющей коммерческую тайну. В качестве примера можно привести следующий судебный прецедент.

ОАО "Нижнекамскшина" обратилось в Нижнекамский городской суд с иском к А., В. и С. о признании недействительным договора "О передаче ноу-хау", заключенного между В. и С. с одной стороны, и А., с другой. Истец обосновывал свое требование тем, что оспариваемый договор относится к договорам коммерческой концессии и, следовательно, В. и С. не имели права на заключение такого вида договора по передаче ноу-хау, так как они не были в установленном порядке зарегистрированы в качестве частных предпринимателей, а согласно правилам статьи 1027 Гражданского кодекса РФ, сторонами по договору коммерческой концессии могут быть лишь коммерческие организации и граждане, зарегистрированные в качестве индивидуальных предпринимателей.

Ответчик искивые требования не признал в полном объеме на том основании, что "спорный договор не является договором коммерческой концессии, а форма договора полностью соответствует требованиям Гражданского кодекса РФ". Однако суд возражения ответчика не убедили, и он принял решение удовлетворить иск, признав, что оспариваемый договор является договором коммерческой концессии.

В обоснование своего решения, суд привел следующие аргументы: в соответствии с пунктами 1.1-1.4 и 5.1-5.4 договора В. и С. передавали А. "материалы по ноу-хау - способ изготовления шипованной шины, ошипованного ленточного протектора для этой шины и шипа противоскольжения для этого протектора". По мнению суда, переданные по договору материалы содержали "коммерческую информацию", права на использование которой были предоставлены А. Суд также сослался на нормы Гражданского кодекса РФ о коммерческой концессии (Глава 54), согласно которым предоставление права на коммерческую информацию входит в состав предмета договорных отношений в рамках коммерческой концессии. А поскольку сторонами договора коммерческой концессии могут быть лишь коммерческие организации, либо предприниматели, договор, как противоречащий закону, в соответствии со статьей 168 Гражданского кодекса РФ, был признан недействительным.

В данном случае приходится констатировать, что суд не принял во внимание, что оспариваемый договор не содержит обязательство о предоставлении комплекса исключительных прав, включая право на фирменное наименование и, следовательно, не может быть признан коммерческой концессией. А в связи с тем, что специальное регулирование договоров о передаче прав на информацию, содержащую коммерческую тайну, законом не установлено, стороны, в соответствии с пунктом 2 статьи 421 и пунктом 2 статьи 1 Гражданского кодекса РФ (принцип "свободы договора"), свободны в определении любых не противоречащих законодательству условий заключенного ими лицензионного договора.

Еще один вопрос, часто возникающий на практике, связан с внесением различного рода информации, составляющей коммерческую тайну, в качестве вклада в имущество хозяйственного товарищества или общества. Действительно, если информация представляет коммерческую ценность (реальную или потенциальную), почему бы не внести ее в указанном качестве в имущество хозяйственного товарищества или общества наравне с другим имуществом. Еще относительно недавно в законодательстве отсутствовали какие-либо нормы, позволяющие однозначно урегулировать этот вопрос. Только в 1996 г. Пленумы Верховного Суда Российской Федерации и Высшего Арбитражного Суда Российской Федерации совместным постановлением поставили точку, указав следующее.

В качестве вклада в имущество хозяйственного товарищества или общества могут вноситься имущественные права, либо иные права, имеющие денежную оценку. В связи с этим, таким вкладом не может быть объект интеллектуальной собственности (патент, объект авторского права, включая программу для ЭВМ, и тому подобное) или ноу-хау. Однако в качестве вклада может быть признано право пользования таким объектом, передаваемое обществу или товариществу в соответствии с лицензионным договором, который должен быть зарегистрирован в порядке, предусмотренном законодательством (п. 17 Постановления Пленума ВС РФ и Пленума ВАС РФ "О некоторых вопросах, связанных с применением части первой Гражданского кодекса РФ" от 1 июля 1996 г. N 6/8).

С этого момента судебная практика приняла единообразный характер. В качестве примера можно привести решение Федерального Арбитражного Суда Ханты-Мансийского автономного округа от 24 января 2002 г., признавшего недействительной сделку по внесению компанией "Norex Petroleum" 50% вклада в уставный капитал ЗАО "Корпорация "Югранефть" в виде ноу-хау. Еще одним примером является Постановление Федерального Арбитражного Суда Московского округа от 1 апреля 2002 г. N КА-А40/1697-02. Суд признал правомерность решения ответчика об отказе в регистрации юридического лица, который был обусловлен тем, что в качестве вклада в уставный капитал была представлена заявка на изобретение, оцененная в некоторую денежную сумму. Вероятно, если бы в качестве вклада фигурировало право на использование новации, описанной в заявке на изобретение (в режиме коммерческой тайны), а не сама заявка, то оснований для отказа в регистрации суд не усмотрел бы. Представляется, что "ноу-хау" применительно к Постановлению N 6/8 нужно понимать в

расширенном значении как любую информацию, составляющую коммерческую тайну.

Если с внесением в качестве вклада прав на использование запатентованного изобретения у налоговых органов вопросов не возникает, то с информацией, составляющей коммерческую тайну, дело обстоит гораздо сложнее. Это связано с тем, что законом не предусмотрено (и в силу особой правовой природы не может быть предусмотрено) официальных государственных свидетельств о факте регистрации коммерческой тайны. Следует отметить, что зачастую такой вид вкладов используется с целью различного рода схем по минимизации налогов. Примером может служить судебное решение Президиума Высшего Арбитражного Суда РФ по иску товарищества с ограниченной ответственностью "Редакция газеты "Прямой контакт" к Государственной налоговой инспекции по городу Саранску (постановление Президиума ВАС РФ N 3225/96 от 24 декабря 1996 г.). Данный пример характерен тем, что отражает отсутствие единой позиции у судов различного уровня по делам, связанным с коммерческой тайной.

Президиум Высшего Арбитражного Суда Российской Федерации рассмотрел протест заместителя Председателя Высшего Арбитражного Суда Российской Федерации на постановление апелляционной инстанции Арбитражного суда Республики Мордовия от 8 апреля 1996 г. по делу N 6/1 и постановление Федерального арбитражного суда Волго-Вятского округа от 24 мая 1996 г. по тому же делу.

Заслушав и обсудив доклад судьи, Президиум установил следующее.

ТОО "Редакция газеты "Прямой контакт" обратилось в Арбитражный суд Республики Мордовия с иском к ГНИ по г.Саранску о признании недействительным решения от 23 февраля 1996г. по акту документальной проверки от 6 декабря 1995 г. N 238 в части взыскания 28 868 300 рублей заниженной прибыли, налога на рекламу и соответствующих санкций.

Решением от 1 марта 1996 г. решение налоговой инспекции от 23 февраля 1996 г. в части взыскания 1677900 рублей признано недействительным. В остальной части иска отказано.

Постановлением апелляционной инстанции от 8 апреля 1996 г. решение изменено. Решение налоговой инспекции от 23 февраля 1996 г. в части взыскания 28 611 500 рублей заниженной прибыли, налога на рекламу и соответствующих санкций признано недействительным. В остальной части иска отказано.

Федеральный арбитражный суд Волго-Вятского округа постановлением от 24 мая 1996 г. оставил без изменения постановление апелляционной инстанции Арбитражного суда Республики Мордовия.

В протесте заместителя Председателя Высшего Арбитражного Суда Российской Федерации предлагается постановления апелляционной и кассационной инстанций отменить, оставить в силе решение Арбитражного суда Республики Мордовия.

Президиум считает, что протест подлежит удовлетворению по следующим основаниям.

Как видно из материалов дела, Государственная налоговая инспекция по городу Саранску при документальной проверке соблюдения налогового законодательства ТОО "Редакция газеты "Прямой контакт" за 1994 г. и 9 месяцев 1995 г. установила занижение налога на рекламу на сумму 155200 рублей и налогооблагаемой прибыли на сумму 13558200 рублей, в том числе, из-за необоснованного включения в себестоимость продукции износа нематериальных активов на сумму 13350000 рублей. По результатам проверки составлен акт от 6 декабря 1995 г. N 238 и принято решение от 23 февраля 1996 г. о взыскании заниженной прибыли, налога на рекламу и соответствующих финансовых санкций.

Учредители товарищества (три физических лица) в качестве вклада в уставный фонд внесли на безвозмездной основе интеллектуальную собственность, которую квалифицировали, как коммерческую информацию, в виде коммерческих условий на опубликование рекламных объявлений, методики начисления комиссионных доходов, поступающих на расчетный счет товарищества от рекламных услуг, реализуемых с участием посредников, и коммерческих условий для рекламодателей.

Принятие в уставный фонд интеллектуальной собственности оформлено договорами от 28 февраля 1994г. N1, 2 от 26 декабря 1994г. N3 и актами от 1 марта 1994г., 26 декабря 1994г. Стоимость коммерческой информации учредители оценили в 1 500 000 рублей, 600 000 рублей и 30 000 000 рублей, отразив ее на счетах баланса товарищества в качестве нематериальных активов. С марта 1994 года по октябрь 1995 года на эти нематериальные активы товариществом ежемесячно начислялся износ в размере 10 процентов и на себестоимость отнесено в 1994 году 2 100 000 рублей, в 1995 году - 11 250 000 рублей (всего 13 350 000 рублей), что повлекло занижение налогооблагаемой прибыли.

Удовлетворяя иски о признании недействительным решения налоговой инспекции от 23 февраля 1996 г. в части взыскания 13 350 000 рублей заниженной прибыли и санкций, суды сослались на Положение о составе затрат по производству и реализации продукции (работ, услуг), включаемых в себестоимость продукции (работ, услуг) и о порядке формирования финансовых результатов, учитываемых при налогообложении прибыли, утвержденное постановлением Правительства Российской Федерации от 5 августа 1992 г. N552 (п. 2 "ш" - в редакции до 1 января 1995 г. и п. 2 "ц" - в редакции постановления Правительства Российской Федерации от 1 июля 1995 г.

№661).

Между тем, согласно пункту 2 "ц" вышеназванного Положения в себестоимость продукции (работ, услуг) включается износ по нематериальным активам, к которым относятся затраты предприятий в нематериальные объекты, используемые в течение долгосрочного периода в хозяйственной деятельности и приносящие доход: права пользования земельными участками, природными ресурсами, патенты, лицензии "ноу-хау", программные продукты, монопольные права и привилегии (включая лицензии на определенные виды деятельности, организационные расходы (включая плату за государственную регистрацию предприятия, брокерское место и т.п.), торговые марки и торговые знаки и тому подобное).

В редакции постановления Правительства Российской Федерации от 1 июля 1995 г. №661 (п. 2 "ц") в себестоимость продукции (работ, услуг) включается амортизация нематериальных активов, используемых в процессе осуществления уставной деятельности, по нормам амортизационных отчислений, рассчитанных организацией, исходя из первоначальной стоимости и срока их полезного использования (но не более срока деятельности организаций).

В соответствии с пунктом 17 постановления совместного Пленума Верховного Суда Российской Федерации и Высшего Арбитражного Суда Российской Федерации от 1 июля 1996 г. №6/8 в качестве вклада в имущество хозяйственного товарищества или общества могут вноситься имущественные права либо иные права, имеющие денежную оценку, и объект интеллектуальной собственности (патент, объект авторского права, включая программу ЭВМ и т.п.) или "ноу-хау" таким вкладом не может быть. Однако в качестве вклада возможно признание права пользования таким объектом, передаваемое обществу или товариществу в соответствии с лицензионным договором, зарегистрированным в порядке, предусмотренном законодательством.

Коммерческая информация, внесенная учредителями ТОО "Редакция газеты "Прямой контакт" в уставный фонд, по существу является условиями типовых договоров, заключаемых товариществом с рекламодателями, и регламентирует стоимость рекламных объявлений, порядок оплаты и расчетов, размер неустойки за нарушение условий упомянутых договоров. Эти условия не содержат каких-либо новаций в области экономической эффективности использования технических, технологических, коммерческих и других знаний. Условия таких договоров прямо вытекают из гражданского законодательства. Право пользования переданной в уставный фонд коммерческой информацией не оформлено в соответствии с зарегистрированным в предусмотренном законодательством порядке лицензионным договором.

Списание нематериальных активов на себестоимость производится при определенных условиях, что отражается по счету 05 "Износ нематериальных активов". Такими условиями являются, в частности, затраты предприятия в нематериальные объекты. В отношении коммерческой информации необходимы доказательства содержания в ней признаков объектов интеллектуальной собственности, предусмотренных статьей 139 Гражданского кодекса Российской Федерации. Нематериальные объекты должны использоваться в хозяйственной деятельности - участвовать в процессе производства продукции (работ, услуг), что подтверждается технологическими документами, сметами, другими учетными документами, фиксирующими факт совершения хозяйственной операции с этими нематериальными объектами. Использование этих объектов должно приносить доход.

В материалах дела нет каких-либо доказательств экономической эффективности использования коммерческой информации в хозяйственной деятельности, связанной с производством и выпуском газеты, и документов, свидетельствующих о доходности предприятия от этой деятельности.

При таких обстоятельствах товарищество неправоммерно включало в себестоимость износ нематериальных активов, уменьшая тем самым налогооблагаемую прибыль. Решение налоговой инспекции от 23 февраля 1996 г. является правоммерным, оснований для признания его в этой части недействительным не имелось.

Исходя из изложенного и руководствуясь статьями 187-189 Арбитражного процессуального кодекса Российской Федерации, Президиум Высшего Арбитражного Суда Российской Федерации постановил: постановление апелляционной инстанции Арбитражного суда Республики Мордовия от 8 апреля 1996 г. по делу № 6/1 и постановление Федерального арбитражного суда Волго-Вятского округа от 24 мая 1996 г. по тому же делу отменить. Оставить в силе решение Арбитражного суда Республики Мордовия от 1 марта 1996 г.

В рассмотренном деле суд смог с достаточной достоверностью установить отсутствие какой бы то ни было коммерческой тайны в информации, переданной в уставный капитал ТОО. Вообще же, реальность факта наличия у информации всех признаков коммерческой тайны бывает весьма сложно подтвердить или опровергнуть. При желании, учредители компании могут выдавать за "секрет фирмы" почти любую информацию, ссылаясь на ее коммерческую ценность, защищенность и неизвестность. Как же доказать налоговикам, что ноу-хау реально существует и право на его использование внесено в качестве вклада в уставный капитал компании? Наиболее эффективный способ - заключение

лицензионного договора на передачу коммерческой тайны (хотя по действующему законодательству регистрация лицензионных договоров о передаче такой информации не предусмотрена).

Но даже если вам удалось убедить контролирующие органы в том, что информация, право на использование которой передано в качестве вклада в уставный капитал, - действительно коммерческая тайна, трудности на этом не заканчиваются. Вопросы могут возникнуть и с имущественной оценкой такого вклада.

Пример из судебной практики - Постановление Федерального Арбитражного Суда Московского округа от 19 июля 2000 г. N КА-А40/3035-00. Суть дела такова: комитет по управлению имуществом обратился в суд с иском к ОАО о признании недействительным заключения эксперта, который провел оценку части вклада в уставный капитал компании (объекта интеллектуальной собственности). Истец полагал, что оценка была произведена с нарушением требований Федерального закона "Об оценочной деятельности в Российской Федерации". Суд, выслушав доводы сторон, признал, что данный спор неподведомственен арбитражному суду в связи с тем, что оспариваемое заключение не является нормативным актом органа, не носит властно-распорядительного характера и не порождает юридических последствий, а достоверность определения величины интеллектуальной собственности объекта в иске не рассматривалась. В рассмотренном деле в качестве вклада выступало право на использование объекта интеллектуальной собственности, но аналогичная ситуация складывается и с информацией, составляющей коммерческую тайну.

Глава 6. Режим коммерческой тайны

6.1. Меры по защите конфиденциальности информации

Как отмечалось ранее, для того, чтобы информация могла быть признана содержащей коммерческую тайну, необходимо выполнение обязательного условия - ее обладатель должен принимать меры к охране конфиденциальности этой информации. Это требование устанавливается статьей 139 Гражданского кодекса. Сходным образом данное условие сформулировано в пункте 2 статьи 3 Закона РФ "О коммерческой тайне". Там речь идет о введении в отношении информации "режима коммерческой тайны".

Режим коммерческой тайны - это и есть меры по охране конфиденциальности информации, составляющей коммерческую тайну. В пункте 3 статьи 3 указанного закона дается перечень возможных мер, к числу которых законодатель отнес правовые, организационные и технические. Данный перечень является открытым - обладателю информации предоставлено право по своему усмотрению формировать систему защиты и противодействия возможным попыткам получения незаконного доступа к своим секретам.

Следует отметить, что в чистом виде, без тесной взаимосвязи, невозможно эффективное применение любой отдельно взятой меры. Чтобы применить какую-либо "техническую меру" в области экономической безопасности, например, оборудовать офисы компании системой внутреннего видеонаблюдения, нужно для начала провести правовую экспертизу проекта - не будут ли нарушены конституционное право сотрудников на неприкосновенность частной жизни и иные права (в условиях все возрастающей юридической грамотности и приоритета прав человека это грозит предпринимателям, пренебрегающим данным условием, значительными финансовыми потерями на оплату судебных исков). Возможно, реализация проекта потребует внести ряд изменений в трудовые договоры (контракты). Затем нужно собрать необходимые разрешения на производство соответствующих работ (возможно, что для их проведения требуется получение лицензии или прохождение иных процедур, предусмотренных законодательством, например, прохождение экспертизы на экологическую безопасность). После этого - оценить целесообразность с точки зрения соотношения затрат на внедрение системы и возможных убытков при утечке охраняемой информации. Нужно разработать ряд внутрикорпоративных (локальных) нормативных актов (положений, инструкций, приказов) по работе и обслуживанию внедряемой системы и подготовить соответствующий персонал.

Как видно из приведенного примера, при применении одной технической меры сразу возникает необходимость принять множество мер юридического и организационного характера, поэтому целесообразней было бы говорить о правовых, организационных и технических компонентах единой политики безопасности от несанкционированного доступа. Попытки некоторых авторов разграничить меры по охране конфиденциальности коммерческой информации, без учета их комплексного, многокомпонентного характера, носят искусственный характер и не обусловлены практической необходимостью. Примером такого подхода может служить классификация, предложенная Э.Я. Соловьевым*(12).

Таблица 6.1. Классификация организационных, технических и специальных мер

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 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 хранения документов	Проведение расследования для документов при утере

Все перечисленные меры включают в себя множество мероприятий самого различного характера, за счет которых они могут быть реализованы. Такая "специальная мера", как применение устройств скрытого фиксирования незаконного доступа к документам, имеет ярко выраженную "техническую природу". Примером такой меры может служить химическая ловушка. В соответствии с рекомендациями МВД России о порядке применения химических ловушек в раскрытии краж имущества, находящегося в государственной, муниципальной, частной собственности и собственности общественных объединений (организаций), это снаряженные (обработанные) специальными химическими веществами (красящими или запаховыми) приспособления или устройства, замаскированные под различные предметы, с помощью которых такие вещества переносятся на тело и одежду человека.

Техническое исполнение химических ловушек может быть самым различным, но принцип действия у них один: попав на кожу правонарушителя, краситель не смывается в течение довольно длительного времени (от суток до нескольких дней). Особенно эффективными на практике показали себя ловушки, начиненные химическими веществами, которые не оставляют заметных пятен, а их метки можно увидеть только с использованием специальных устройств (например, источника излучения в ультрафиолетовом диапазоне). Злоумышленник может и не догадываться, что теперь он сам является вещественным доказательством по делу об "экономическом шпионаже", и не принять мер предосторожности для уничтожения следов (в буквальном смысле) преступления.

Однако в последнее время некоторыми правоведами была поставлена под сомнение правомочность использования таких средств защиты от посягательства на том основании, что, якобы, их применение может повлечь нарушение личных неимущественных прав граждан, в частности, чести, достоинства и репутации. Не совсем понятно, каким образом добропорядочный сотрудник может уронить свои честь, достоинство и деловую репутацию. А вот даже если он и не собирался продавать секреты своей компании, а решил из любопытства поближе познакомиться с каким-либо из носителей конфиденциальной информации - в любом случае им нарушается порядок разграничения доступа, который должен устанавливаться локальными инструкциями (отсюда еще раз видно, кстати, насколько взаимосвязаны все компоненты мероприятий по защите информации). Как минимум странными можно назвать и опасения по поводу того, что в определенных условиях использование химических ловушек может быть расценено, как средство получения информации о личности без ее ведома и согласия, что является нарушением положений Конституции РФ*(13).

Чтобы таких вопросов не возникало, химические ловушки можно с успехом заменить на электронные. Это небольшое устройство (размером с зажигалку), которое активизируется при освещении его поверхности. Его можно заложить в сейф или любой другой светонепроницаемый контейнер с конфиденциальными документами. При срабатывании оно может издавать звуковой сигнал, а также с помощью радиопередающего устройства передать сигнал на центральный пункт сигнализации.

В настоящее время стоимость таких устройств не превышает 20 долларов США, и их использование может позволить себе даже небольшая компания.

6.2. Применение специальных технических систем для защиты коммерческой тайны

Использование технических систем для охраны конфиденциальности информации с течением времени приобретает все большее значение. Это обусловлено тем, что в результате бурного развития техники, прежде всего микроэлектроники, практически не осталось предприятий и организаций, где для обработки, хранения и передачи информации, в том числе конфиденциального характера, не использовались бы те или иные технические устройства. В первую очередь, это касается использования компьютерной техники. Соответственно, появились целые классы технических устройств для несанкционированного снятия, копирования и передачи такой информации. Наибольшее распространение в силу своей относительной простоты и удобства использования получили радиомикрофоны, в простонародье именуемые "жучками". Специалисты используют другой термин - "закладка". Закладки могут быть самыми разными - телефонными, акустическими, лазерными, комбинированными.

Телефонные радиомикрофоны предназначены для съема информации, передаваемой по телефонным сетям, и передачи ее на специальное приемное устройство, которое может быть удалено от закладки на расстояние от 20 до 250 м. Такие закладки могут устанавливаться непосредственно в телефонный аппарат, телефонные розетки, "живляться" в телефонные провода. Телефонные радиомикрофоны могут быть линейные или индукционные. Линейные подключаются к телефонной линии параллельно и не нуждаются в автономном источнике электропитания, они одновременно снимают информацию и получают питание от телефонной сети. Индукционные радиомикрофоны крепятся на один из проводов телефонной пары и питаются за счет компактных аккумуляторов. Это является их основным минусом при использовании - время их действия ограничено (пока не разрядится источник питания, современные индукционные радиомикрофоны могут действовать без подзарядки от двух до семи суток). Кроме того, необходимость в автономном источнике питания сказывается на их размерах. Зато этот тип закладок практически невозможно вычислить с помощью анализаторов телефонных линий, принцип действия которых основан на измерении электрического сопротивления телефонной линии. При использовании линейных радиомикрофонов электрическое сопротивление линии изменяется по сравнению с его нормальной величиной, и анализатор позволяет выявить жучок на линии. Подключение же индукционного радиомикрофона не влияет на сопротивление линии.

Самым надежным способом обнаружения телефонных радиомикрофонов является простой осмотр телефонного аппарата и доступного отрезка телефонной линии. Не стоит полностью полагаться на такие средства противодействия телефонным жучкам, как "зашумление" и подъем напряжения в линии, который осуществляется с помощью разрядника. Сначала от телефонной сети отключается вся оргтехника, разрядник подключают к телефонной розетке и подают в телефонную сеть электрический импульс высокого напряжения, который "выжигает" установленные жучки. Есть принципиально иной метод - не ликвидировать жучок, а попробовать провести "встречную игру", давая ложную информацию с целью ввести в заблуждение хозяина закладки.

Акустические радиомикрофоны представляют собой электронные устройства для ретранслирования всей звуковой информации из помещения, где они заложены на специальный приемник. В настоящее время их конструкция позволяет вмонтировать их в мелкие (чаще всего канцелярские) предметы - в шариковую ручку, пачку сигарет, зажигалку и т.д. Существуют акустические радиомикрофоны как питаемые от собственных автономных источников, так и монтируемые к сети электропитания (чаще всего такие закладки устанавливаются в офисе во время ремонта, что позволяет надежно замаскировать их под внешним покрытием стен). Акустические жучки позволяют "снимать" информацию даже с такого допотопного и, на первый взгляд, безопасного аппарата, как механическая пишущая машинка (некоторые специалисты по безопасности, не доверяя ЭВМ, предлагают печатать особо важные конфиденциальные документы именно таким способом с последующим уничтожением отработанной копировальной перфоленты). Однако следует учитывать, что по стуку клавишей пишущей машинки специалист с помощью электроники может восстановить текст отпечатанного документа. То же самое можно сказать и о шуме, издаваемом печатающим принтером.

Лазерные микрофоны используются для дистанционного снятия информации на расстоянии прямой "видимости" лазерным излучателем оконных стекол автомобиля или офиса. Принцип их действия заключается в анализе микровибраций оконных стекол от акустических колебаний, возникающих, как это не покажется невероятным, от колебаний воздуха при разговоре внутри помещения. Лазерные микрофоны могут устанавливаться только на неподвижную поверхность. Они плохо работают при наличии посторонних источников вибраций, например, вблизи автомобильных

магистралей. Стоимость их достаточно высока, однако они пользуются высоким спросом, так как обнаружить это прослушивание практически невозможно.

Так называемые комбинированные радиомикрофоны совмещают в себе возможности телефонных и акустических закладок. Когда ведутся разговоры по телефону, они осуществляют контроль как линейные телефонные жучки, когда же трубка положена на рычаг, они действуют как акустические, передавая любые разговоры в помещении на приемное устройство. Питание таких радиомикрофонов осуществляется чаще всего за счет телефонной линии.

Для борьбы со всеми видами радиомикрофонов применяются индикаторы поля, которые позволяют выявить локализацию закладки для дальнейшего визуального поиска.

Вне помещений на открытом пространстве применяются направленные микрофоны, которые имеют узкий сектор перехвата - всего от 2 до 40 градусов и очень высокую чувствительность, что позволяет прослушивать разговор на значительном расстоянии (до 80 м). При этом требуется выполнить два условия. Первое - четко позиционировать микрофон в сторону интересующего объекта. Второе - между микрофоном и объектом прослушивания не должно быть непрозрачных для колебаний воздуха препятствий (например, заборов, зданий), а также источников более интенсивных вибраций, таких как транспортные магистрали с интенсивным движением. Направленные микрофоны камуфлируются под зонты, портфели и так далее и могут быть снабжены магнитофоном для записи переговоров, либо передатчиком, передающим сигналы оператору на значительное расстояние.

Существуют на вооружении у экономических шпионов и средства перехвата радиопереговоров - сканирующие приемники или сканеры. Они позволяют производить прослушивание сотовых и радиотелефонов, аппаратов спутниковой связи. Кстати, этот вид орудий шпионажа применяется и как средство для борьбы с ним - сканеры могут применяться и для поиска скрытых радиомикрофонов.

Особое место для любого хозяйствующего субъекта занимает безопасность автоматизированных информационных систем. Многие отечественные фирмы несут многомиллионные убытки от утечки информации в результате несанкционированного доступа к компьютерным базам данных. От компьютерных преступлений страдают не только отечественные бизнесмены. О размахе этого вида незаконной деятельности можно судить по следующим цифрам: ежегодно потери частных компаний от компьютерных преступлений в США и Западной Европе составляют около 150 млрд. долларов. Согласно расчетам американских экспертов отключение систем защиты от несанкционированного доступа к локальным корпоративным сетям приведет к банкротству 25-30% средних компаний в течение суток, 40-45% средних и 20% крупных фирм разорятся в течение нескольких дней, 30% кредитных организаций лопнут за 2-5 ч, 45% банков перестанут существовать через 2-3 дня.

Специалисты по защите автоматизированных систем выделяют следующие виды угроз информационным объектам:

1) угроза конфиденциальности данных и программ (представляют собой несанкционированный доступ к массивам информации, программам или каналам связи);

2) угроза целостности данных, программ, аппаратуры. Модификация данных - изменение имеющейся информации или добавление лишних записей, например внесение изменений в базы данных по банковским счетам. Модификация программ может привести к несанкционированным действиям программного обеспечения и, как следствие, к уничтожению, модификации или неправильной обработке информационного массива;

3) угроза доступу к данным - несанкционированное блокирование доступа законных пользователей к данным, что может привести к параличу всей информационной системы.

Типичным приемом для атак корпоративных информационных систем является применение различного рода "программ-ловушек". Рассмотрим наиболее распространенные и опасные их типы.

Прежде всего, это "люки" в программах. Под "люком" подразумевается переход в неотраженный в документации режим работы программного продукта, дающий доступ пользователю к дополнительному набору инструментов и функций программы (переход в так называемый "привилегированный режим"). Возникновение люков связано с различными предусмотренными на стадии разработки продукта механизмами, необходимыми для отладки основной программы, и по забывчивости, либо недосмотру не удаленными после завершения тестирования программного продукта. В ряде случаев люки могут умышленно оставлять в программе с целью возможности скрытого доступа уже после реализации продукта. Если программа написана некачественно, и в ней имеются люки, самым простым способом попытаться выявить их является "некорректный ввод". Суть его заключается во вводе ничего не значащей информации ("абракадабры") при каком-либо системном запросе. При возникновении "нештатной" ситуации некачественная программа реагирует нестандартно (ее "глючит"). Таким образом, злоумышленник может воспользоваться этой ситуацией для выполнения каких-либо своих действий, например, попытаться перехватить функции администрирования. Любой программный продукт должен во избежание подобных ситуаций иметь "защиту от дурака" или, иными

словами, от некорректного ввода.

Следующим типом "программ-ловушек" являются так называемые "троянские кони". Уже из самого названия можно догадаться о принципе их действия. Это программы, реализующие, помимо функций, описанных в документации, и некоторые другие функции, о которых пользователь может даже не подозревать. Диапазон этих "других" функций весьма широк. Наибольшую опасность представляют "троянские кони", которые умеют маскировать следы своей деятельности и в течение длительного времени могут "уживаться" с защитными программами. Например, ничего не изменяя в структуре закрытого файла, временно снять защиту, скопировать и переслать его содержимое, после чего защита устанавливается на место - это "скрытые каналы", организующие утечку конфиденциальной информации через компьютерные сети.

Классическим способом мести бывшему работодателю со стороны уволенного программиста являются "логические бомбы". Это отдельная программа или участок кода обычной программы, которая при наступлении определенных заданных условий, например, открытия определенного "нейтрального" файла или при запуске прикладной программы, "взрывается" - удаляет, модифицирует или даже пересылает корпоративные информационные ресурсы.

Компьютерные вирусы отличаются от "логических бомб" только возможностью размножаться и самостоятельно обеспечивать свой запуск.

Чаще всего указанные виды "программ-ловушек" применяются комбинированно, что во много раз усложняет борьбу с ними. С целью обеспечения безопасности информационной системы от потенциальных угроз необходима проработка сценариев действий системы комплексной защиты на разнообразные попытки воздействия на информационные ресурсы. К возможным каналам преднамеренной несанкционированной утечки информации относятся: ЭВМ пользователей, серверы локальных сетей, внешние машинные носители информации - дискеты, лазерные диски, модули памяти (флэш-память) и т.д., внешние линии связи, линии связи между аппаратными средствами, внутренний монтаж аппаратуры.

Многие компании, не гнушающиеся экономическим шпионажем, вместо использования дорогостоящей спецтехники для получения информации прибегают к услугам хакеров. А если такого специалиста удастся внедрить в персонал конкурирующей фирмы, можно рассчитывать, что одним конкурентом стало меньше. Кроме этого существует большое количество и других способов изъятия интересующей информации, хранящейся и обрабатываемой на ЭВМ, через технические каналы утечки. Принцип действия применяемой для этих целей аппаратуры основан на измерении электромагнитного фона, возникающего при работе компьютера. Это довольно сложная, с точки зрения технического исполнения, методика, для применения которой нужны высококвалифицированные специалисты. Она позволяет считывать информацию, выводимую на экран компьютера, работающего в офисе конкурентов. Таким образом, в неприметном фургоне, стоящем по другую сторону улицы в квартале от помещения вашей фирмы (расстояние перехвата превышает один километр), может находиться сотрудник конкурирующей компании с приемным пультом.

Для предотвращения утечки информации через электромагнитные "наводки" помещения, в которых установлены компоненты автоматизированной информационной системы, экранируют - стены, пол и потолок покрываются проволочной сеткой или фольгой, или блоками из специальной пластмассы, окна остекляются специальными стеклами с токопроводящим покрытием (лучше, если в таких помещениях, где происходит обработка особо ценной информации, вообще будут отсутствовать окна, чтобы исключить возможность визуального контроля и применение лазерных микрофонов, считывающих вибрации стекол). Металлические трубы, проходящие через экранируемое помещение (водопроводные, газовые и т.д.), снабжают вставками из диэлектрического материала, которые не позволяют электромагнитным наводкам распространяться за пределы контролируемой зоны.

Генераторы шума эффективны для предотвращения утечки информации с компьютеров через излучение с экранов дисплеев, однако их применение может вызывать у людей, постоянно находящихся в зоне их действия, головные боли, быструю утомляемость и, возможно, более серьезные последствия. Применение генераторов шума может быть оправдано там, где обработка информации осуществляется без участия обслуживающего персонала.

Создание и использование внутрикорпоративных локальных компьютерных сетей, без сомнения, служит более эффективному использованию имеющихся информационных ресурсов - облегчается передача данных между отдельными структурными подразделениями, появляется возможность совместного использования аппаратной базы. Однако уязвимость локальной сети с точки зрения информационной безопасности многократно возрастает по сравнению с совокупностью отдельно работающих ЭВМ - несанкционированный доступ в сеть осуществить проще и незаметнее, чем к отдельному компьютеру. Для защиты информации, циркулирующей в локальной сети, применяются специальные программные средства. Они позволяют осуществлять контроль входа в систему посредством персональной идентификации (пароли и коды), контроль за работой пользователей - путем

составления протоколов по данным в регистрационном журнале, разграничивать доступ к информационным ресурсам.

Большинство специалистов в области защиты информации считают, что задачу контроля доступа надежно решает только применение криптографических средств защиты. Согласно Указу Президента РФ "О мерах по соблюдению законности в области разработки производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации" N 334 от 3 апреля 1995 г., запрещается "использование государственными организациями и предприятиями в информационно-телекоммуникационных системах шифровальных средств, включая криптографические средства обеспечения подлинности информации (электронная подпись), и защищенных технических средств хранения, обработки и передачи информации, не имеющих сертификата Федерального агентства правительственной связи и информации при Президенте Российской Федерации". Таким образом, для того, чтобы осуществлять эксплуатацию шифровальных средств, необходимо получить лицензию ФАПСИ.

6.3. Организационная и правовая составляющие режима коммерческой тайны

Нельзя не отметить, что выбор превентивных мер, необходимых для обеспечения недоступности третьим лицам соответствующих ресурсов информации, составляющей коммерческую тайну, и объединение их в четко работающую систему мер информационной безопасности организации - процесс интеллектуальный и достаточно трудоемкий. Для любой коммерческой компании создание концепции ее внутренней системы защиты информационных ресурсов зависит от следующих факторов:

- 1) финансовые возможности компании;
- 2) объем информации, в отношении которой введен режим коммерческой тайны;
- 3) технические возможности компании;
- 4) наличие филиалов и дочерних структур;
- 5) наличие других хозяйствующих субъектов в данном секторе экономики, в том числе иностранных ("острота" конкуренции);
- 6) номенклатура выпускаемой продукции;
- 7) система внутреннего документооборота.

И здесь возможны, как минимум, три подхода к решению этой проблемы. Первый - создание собственной службы безопасности. Этот вариант приемлем только для достаточно крупных хозяйствующих субъектов - для его осуществления необходимо провести подбор квалифицированных кадров, которые смогли бы осуществлять постоянный мониторинг текущего состояния информационной безопасности фирмы и создать надежную систему контроля за использованием конфиденциальной информации и доступом к ней. Все это требует довольно значительных затрат, которые может позволить себе далеко не каждая фирма, однако в идеале только такой подход может гарантировать максимальную информационную безопасность частного бизнеса.

Второй подход, используемый, в основном, небольшими фирмами и частными предпринимателями, - привлечение сторонних структур, занимающихся предоставлением услуг по обеспечению информационной безопасности. Плюсом такого подхода является возможность широко варьировать спектр защитных мероприятий - от создания комплексной системы защиты конфиденциальной информации до проведения разовых проверок офиса на наличие "закладок" - электронных прослушивающих устройств. Очевидный минус - вы полностью полагаетесь на добросовестность привлекаемой компании. Причем, речь здесь может идти как о частных, так и о государственных структурах. Простейшим примером может служить заключение договора со службой вневедомственной охраны МВД России об установке централизованной сигнализации или организации поста круглосуточной охраны. В особом положении оказываются компании, получившие государственный заказ на разработку или выпуск продукции, имеющей стратегическое значение (например, военной). В этом случае они могут рассчитывать на содействие государственных правоохранительных органов и специализированных служб.

И последний подход - комплексный, сочетающий в себе элементы двух предыдущих, - часть функций по защите возлагается на собственную службу безопасности, часть - на привлекаемую по договору компанию, специализирующуюся на рынке оказания охранных услуг (такой подход приемлем в основном для среднего бизнеса и отдельных крупных предприятий).

При выборе любого подхода в организации службы безопасности необходимо разработать и утвердить пакет внутренних нормативных документов (локальных актов), регламентирующих все аспекты деятельности сотрудников компании при обращении с конфиденциальной информацией независимо от материальных форм ее представления (регламент обеспечения безопасности). Стандартный регламент должен урегулировать такие вопросы, как:

1) организацию подразделения, ответственного за защиту конфиденциальной информации (службы безопасности (СБ) или специально выделенного сотрудника, на которого возложены функции СБ);

2) права, обязанности и функции СБ;

3) определение перечня сведений, составляющих коммерческую тайну, установление категории конфиденциальности информации и работ, порядок изменения категории конфиденциальности работ и информации;

4) регламентация учета, хранения и обращения носителей информации, составляющей коммерческую тайну;

5) порядок допуска сотрудников к носителям конфиденциальной информации;

6) определение обязанностей и ограничений, накладываемых на сотрудников, имеющих доступ к конфиденциальной информации;

7) порядок ведения конфиденциального делопроизводства;

8) порядок проведения служебного расследования по фактам утечки и разглашения конфиденциальной информации;

8) ответственность за нарушения требований регламента безопасности; 10) прочие вопросы организации защиты конфиденциальной информации. Перечень локальных нормативных актов, составляющих регламент обеспечения безопасности (типовой).

1. Инструкция по обеспечению режима конфиденциальности на предприятии.

2. Инструкция по пропускному и внутриобъектному режиму.

3. Требования по разграничению доступа в помещения, где производится обработка и хранение конфиденциальной информации.

4. Требования к лицам, оформляемым на должности, по которым предусмотрен доступ к конфиденциальной информации.

5. Инструкции по обеспечению безопасности при обработке и хранении конфиденциальной информации с использованием средств вычислительной техники (инструкция пользователя, оператора, системного администратора).

6. Инструкция о порядке обслуживания и ремонта элементов автоматизированной системы, используемых для обработки и хранения конфиденциальной информации.

Одной из важнейших задач является организация внутреннего документооборота, который должен включать в себя учет, хранение, использование и уничтожение служебных документов, содержащих конфиденциальную информацию. В инструкцию (положение) о порядке обращения со служебными документами, содержащими коммерческую тайну, рекомендуется включить следующие положения:

1) для обеспечения режима конфиденциальности служебных документов, содержащих сведения, составляющие коммерческую тайну фирмы, на этих документах проставляется ограничительный реквизит - гриф "Коммерческая тайна";

2) все документы с грифом "Коммерческая тайна" имеют режим ограниченного распространения, подлежат регистрации (учету), надлежащему хранению и означают доступ к ним (допуск) на основе разрешений должностных лиц. Учету подлежат бумажные, магнитные и прочие виды материальных носителей конфиденциальной информации;

3) установление грифа конфиденциальности на служебных документах определяется их исполнителями (составителями) и должностным лицом, подписывающим или утверждающим документы;

4) решение вопроса о снятии ограничительных грифов с документа принимает должностное лицо, подписавшее (утвердившее) этот документ. При снятии ограничительного грифа с документа правомочное должностное лицо делает отметку на самом документе путем зачеркивания грифа с проставлением своей подписи и даты;

5) ответственность за обеспечение безопасности информации, составляющей коммерческую тайну, и порядок обращения с документами, содержащими такую информацию, возлагается на руководителей всех структурных подразделений фирмы;

6) контроль за обеспечением режима конфиденциальности сведений, составляющих коммерческую тайну, возлагается на службу безопасности фирмы (отдел информационной безопасности);

7) все поступающие документы с грифом "Коммерческая тайна" принимаются и вскрываются ответственным сотрудником службы безопасности. Поступивший конверт проверяется на целостность. У документа и всех приложений сверяются количество листов и экземпляров. При отсутствии или недостачи документов с грифом "Коммерческая тайна" составляется акт в двух экземплярах, один из которых возвращается отправителю;

8) все документы, содержащие конфиденциальную информацию (входящая корреспонденция,

внутренние распорядительные документы и прочее), подлежат учету и регистрации.

Входящая корреспонденция, содержащая конфиденциальную информацию, регистрируется в "Журнале регистрации входящей корреспонденции ограниченного пользования"; внутренние документы, содержащие КИ, регистрируются в зависимости от вида документа: в "Журнале регистрации приказов", "Журнале регистрации распоряжений" и так далее, в которых проставляется отметка о конфиденциальности.

Все листы журналов, учитывающих конфиденциальные документы, нумеруются, прошиваются и опечатываются. В конце журнала в заверительном листе указывается общее количество листов прописью, ставится подпись ответственного лица, которая скрепляется печатью.

В журналах регистрации документов ограниченного пользования документу присваивается учетный номер. Каждое приложение к основному документу имеет свой учетный номер. Каждому экземпляру документа присваивается номер, количество экземпляров соответствует количеству направленных копий документа в адрес лиц, указанных в списке рассылки. Экземпляр документа, хранящийся в службе безопасности фирмы, имеет номер 1.

Конфиденциальные входящие и внутренние документы формируются в отдельные дела, дела хранятся в сейфе.

Выдача документа с грифом "Коммерческая тайна" производится на основании служебной записки с разрешающей визой начальника структурного подразделения компании и начальника службы безопасности. Выдача и возврат документов отражаются в "Журнале учета выдачи документов ограниченного пользования". Работник, получивший документ с грифом "Коммерческая тайна", должен сверить учетный номер полученного документа с номером в журнале, проверить количество листов и поставить в журнале свою подпись. Выданные для работы документы подлежат возврату в тот же день. При возврате документа ответственный работник службы безопасности сверяет номер документа по журналу, проверяет количество листов документа и в присутствии работника ставит в графе "Отметка о возврате" свою подпись и дату возврата документа.

Копирование документа с грифом "Коммерческая тайна" производится на основании наряда на размножение с разрешающей визой начальника структурного подразделения компании и начальника службы безопасности. Все копии документов берутся на учет в специальном журнале. Все бракованные копии документа подлежат немедленному уничтожению с составлением акта. Множительная техника для копирования документов конфиденциального характера должна быть оборудована счетчиком снятых копий. По окончании рабочего дня специально выделенный сотрудник службы безопасности сверяет количество снятых копий по счетчику сданными журнала размноженных документов и актами на уничтожение бракованных копий, после чего расписывается в журнале с отметкой о соответствии количества размноженных документов учетным формам;

9) документы с грифом "Коммерческая тайна", не подлежащие брошюрованию в дела, берутся на инвентарный учет с проставлением инвентарного номера и даты регистрации;

10) пересылка (отправка) документов с ограничительным грифом осуществляется по предписанию должностных лиц, которым даны на это соответствующие полномочия. Документы с грифом "Коммерческая тайна" пересылаются (отправляются) ценной заказной корреспонденцией или нарочным в двойных конвертах. Гриф "Коммерческая тайна" на внешнем конверте (пакете) не проставляется;

11) уничтожение документов с грифом "Коммерческая тайна", утративших свое практическое значение и ценность для фирмы, производится по акту лицом, ведущим данное делопроизводство, в присутствии не менее чем одного сотрудника отдела информационной безопасности (службы безопасности), по согласованию с руководителем структурного подразделения и начальником службы безопасности в соответствии со сроками и порядком, определенными номенклатурой дел, и с внесением отметок в журналах учета;

12) уничтожение документов с грифом "Коммерческая тайна" производится путем их сожжения, измельчения или другим путем, исключающим восстановление текста документа;

13) проверка наличия документов с ограничительным грифом проводится не реже одного раз в год комиссией, назначенной приказом руководителя фирмы. В состав комиссии включаются работники, ответственные за учет и хранение вышеназванных документов и имеющие допуск к ним. Результаты проверки оформляются актами. Акты подписываются членами комиссии и утверждаются руководителем фирмы;

14) при смене (увольнении, переводе на другую работу) сотрудников фирмы, ответственных за учет и регистрацию документов с ограничительным грифом, передача делопроизводства производится по акту приема-передачи, утверждаемому руководителем фирмы;

15) документы, в том числе и машинные носители, с грифом "Коммерческая тайна" в нерабочее время должны храниться в запираемых и опечатываемых металлических шкафах. Хранение в других хранилищах допускается по разрешению руководителя службы безопасности при наличии условий,

обеспечивающих их сохранность.

6.4. Служба безопасности в коммерческой организации

Одно из центральных мест в организации защиты информации, составляющей коммерческую тайну, а следовательно, и в обеспечении экономической безопасности крупных и средних коммерческих компаний занимает создание службы безопасности. Основными задачами службы безопасности являются обеспечение охраны предприятия, производства, продукции и защита коммерческой информации. Рассмотрим основные принципы ее функционирования. Служба безопасности является отдельным структурным подразделением и, как правило, находится в прямом подчинении руководителя компании. Его исключительной прерогативой является также назначение и освобождение от должности начальника службы безопасности и его заместителей. Правовой статус службы безопасности, задачи, функции, структура, права и обязанности сотрудников должны быть закреплены в Положении о службе безопасности.

Вопрос подбора персонала службы должен определяться, исходя из особенностей осуществляемого компанией вида производственно-коммерческой деятельности. Даже неспециалисту ясно, что составы службы безопасности банка и сети обувных магазинов будут существенно отличаться. Вообще, действует общий принцип - чем более "научным" видом деятельности занимается компания, тем больше специалистов инженерно-технического профиля должно входить в штат службы. Это и понятно - повышается значение функции по обеспечению информационной безопасности.

К числу основных функций по обеспечению информационной безопасности независимо от сферы деятельности компании можно отнести следующие:

- 1) анализ целесообразности отнесения той или иной информации, касающейся деятельности фирмы, к категории конфиденциальной. На основе такого анализа разрабатывается перечень сведений, составляющих коммерческую тайну. Анализ проводится систематически с целью своевременного реагирования на происходящие изменения;
- 2) подготовка перечня должностей работников фирмы, которые при исполнении своих служебных обязанностей имеют право знакомиться с определенными сведениями, составляющими коммерческую тайну. Установление процедур допуска к конфиденциальным сведениям;
- 3) разработка порядка обращения с носителями конфиденциальной информации (технологии создания, учет, правила работы, хранение, пересылка, транспортировка, размножение, уничтожение);
- 4) составление перечня помещений, выделенных для проведения работ, а также постоянного или временного хранения носителей информации, составляющей коммерческую тайну. Выработка требований, предъявляемых к оборудованию таких помещений, и проверка их пригодности. Определение порядка доступа в эти помещения;
- 5) осуществление профилактических технических мероприятий с целью недопущения утечки закрытой информации по техническим каналам;
- 6) разработка порядка и контроль за проведением закрытых совещаний и переговоров;
- 7) осуществление пропускного и внутриобъектного режимов (разграничение доступа в помещения);
- 8) правовой анализ подготавливаемых локальных нормативных актов, договоров с контрагентами на предмет их соответствия требованиям регламента обеспечения безопасности;
- 9) установка технических средств охраны, обеспечение их бесперебойного функционирования;
- 10) систематический контроль выполнения режимных требований;
- 11) проведение служебных расследований по фактам утечки конфиденциальной информации.

Для осуществления своих функций службе безопасности должны быть предоставлены следующие права:

- 1) давать сотрудникам и руководителям структурных подразделений обязательные для исполнения рекомендации по вопросам обеспечения информационной безопасности; проводить их обучение и инструктаж;
- 2) контролировать состояние и надежность режима коммерческой тайны;
- 3) выходить с ходатайством о внесении изменений и дополнений в локальные нормативные акты в рамках своей компетенции;
- 4) проводить расследование фактов утечки информации, составляющей коммерческую тайну, нарушений требований регламента обеспечения безопасности. Ходатайствовать перед руководством об отстранении и привлечении к ответственности виновных лиц;
- 5) ходатайствовать о поощрении сотрудников компании, активно участвующих в работе по предупреждению разглашения конфиденциальной информации.

В качестве примера осуществления одной из своих обычных функций рассмотрим типовую схему

действий службы безопасности при подготовке и проведении закрытых совещаний и переговоров.

На начальном этапе руководством компании определяется предмет переговоров или вопросы, которые необходимо обсудить на совещании, а также участники этого мероприятия. Кроме того, выбирается наиболее удобное время проведения, после чего информация о месте, времени и приглашенных лицах поступает начальнику службы безопасности. С этого момента начинается этап непосредственного планирования мероприятий по обеспечению конфиденциальности переговоров или совещания. Разрабатывается пошаговый план, который должен включать в себя такие пункты, как:

- 1) предварительная проверка помещений, в которых будут происходить переговоры или совещание, на предмет наличия подслушивающей аппаратуры, в отдельных случаях, для проведения особо важных переговоров помещение должно быть оборудовано экранами и генератором шума;
- 2) встреча прибывающих лиц (следует обратить внимание на то, что приглашенных лиц могут сопровождать сотрудники их службы безопасности или телохранители, поэтому необходимо заранее скоординировать степень их участия и полномочия во избежание недоразумений с "коллегами", кроме того, следует заранее проконсультироваться с руководством о возможности проноса гостями аудио- или видеоаппаратуры, сотовых телефонов, пейджеров и носимых радиостанций);
- 3) с целью недопущения провокаций и других возможных инцидентов необходимо предусмотреть охрану и контроль за оставленной одеждой, вещами и машинами приглашенных;
- 4) при наличии предварительной информации о неприязненных отношениях между кем-либо из приглашенных (особенно, при наличии у них собственной охраны) необходимо быть готовыми к предупреждению и локализации возможных конфликтов;
- 5) выявление лиц, не включенных в список приглашенных, находящихся на мероприятии или в смежных помещениях, а также всех подозрительных лиц.

В плане за каждым пунктом должен быть закреплен ответственный за его выполнение сотрудник. Кроме того, разрабатывается общая схема дислокации сотрудников службы безопасности и привлеченных специалистов. На стадии непосредственного проведения мероприятий каждый задействованный сотрудник должен действовать точно в соответствии с разработанным планом. В ходе рабочего этапа сотрудники службы безопасности (охранного предприятия) должны точно выполнять свои обязанности, оговоренные на стадии подготовки. При этом особо следует отслеживать следующие моменты: опоздавшие участники мероприятия должны подвергаться такому же тщательному осмотру, как и все остальные (возможно, они специально задержались в надежде, что после начала совещания пропускной режим будет ослаблен, и под видом спешки удастся пронести запрещенные предметы или провести лицо, не включенное в список приглашенных).

Необходимо учитывать, что стопроцентной гарантии отсутствия радиозакладок в помещении, где проходит совещание или переговоры, а так же в смежных помещениях не может дать даже самая тщательная проверка. Поэтому нужно максимально расширить область контролируемой зоны вокруг места проведения мероприятия, в идеале - до границ зоны досягаемости действия приемной аппаратуры. Лучше, конечно, подобрать помещение без окон, но если это невозможно, сотрудники службы безопасности должны заранее позаботиться, чтобы под окнами не было припаркованных автомобилей (если здание, где происходят переговоры или совещание, находится в городе рядом с оживленной дорогой, в опасной близости заблаговременно "паркуют" свои автомобили с таким расчетом, чтобы "чужак" не смог оставить машину в опасной зоне). После окончания мероприятия снова осуществляется зачистка помещений, в которые имели доступ приглашенные. Проверяются сувениры и подарки от гостей - современная техника позволяет установить закладку даже в достаточно мелкие предметы. Целесообразно проанализировать ход всей операции с целью выявления возможных недочетов в планировании и действиях сотрудников службы безопасности.

Если у небольшой фирмы нет возможности обеспечить безопасность ведения конфиденциальных переговоров в офисе, некоторые предприниматели предпочитают для таких целей использовать рестораны или другие подобные заведения. Бытует мнение, что музыка и общий гвалт голосов служат надежной защитой от использования направленных микрофонов и других видов прослушивающих устройств. Однако для современного оборудования живой оркестр не помеха, а статичное положение очень облегчает задачу любопытствующей стороне. Гораздо целесообразней использовать для этой цели автомобиль. Какое именно транспортное средство будет использовано для этой цели, должен знать очень узкий круг людей. Перед началом сотрудниками службы безопасности также проводится зачистка автомобиля для защиты от закладок. Переговоры можно начинать только после начала движения автомобиля. Следует придерживаться правила - при вынужденных остановках (светофор, наличие помехи и т.д.) вопросы конфиденциального характера обсуждаться не должны. Естественно, окна в автомобиле на всем протяжении операции должны быть плотно закрыты.

На одном примере организации закрытых переговоров видно, сколько задач приходится решать службе безопасности для предотвращения возможных утечек информации. Естественно, все это требует значительных затрат, но если не позаботиться об информационной безопасности бизнеса,

потери будут несравнимо больше.

6.5. Обязательные меры по охране коммерческой тайны

Все меры, подпадающие под понятие режима коммерческой тайны, можно условно разделить на обязательные, которые обладатель информации должен предпринимать для охраны ее конфиденциальности в силу требования законодательных актов, и произвольные - они осуществляются по собственной инициативе обладателя.

Единственное условие, накладываемое на них, - они не должны противоречить законодательству Российской Федерации.

Остановимся сначала на том минимальном наборе требований, который установлен в Законе "О коммерческой тайне". Некоторую неясность по данному вопросу вносит структура данного закона: в статье 10 "Охрана конфиденциальности информации" устанавливается перечень мер, которые должен принять в отношении информации, составляющей коммерческую тайну, ее обладатель. В этой статье под понятием "обладатель" понимается "лицо, которое владеет информацией, составляющей коммерческую тайну на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны" (п. 4 ст. 3 Закона "О коммерческой тайне"), то есть в широком смысле слова. В статьях 11-13 Закона устанавливаются перечни мер, которые должны принять в отношении информации уже конкретные обладатели - работодатели, контрагенты (согласно п. 7 ст. 3 указанного закона, контрагент - сторона гражданско-правового договора, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию) и органы государственной власти, иные государственные органы, органы местного самоуправления (в лице должностных лиц, государственных или муниципальных служащих указанных органов).

Из-за несовершенной юридической техники трудно четко ответить на вопрос о том, являются ли обязательные меры, установленные статьей 10 Закона "О коммерческой тайне" для обезличенного обладателя, обязательными для отдельных категорий обладателей (ст. 11-13). Ясно, что органы государственной власти, которым информация, составляющая коммерческую тайну, была предоставлена ее обладателем в целях выполнения их функций, не должны сами определять, является ли поступившая информация конфиденциальной (это право ее "основного" обладателя), как того требует пункт 1 части 1 статьи 10 Закона.

Итак, часть 1 статьи 10 содержит следующие пять обязательных мероприятий:

- 1) определение перечня информации, составляющей коммерческую тайну;
- 2) ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;
- 3) учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;
- 4) регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;
- 5) нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа "Коммерческая тайна" с указанием обладателя этой информации (для юридических лиц - полное наименование и место нахождения, для индивидуальных предпринимателей - фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

Интересным с практической точки зрения является вопрос: в случае разглашения информации, составляющей коммерческую тайну, может ли ее обладатель рассчитывать на гражданско-правовые способы защиты своего нарушенного права, если им были приняты не все установленные Законом "О коммерческой тайне" обязательные меры по охране конфиденциальности информации?

Для того, чтобы уяснить суть проблемы, обратимся к части 5 статьи 10 Закона, которая гласит, что меры по охране конфиденциальности информации признаются разумно достаточными, если:

- 1) исключается доступ к информации, составляющей коммерческую тайну, любых лиц без согласия ее обладателя;
- 2) обеспечивается возможность использования информации, составляющей коммерческую тайну, работниками и передачи ее контрагентам без нарушения режима коммерческой тайны.

Таким образом, меры должны удовлетворять условию "разумной достаточности". Сам по себе принцип "разумной достаточности", вытекающий из общих положений гражданского права, мог бы служить критерием, при определении, насколько полно обладатель информации, составляющей коммерческую тайну, позаботился об охране ее конфиденциальности. Однако толкование этого принципа в части 5 статьи 10, приведенное выше, никак нельзя назвать удачным. На его основании

("меры по охране конфиденциальности информации признаются разумно достаточными, если исключается доступ к информации, составляющей коммерческую тайну, любых лиц без согласия ее обладателя") можно сделать абсурдный вывод, что, если профессиональному "экономическому шпиону" несмотря на все предпринятые меры по защите удалось все же заполучить информацию, получается, что принятые меры должны быть признаны недостаточными.

Таким образом, трудно однозначно ответить на поставленный вопрос. Думаю, что даже если судом будет признано, что принятые обладателем коммерческой тайны меры не удовлетворяют принципу "разумной достаточности", он все же может рассчитывать на гражданско-правовые способы защиты своего нарушенного права. Но в этом случае при определении размера ответственности должны применяться принципы, относящиеся к "смешанной" вине: для договорных отношений - статья 404 Гражданского кодекса РФ, для бездоговорных отношений - статья 1083 Гражданского кодекса РФ*(14). Лицо, допустившее разглашение коммерческой тайны или использовавшее ее в своих интересах, если оно докажет отсутствие своей вины, должно быть по решению суда освобождено от ответственности (на основании ст. 401 Гражданского кодекса РФ в рамках договора, ст. 1064 Гражданского кодекса РФ при внедоговорных отношениях сторон).

Здесь мы более подробно рассмотрим некоторые из тех мер по защите конфиденциальности информации, которые законодатель отнес к обязательным для всех ее обладателей. Согласно статье 10 Закона "О коммерческой тайне", первое, что должен сделать обладатель информации, составляющей коммерческую тайну, - это определить перечень данной информации. Зачастую руководители частных компаний не вполне четко представляют себе, какие объективные данные об их бизнесе должны входить в такой перечень.

Отнесение информации к категории коммерческой тайны компании должно основываться на принципе экономической обоснованности и своевременности. При этом, обязательно надо учитывать, что затраты на обеспечение информационной безопасности должны быть меньше в сравнении с возможными экономическими потерями от утечки конфиденциальной информации. Задача эта не так проста, как может показаться на первый взгляд. Здесь не применим принцип: "лучше перебдеть, чем недобдеть".

Чрезмерная секретность может обернуться потерей прибылей, так как рыночные отношения для достижения успеха требуют широкой рекламы выпускаемой продукции. При излишнем засекречивании рост расходов на эти цели неадекватен снижению вероятности утечки конфиденциальных сведений. Наоборот, чрезмерная открытость неизбежно приведет к таким же отрицательным последствиям, так как рынок - это всегда конкуренция. Экономически целесообразно обеспечивать защиту только той части информации о деятельности фирмы, которая гарантирует расширение рынков сбыта продукции, улучшение ее качества, заключение выгодных контрактов с партнерами по бизнесу.

При составлении перечня сведений, составляющих коммерческую тайну, следует принимать во внимание и то, какая именно информация вызывает повышенный интерес со стороны конкурентов. По мнению специалистов, частные компании в наибольшей степени заинтересованы в получении сведений о конкурирующих фирмах по таким вопросам:

- 1) финансовые отчеты и прогнозы;
- 2) перспективные планы развития производства;
- 3) финансовое положение компании;
- 4) используемые "ноу-хау";
- 5) маркетинг и стратегия ценообразования;
- 6) условия заключаемых сделок (в ряде случаев сам факт заключения);
- 7) структура системы безопасности;
- 8) информация о рационализаторском предложении, изобретении и так далее, находящемся на стадии разработки;
- 9) возможность доступа к информационным ресурсам.

Кроме всего вышеперечисленного, к закрытой информации целесообразно отнести такие сведения, как номера домашних телефонов, адреса руководителей и сотрудников фирмы, информация о различных конфликтных ситуациях и тому подобное.

Регламентированный перечень сведений, относимых к коммерческой тайне предприятия, следует регулярно пересматривать в зависимости от изменения направлений и результатов его научно-исследовательских и опытно-конструкторских работ, выбранной рыночной стратегии, заключенных договоров.

Учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана, - еще одно мероприятие, необходимое для обеспечения конфиденциальности информации. Обычно информация проходит несколько ступеней "фильтрации". Круг пользователей соответствующих категорий информации сужается на каждом "уровне сложности", ограничиваясь, в конце концов, учредителями организации (например, информация о

долгосрочных планах деятельности не всегда доводится даже до сведения руководителя, не входящего в состав учредителей). Это связано с тем, что персонал - один из главных каналов утечки информации, составляющей коммерческую тайну.

Повышенную угрозу экономической безопасности компании потенциально представляют, прежде всего, три категории сотрудников. Во-первых, это сотрудники, которые подрабатывают по совместительству в других фирмах. Во-вторых, это вновь нанятые на службу работники. И, в-третьих, те, кто подлежит увольнению. Эти категории сотрудников наименее надежны в морально-психологическом отношении и требуют повышенного внимания со стороны службы безопасности и руководства компании.

Включение в трудовые и гражданско-правовые договоры, заключаемые работодателем конфиденциальной информации, положений, регулирующих условия об обеспечении конфиденциальности, обязательства о неразглашении, порядок использования информации в период действия договора и после его прекращения, также являются, согласно статье 10 Закона "О коммерческой тайне", обязательными мерами по защите коммерческой тайны. Отношения, возникающие между работодателем, обладателем конфиденциальной информации, и работниками, в силу своих должностных обязанностей имеющими доступ к ней, характеризуются целым комплексом взаимных прав и обязанностей. Однако некоторые моменты, имеющие принципиальное значение, остаются неохваченными.

Например, в некоторых зарубежных странах существует практика заключения с работником соглашения, по которому ему после увольнения в течение определенного срока (по истечении которого, как предполагается, конфиденциальная информация потеряет свою потенциальную ценность) запрещено поступать на работу в конкурирующие компании. В течение срока действия ограничения бывший сотрудник может получать денежную компенсацию. Это, конечно, в определенной степени защищает интересы владельцев компаний, но ставит в очень невыгодные условия высококвалифицированных узких специалистов. В нашей стране такие соглашения пока неизвестны. Комплекс отношений между работодателями и работниками в аспекте сохранения информации, составляющей коммерческую тайну, и ответственность за ее разглашение, мы рассмотрим в [главе 8](#).

Глава 7. Ответственность за нарушение права на коммерческую тайну

7.1. Понятие, виды и условия ответственности

В этой [главе](#) мы рассмотрим гражданско-правовые способы защиты интересов обладателей информации, составляющей коммерческую тайну, меры административной и уголовной ответственности за преступления, связанные с ее разглашением и несанкционированным использованием. Ответственность работников, незаконно разгласивших или использовавших конфиденциальную информацию работодателя, имеет ряд принципиальных особенностей, поэтому более подробно мы остановимся на ней в следующей [главе](#).

Ответственности за нарушение положений Закона "О коммерческой тайне" посвящена статья 14 указанного Закона. Согласно этой статье за нарушение права на коммерческую тайну лицо, совершившее противоправное деяние, может быть привлечено к дисциплинарной, гражданско-правовой, административной или уголовной ответственности. Следует обратить внимание, что по отношению к юридическим лицам можно говорить только о гражданско-правовой ответственности.

Говоря о возникновении и пределах ответственности за нарушение права на коммерческую тайну, различают четыре ситуации:

- 1) лицо получило доступ к информации, составляющей коммерческую тайну, в качестве контрагента по гражданско-правовому договору;
- 2) лицо (работник) получило доступ к информации, составляющей коммерческую тайну, работодателем которой является работодатель, в рамках заключенного трудового договора;
- 3) должностное лицо органа государственной власти, иного государственного органа, органа местного самоуправления получило доступ к информации, составляющей коммерческую тайну, поступившую от ее обладателя в порядке статьи 6 Закона "О коммерческой тайне";
- 4) лицо получило доступ к информации, составляющей коммерческую тайну, в результате своих противоправных действий.

Во всех вышеперечисленных случаях нарушение права законного обладателя на коммерческую тайну выражается в ее разглашении третьим лицам или в использовании конфиденциальной информации в личных целях.

Основной формой защиты права на коммерческую тайну является юрисдикционная процедура, суть которой состоит в обращении обладателя конфиденциальной информации, права и законные

интересы которого нарушены, за помощью к компетентным государственным органам. Выделяют два вида юрисдикционной процедуры - рассмотрение дела в судебном и административном порядке.

Наиболее важное значение имеет судебный порядок защиты нарушенных прав, который предполагает обращение в суд. Так как в качестве обладателей информации, составляющей коммерческую тайну, могут выступать только юридические лица и частные предприниматели, большинство обращений относится к компетенции арбитражных судов. Арбитражным судам подведомственны и разбирательства с участием органов государственной власти, иных государственных органов и органов местного самоуправления. Суды общей юрисдикции рассматривают иски работодателей к работникам, нарушившим режим коммерческой тайны в рамках трудовых отношений.

Административный порядок защиты права на коммерческую тайну применяется гораздо реже. Это связано с тем, что, во-первых, его применение возможно лишь в случаях специально предусмотренных в законе. А, во-вторых, любое решение, принятое в административном порядке, может быть обжаловано в суд. В качестве примера можно привести Закон РСФСР "О конкуренции и ограничении монополистической деятельности на товарных рынках", который предусматривает возможность обращения с заявлением о допущенном нарушении права на коммерческую тайну в федеральный антимонопольный орган, который наделен правом выносить обязательные для исполнения предписания об устранении нарушений и применять к правонарушителю установленные законом санкции.

Следует особо подчеркнуть, что ответственность за разглашение и незаконное использование информации, составляющей коммерческую тайну, может быть возложена на правонарушителя только при соблюдении требований, предъявляемых статьей 139 Гражданского кодекса РФ к информации подобного рода:

- 1) реальная или потенциальная коммерческая ценность в силу неизвестности такой информации третьим лицам;
- 2) отсутствие свободного доступа к закрытой информации для третьих лиц на законном основании;
- 3) обладатель информации принимает превентивные меры, препятствующие общему доступу к этой информации.

Таким образом, закон возлагает бремя доказывания наличия вышеперечисленных признаков коммерческой тайны на обладателя информации, обратившегося к уполномоченным государственным органам для защиты своих прав, поэтому необходимо четкое выполнение всех формальностей (таких как разработка и утверждение локального перечня сведений, отнесенных к коммерческой тайне, нанесение соответствующего грифа на материальные носители "секретной" информации и так далее).

В связи с тем, что при попытке привлечь кого-либо к юридической ответственности за нарушение прав на коммерческую тайну рассмотрение в судах гражданско-правовых споров и уголовных дел связано с необходимостью раскрытия конфиденциальной информации компетентным государственным органам, процессуальное законодательство предусматривает особый порядок судопроизводства для таких случаев. Согласно части 2 статьи 11 Арбитражного процессуального кодекса РФ, разбирательство дела в закрытом судебном заседании допускается в случаях, если открытое разбирательство дела может привести к разглашению государственной тайны, в иных случаях, предусмотренных федеральным законом, а также при удовлетворении ходатайства лица, участвующего в деле и ссылающегося на необходимость сохранения коммерческой, служебной или иной охраняемой законом тайны. Аналогичное положение содержит и Гражданский процессуальный кодекс РФ: "Разбирательство в закрытых судебных заседаниях допускается и при удовлетворении ходатайства лица, участвующего в деле и ссылающегося на необходимость сохранения коммерческой или иной охраняемой законом тайны, неприкосновенность частной жизни граждан или иные обстоятельства, гласное обсуждение которых способно помешать правильному разбирательству дела либо повлечь за собой разглашение указанных тайн или нарушение прав и законных интересов гражданина" (ч. 2 ст. 10 ГПК РФ).

7.2. Гражданско-правовая ответственность за нарушение права на коммерческую тайну

Гражданско-правовые меры ответственности за нарушение права на коммерческую тайну имеют, пожалуй, наиболее важное значение, так как они в отличие от остальных видов ответственности, предусмотренных законом, носят не только превентивный (сдерживающий), но и восстановительный характер. Иными словами, их главное значение состоит в том, чтобы лицо, права и законные интересы которого нарушены, имело возможность компенсировать свои материальные потери.

Статья 139 Гражданского кодекса содержит прямое указание только на один из гражданско-правовых способов защиты права на коммерческую тайну, а именно на возмещение причиненных

убытков, но допускает возможность применения и других способов защиты, предусмотренных Гражданским кодексом РФ и иными правовыми актами. Общий, хотя и не исчерпывающий, перечень этих способов содержится в статье 12 Гражданского кодекса. Следует учитывать, что правовая природа нарушенного права и способ нарушения накладывают определенные ограничения на их применение - не все они могут быть использованы в сфере обеспечения защиты коммерческой тайны от неправомерных посягательств.

Если нарушением права на коммерческую тайну ее обладателю причинены убытки, лицо, совершившее противоправное деяние, должно эти убытки возместить. Это требование, в соответствии со статьей 16 Гражданского кодекса РФ, распространяется и на должностных лиц органов государственной власти или местного самоуправления, в результате действий (бездействия) которых были нарушены законные права и интересы обладателя коммерческой тайны. Противоправные действия третьих лиц могут выражаться в незаконном получении информации, составляющей коммерческую тайну, ее разглашении или использовании без законных оснований. Напомним, что коммерческая тайна считается полученной незаконно, если получение было осуществлено с умышленным преодолением принятых обладателем коммерческой тайны мер по защите ее конфиденциальности, а также если получившее информацию лицо знало (или должно было при данных обстоятельствах знать), что полученные сведения составляют коммерческую тайну, обладателем которой является другое лицо, и что осуществляющее передачу информации лицо не имеет на это законных оснований.

Согласно части 2 статьи 15 Гражданского кодекса РФ под убытками понимаются расходы, которые лицо, чье право нарушено, произвело или должно будет произвести для восстановления нарушенного права, утрата и повреждение его имущества (реальный ущерб), а также неполученные доходы, которые это лицо получило бы при обычных условиях гражданского оборота, если бы его право не было нарушено (упущенная выгода). Таким образом, закон предусматривает возмещение убытков в полном объеме (за исключением ситуаций, когда в качестве виновного лица выступает работник обладателя коммерческой тайны) - компенсации подлежит как реальный ущерб в имуществе потерпевшего, так и упущенная им выгода. Как показывает практика, отрицательные имущественные последствия от разглашения или использования "секрета фирмы" третьими лицами за очень редким исключением выражаются именно в упущенной выгоде (чаще всего это утрата обладателем коммерческой тайны определенных преимуществ перед конкурентами), а не в реальном ущербе. Необходимо также обратить внимание, что применение данного способа защиты права на коммерческую тайну на практике во многом усложняется тем, что потерпевший должен доказать как наличие убытков, так и их размер. Проще всего это сделать, когда правонарушитель незаконно использовал чужой "секрет" для извлечения доходов - в этом случае, на основании пункта 2 статьи 15 Гражданского кодекса РФ, обладатель коммерческой тайны вправе потребовать возмещения наряду с другими убытками упущенной выгоды в размере не меньшем, чем такие доходы.

Если обладатель информации, составляющей коммерческую тайну, вводит ее в гражданский оборот посредством заключения договоров с контрагентами, с учетом вышесказанного есть смысл предусмотреть в договоре условие, согласно которому сторона, получившая конфиденциальную информацию и разгласившая ее, обязана выплатить неустойку в виде штрафа. Штраф определяется в виде фиксированной суммы и получает четкое закрепление в договоре. В этом случае потерпевшей стороне не придется доказывать причинение убытков недобросовестным контрагентом. Согласно статье 330 Гражданского кодекса РФ по требованию об уплате неустойки кредитор не обязан доказывать причинение убытков. Таким образом, с точки зрения практического применения указанный способ гражданско-правовой защиты является более предпочтительным по сравнению с возмещением убытков в полном объеме.

В соответствии со статьей 394 Гражданского кодекса РФ по общему правилу - если за неисполнение или ненадлежащее исполнение договора установлена неустойка, то убытки возмещаются в части, не покрытой неустойкой. В договоре, однако, это правило может быть изменено. Ответственность контрагента может выражаться:

- 1) во взыскании только неустойки, но не убытков;
- 2) во взыскании убытков в полной сумме сверх неустойки;
- 3) во взыскании по выбору кредитора либо неустойки, либо убытков.

Защита интересов обладателя информации может быть осуществлена и другими гражданско-правовыми способами. Выбор того или иного способа зависит от конкретной ситуации. К примеру, иск о признании права на коммерческую тайну может быть подан тогда, когда данное право кем-либо оспаривается. Этот же способ защиты используется и в том случае, когда от обладателя информации, составляющей коммерческую тайну, без установленных законом оснований кто-либо требует ее предоставления. Например, если государственный орган необоснованно относит определенную информацию к одной из категорий, которые в соответствии со статьей 5 Закона "О коммерческой тайне"

не могут составлять коммерческую тайну.

В том случае, когда совершенное правонарушение еще не привело к утрате обладателем информации, составляющей коммерческую тайну, фактической монополии на нее, защита его интересов возможна путем восстановления положения, существовавшего до нарушения, и пресечения действий, нарушающих интересы обладателя информации или создающих угрозу их нарушения. В качестве примера можно привести такую ситуацию. Лицо незаконными методами завладело информацией, однако своевременно было разоблачено и еще не успело воспользоваться чужим секретом или разгласить его. В этом случае на него может быть возложена обязанность по возврату или уничтожению материальных носителей информации, ему может быть запрещено использовать данную информацию самостоятельно, а также передавать информацию третьим лицам.

7.3. Административная ответственность за нарушение права на коммерческую тайну

Ответственность за административные правонарушения в области информации установлена статьями 13.11-13.23 Кодекса РФ об административных правонарушениях. Кратко остановимся на тех из них, которые устанавливают ответственность за правонарушения, тем или иным образом нарушающие право обладателя на коммерческую тайну.

Прежде всего, это касается статьи 13.14 Кодекса РФ об административных правонарушениях, которая устанавливает ответственность за разглашение информации с ограниченным доступом. Перечень таких видов информации утвержден Указом Президента РФ от 6 марта 1997 г. N 188 и включает в себя, в частности, "сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом и федеральными законами (коммерческая тайна)". К информации с ограниченным доступом относятся также персональные данные работника, под которыми понимаются информация, необходимую работодателю в связи с трудовыми отношениями и касающуюся конкретного работника. Согласно статье 88 Трудового кодекса РФ работодатель не вправе сообщать персональные данные работника третьим лицам без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом, и сообщать персональные данные работника в коммерческих целях без его письменного согласия. Таким образом, разглашение информации, составляющей коммерческую тайну, а также персональных данных работника квалифицируется по статье 13.14 Кодекса РФ об административных правонарушениях. Кроме того, по указанной статье будут квалифицироваться и правонарушения, связанные с разглашением профессиональной и служебной тайны.

Субъектами данного административного правонарушения могут выступать граждане или должностные лица, получившие доступ к указанной информации в связи с исполнением служебных или профессиональных обязанностей, допустившие ее разглашение, то есть распространение в устной или иной форме сведений, относимых к такой информации, когда они стали достоянием других лиц.

Что же грозит правонарушителю, разгласившему коммерческую тайну? Кодекс РФ об административных правонарушениях устанавливает санкцию в виде административного штрафа в размере от пяти до десяти минимальных размеров оплаты труда для граждан. Для должностных лиц предусмотрена повышенная ответственность. Для них размер административного штрафа составляет от сорока до пятидесяти минимальных размеров оплаты труда. Необходимо отметить, что лицо может быть привлечено к административной ответственности по статье 13.14 Кодекса РФ об административных правонарушениях только в том случае, если разглашение информации, составляющей коммерческую тайну, не образует состава преступления, предусмотренного статьей 183 Уголовного кодекса РФ, и не влечет уголовную ответственность. Определяющим фактором здесь выступает степень общественной опасности деяния и причинение тяжких последствий. За одно и то же деяние лицо не может быть привлечено к административной и уголовной ответственности (в отличие от мер гражданско-правовой защиты, которые могут сочетаться с другими видами ответственности или применяться самостоятельно).

Дела об административных правонарушениях, предусмотренных статьей 13.14 Кодекса РФ об административных правонарушениях, рассматриваются судьями. Под рассмотрением дела понимаются процессуальные действия, осуществляемые после составления протокола об административном правонарушении и предшествующие вынесению постановления (решения) о назначении административного наказания. Дела о правонарушениях, производство по которым осуществляется в форме административного расследования, рассматриваются судьями районных судов, а в случаях, не требующих проведения административного расследования, - мировыми судьями. В соответствии со статьей 29.6 Кодекса РФ об административных правонарушениях дело об административном правонарушении рассматривается в пятнадцатидневный срок со дня получения судьей, органом,

должностным лицом, правомочным рассматривать дело, протокола об административном правонарушении и других материалов дела.

Следующий состав правонарушения предусмотрен статьей 13.12 Кодекса РФ об административных правонарушениях, которая предусматривает ответственность за нарушение правил защиты информации. Согласно пункту 1 статьи 21 Федерального закона "Об информации, информатизации и защите информации" защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу. Под названную категорию попадают и сведения, составляющие коммерческую тайну. Ясно, что если система защиты информации в каком-либо государственном органе не соответствует установленным нормативам, это может привести к нарушению права на коммерческую тайну лица, предоставившего свои секреты уполномоченному органу в порядке статьи 6 Закона "О коммерческой тайне". Права и обязанности юридических, физических лиц в области защиты информации, а также защита права на доступ к информации определены соответственно статьями 22 и 24 Федерального закона "Об информации, информатизации и защите информации". В соответствии со статьей 19 указанного закона информационные системы, базы и банки данных, предназначенные для информационного обслуживания граждан и организаций, которые обрабатывают документированную информацию с ограниченным доступом, а также средства защиты этих систем подлежат обязательной сертификации, в порядке, установленном Федеральным законом от 27 декабря 2002 г. N 184-ФЗ "О техническом регулировании". Согласно части 1 статьи 13.12 Кодекса РФ об административных правонарушениях нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации (за исключением информации, составляющей государственную тайну), влечет наложение административного штрафа на граждан в размере от трех до пяти минимальных размеров оплаты труда; на должностных лиц - от пяти до десяти минимальных размеров оплаты труда; на юридических лиц - от пятидесяти до ста минимальных размеров оплаты труда.

Часть 2 указанной статьи предусматривает ответственность за использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну). Указанное правонарушение влечет наложение административного штрафа на граждан в размере от пяти до десяти минимальных размеров оплаты труда с конфискацией несертифицированных средств защиты информации или без таковой; на должностных лиц - от десяти до двадцати минимальных размеров оплаты труда; на юридических лиц - от ста до двухсот минимальных размеров оплаты труда с конфискацией несертифицированных средств защиты информации или без таковой.

Еще один состав правонарушения, косвенно связанный с защитой права на коммерческую тайну, предусмотрен статьей 13.13 Кодекса РФ об административных правонарушениях. Занятие видами деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) без получения в установленном порядке специального разрешения (лицензии), если такое разрешение (такая лицензия) в соответствии с федеральным законом обязательно (обязательна), влечет наложение административного штрафа на граждан в размере от пяти до десяти минимальных размеров оплаты труда с конфискацией средств защиты информации или без таковой; на должностных лиц - от двадцати до тридцати минимальных размеров оплаты труда с конфискацией средств защиты информации или без таковой; на юридических лиц - от ста до двухсот минимальных размеров оплаты труда с конфискацией средств защиты информации или без таковой. Дела об административных правонарушениях, предусмотренных частью 1 статьи 13.13 Кодекса РФ об административных правонарушениях, рассматриваются должностными лицами органов ФСБ и Гостехкомиссии.

7.4. Уголовная ответственность за нарушение права на коммерческую тайну

Помимо вышеперечисленных видов ответственности за нарушение права на коммерческую тайну закон предусматривает и уголовно-правовые санкции за противоправные посягательства на законные права и интересы обладателя конфиденциальной информации.

В действующей редакции статьи 183 Уголовного кодекса РФ "Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну", в отличие от действовавшей до 1 февраля 2002 года, существенно расширен круг регулируемых правоотношений, усилена ответственность за незаконное получение и разглашение конфиденциальных сведений, совершенных из корыстной заинтересованности.

Часть 1 статьи 183 Уголовного кодекса РФ предусматривает уголовную ответственность за сбор информации, составляющей коммерческую, налоговую или банковскую тайну, путем похищения

документов, подкупа или угроз, а равно иным незаконным способом. Уголовный кодекс РФ предусматривает наказание в виде штрафа в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период от 1 до 6 месяцев либо лишение свободы на срок до двух лет. Наступление вредоносных последствий как достижение преступного результата является необязательным. Объективная сторона части 1 статьи 183 Уголовного кодекса носит формальный характер. Преступление считается оконченным с момента совершения действий по собиранию сведений, составляющих коммерческую, банковскую или налоговую тайну. Субъектом преступления является физическое вменяемое лицо, достигшее ко времени его совершения шестнадцатилетнего возраста и не имеющее законного доступа к указанной информации. В случае если способом собирания сведений, составляющих коммерческую, налоговую или банковскую тайну, является подкуп лиц, выполняющих управленческую функцию в коммерческой или иной организации, или (и) должностных лиц, они должны быть привлечены к ответственности не только за нарушение части 1 статьи 183 Уголовного кодекса, но и за нарушение части 1 или 2 статьи 204 или статьи 291 Уголовного кодекса РФ. Мотив преступления на квалификацию не влияет.

Часть 2 статьи 183 Уголовного кодекса РФ относит к разряду уголовно-наказуемых деяний 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. Такие деяния наказываются штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет либо лишением свободы на срок до трех лет. Незаконное использование может осуществляться посредством передачи закрытой информации третьим лицам либо путем принятия различных решений и осуществления действий на основе собранных сведений самим виновным. Под разглашением понимается предание сведений огласке, в результате которой они стали известны посторонним лицам (даже если информация стала известна хотя бы одному лицу, не имеющему права на ознакомление с ней).

Согласно части 2 рассматриваемой статьи субъектом преступления может быть любой работник организации или иные лица, которым сведения, составляющие коммерческую, налоговую или банковскую тайну, стали известны в связи с их профессиональной или служебной деятельностью. Это могут быть работники органов государственной власти и управления, правоохранительных органов, суда, прокуратуры и т.д. Режим конфиденциальности должен соблюдаться и в тех случаях, когда лицо уволилось с работы (в течение того времени, пока сведения не перестали быть охраняемой тайной). Есть все основания предполагать, что состав преступления будет и в действиях тех лиц, к которым информация попала случайно, либо если лица незаконно получили ее, либо она была доверена им. При этом судом должно быть однозначно установлено, что обвиняемому действительно известен характер разглашаемых сведений. Как и для состава преступления, предусмотренного частью 1 статьи 183 Уголовного кодекса РФ, мотив преступления на квалификацию не влияет.

Если в результате совершения указанных деяний был причинен крупный ущерб, или они были совершены из корыстной заинтересованности (ч. 3 ст. 183), то Уголовный кодекс предусматривает наказание в виде штрафа в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до 18 месяцев с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет либо лишение свободы на срок до пяти лет. В статье 183 Уголовного кодекса РФ не раскрывается понятие "крупный ущерб". Не следует думать, что это понятие носит оценочный характер (как, например, "значительный" ущерб). В примечании к статье 169 Уголовного кодекса РФ установлен его четко фиксированный размер - на сумму более 250 тысяч рублей. Для привлечения виновного лица к ответственности за нарушение части 3 статьи 183 Уголовного кодекса на основании причинения крупного ущерба, сторона обвинения должна представить убедительные доказательства наличия причинной связи между наступлением крупного ущерба и анализируемым деянием, так как наступление крупного ущерба может совпадать по времени с совершением деяния, но находиться в причинной связи с другими обстоятельствами (например, появлением у потерпевшего новых конкурентов на рынке).

Следует обратить внимание, что в научной литературе присутствует точка зрения, согласно которой "корыстная заинтересованность может быть не только материальной - стремление обогатиться, но может заключаться также в иной личной заинтересованности: зависть, обида, месть, стремление добиться первенства в конкурентной борьбе, уменьшить клиентскую базу хозяйствующего субъекта, желание устранить конкурента путем причинения ему убытков и так далее". С таким подходом нельзя согласиться - зависть, обида, месть и так далее никак не могут считаться корыстными мотивами. Здесь происходит смешивание и подмена неравнозначных понятий "корыстная" и "иная личная заинтересованность". Таким образом, если в качестве мотива выступала месть (что, впрочем, не характерно для преступлений, связанных с экономической деятельностью), то отсутствует

квалифицирующий признак рассматриваемой нормы. В качестве типичного примера можно привести следующий случай. В Иркутске были задержаны 2 сотрудника частного детективного агентства за попытку незаконного получения информации, составляющей коммерческую тайну. Детективы получили заказ от одной из иркутских коммерческих компаний собрать конфиденциальную информацию о конкурирующей фирме. Детективы осуществили "разработку" главного бухгалтера предприятия, предложив ему за вознаграждение предоставлять информацию о предприятии. Бухгалтер сообщил об этом своему директору, который обратился в УБОп. На встрече бухгалтера с детективами при передаче пакета документов они были задержаны, им предъявлено обвинение по нарушению части 3 статьи 183 Уголовного кодекса РФ.

Деяния, предусмотренные частями 2 и 3 статьи 183 Уголовного кодекса РФ, повлекшие тяжкие последствия, наказываются лишением свободы на срок до десяти лет. Для сравнения: часть 2 статьи 183 Уголовного кодекса РФ в действовавшей ранее редакции предусматривала максимальное наказание в виде лишения свободы на срок до 3-х лет. Можно сделать вывод, что законодатель гораздо более серьезно стал относиться к преступлениям, связанным с незаконным использованием коммерческой тайны. В качестве квалифицирующего признака объективной стороны в части 4 рассматриваемой статьи выступает наступление "тяжких последствий". Законодатель не дает четкого определения этого признака и не раскрывает какие-либо его признаки. Правоприменительная практика должна сама выработать те условия, которые позволяют отнести общественно опасные последствия к тяжким. Можно предположить, что под эту категорию подпадают, например, банкротство организации и (или) предпринимателя, причинение обладателю "тайн" особо крупного ущерба, вынужденную безработицу работников и так далее.

Все преступления, предусмотренные статьей 183 Уголовного кодекса РФ, совершаются с прямым умыслом, то есть лицо желает наступления неблагоприятных тяжких последствий обладателю "закрытых" сведений и сознательно их допускает.

Помимо уголовно-правовых санкций за незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну, уголовная ответственность также предусмотрена за преступления в сфере компьютерной информации, под которой Уголовный кодекс РФ понимает информацию, содержащуюся на машинном носителе, в памяти компьютера, системе ЭВМ или их сети. В отношении компьютерной информации, содержащей конфиденциальные сведения коммерческого характера, уголовно наказуемыми признаются следующие деяния:

1) неправомерный доступ (ст. 272 Уголовного кодекса РФ).

Для признания лица виновным в совершении данного преступления необходимо выполнение следующих условий - в результате неправомерного доступа произошло уничтожение, блокирование, модификация или копирование этой информации, нарушение работы ЭВМ, системы ЭВМ или их сети; имеются доказательства причинной связи между неправомерным доступом и указанными последствиями;

2) создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящее к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или носителей с такими программами (ст. 273 Уголовного кодекса РФ);

3) нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию конфиденциальной информации, если это деяние причинило существенный вред (ст. 274 Уголовного кодекса РФ).

Глава 8. Охрана конфиденциальности информации в рамках трудовых отношений

Одно из главных мест в организации защиты информации, составляющей коммерческую тайну, должно отводиться работе с персоналом. Человек остается самым слабым звеном в системе информационной безопасности. По оценке экспертов сохранность секретов на две трети зависит от правильного подбора, расстановки и воспитания кадров. В этой главе мы постараемся охватить весь комплекс проблем, связанных с охраной конфиденциальности информации в рамках трудовых отношений.

8.1. Кому принадлежит информация, составляющая коммерческую тайну, полученная в рамках трудовых отношений

Ответ на этот вопрос содержится в статье 8 Закона "О коммерческой тайне". В соответствии с

частью 1 указанной статьи обладателем информации, составляющей коммерческую тайну, полученной в рамках трудовых отношений, является работодатель. Хотя закон прямо не раскрывает используемое в данной норме понятие "получением информации, составляющей коммерческую тайну", исходя из контекста, можно сделать однозначный вывод, что авторы Закона подразумевали под ним некий интеллектуальный процесс, ведущий к генерации новых знаний работником в процессе осуществления своих трудовых функций. Таким образом, работник, получивший информацию в процессе трудовой деятельности, не будет считаться обладателем данной информации в смысле Закона "О коммерческой тайне". Рассматриваемая норма сформулирована как императивная, основанная на требовании закона, поэтому соответствующие условия не нуждаются в специальном закреплении в трудовом договоре или в ином договоре с работником.

Иначе обстоит дело с полученной работником информацией (или другим результатом деятельности), способной к правовой охране в качестве изобретения, полезной модели, промышленного образца, топологии интегральной микросхемы, программы для ЭВМ или базы данных. Как мы уже отмечали в [главе 1](#), объекты интеллектуальной собственности могут составлять содержание коммерческой тайны или входить в коммерческую тайну. В этом случае, согласно части 2 статьи 8 Закона "О коммерческой тайне" отношения между работником и работодателем регулируются в соответствии с законодательством РФ об интеллектуальной собственности. Следовательно, для таких случаев подлежит применению пункт 2 статьи 8 Патентного закона РФ от 23 сентября 1992 г. N 3517-1, согласно которому право на получение патента на изобретение, полезную модель или промышленный образец, созданные работником (автором) в связи с выполнением своих трудовых обязанностей или конкретного задания работодателя (служебное изобретение, служебная полезная модель, служебный промышленный образец), принадлежит работодателю, если договором между ним и работником (автором) не предусмотрено иное. Как мы видим, здесь уже нет императивного требования как в части 1 статьи 8 Закона "О коммерческой тайне", поэтому в договоре между работодателем и работником могут быть предусмотрены и другие варианты.

Работник-автор, создавший в процессе трудовой деятельности патентоспособный объект, но которому не принадлежит право на получение патента на данный объект промышленной собственности, имеет право на получение вознаграждения в том случае, если:

- 1) работодатель получит патент;
- 2) работодателем будет принято решение о сохранении информации об изобретении, полезной модели или промышленном образце в режиме коммерческой тайны (если, несмотря на принятие работодателем в установленный законом срок именно этого варианта охраны своих прав, работник предпримет попытку подачи заявки на выдачу патента либо иным образом будет пытаться раскрыть полученную информацию третьим лицам, работодатель имеет право защитить свои законные интересы с помощью иска о признании права на коммерческую тайну);
- 3) работодатель передаст право на получение патента третьему лицу;
- 4) работодатель не получит патент по поданной им заявке по зависящим от него причинам.

Размер вознаграждения должен быть соразмерным выгоде, которая получена работодателем или может быть им получена при надлежащем использовании объекта промышленной собственности. Размер и порядок выплаты вознаграждения определяются соглашением работника-автора служебной разработки и работодателя. Такое соглашение может быть заключено как заранее (например, при приеме автора на работу), так и в последующем (когда автор сообщит работодателю о своей разработке). Если достичь соглашения об условиях договора не удастся в течение трех месяцев после того, как одна из сторон сделает другой стороне предложение в письменной форме об этих условиях, вопрос может быть передан на рассмотрение суда. Следует подчеркнуть, что работодатель имеет полное право "засекретить" результат служебной разработки. Более того, согласно Патентному закону РФ для реализации данного права ему даже не требуется получения согласия работника-автора - достаточно только уведомить последнего об этом. В этом случае у работника возникают соответствующие обязанности по соблюдению конфиденциальности этой информации.

Работник-автор получает право запатентовать свою служебную разработку в том случае, если работодатель в течение четырех месяцев с даты получения уведомления от него о полученном им патентоспособном результате:

- 1) не приступит к оформлению патента на этот результат (то есть не подаст заявку на выдачу патента на изобретение, полезную модель или промышленный образец) в федеральный орган исполнительной власти по интеллектуальной собственности;
- 2) не передаст право на получение патента третьему лицу;
- 3) не сообщит работнику-автору о сохранении информации о соответствующем патентоспособном результате в режиме коммерческой тайны.

Следует обратить внимание, что законом предусмотрено право работодателя использовать служебное изобретение, служебную полезную модель или служебный промышленный образец в

собственном производстве в течение срока действия патента, даже если они были запатентованы работником. За такое использование работодатель обязан отчислить патентообладателю (работнику-автору) компенсацию, сумма которой определяется в договоре между ними.

Несмотря на то, что в текст части 2 статьи 8 Закона "О коммерческой тайне" не включены авторские произведения, следует толковать требования данной нормы расширенно - они должны распространяться на все без исключения объекты интеллектуальной собственности.

В соответствии со статьей 14 Закона РФ от 9 июля 1993 г. N5351-1 "Об авторском праве и смежных правах", которая посвящена регулированию авторских прав на произведения науки, литературы и искусства, созданные в порядке выполнения служебных обязанностей или служебного задания работодателя (служебные произведения), личные неимущественные права на такое произведение принадлежат его автору, а имущественные - работодателю автора.

К личным неимущественным правам автора в отношении его произведения относятся:

- 1) право признаваться автором произведения (право авторства);
- 2) право использовать или разрешать использовать произведение под подлинным именем автора, псевдонимом либо без обозначения имени, т.е. анонимно (право на имя);
- 3) право обнародовать или разрешать обнародовать произведение в любой форме (право на обнародование), включая право на отзыв;
- 4) право на защиту произведения, включая его название, от всякого искажения или иного посягательства, способного нанести ущерб чести и достоинству автора (право на защиту репутации автора);
- 5) право отказаться от ранее принятого решения об обнародовании произведения (право на отзыв) при условии возмещения пользователю причиненных таким решением убытков, включая упущенную выгоду. Если произведение уже было обнародовано, автор обязан публично оповестить о его отзыве. При этом он вправе изъять за свой счет из обращения ранее изготовленные экземпляры произведения. При создании служебных произведений положения настоящего пункта не применяются.

Личные неимущественные права принадлежат автору независимо от его имущественных прав и сохраняются за ним в случае уступки исключительных прав на использование произведения.

К исключительным имущественным правам автора на использование произведения относятся:

- 1) право воспроизводить произведение (право на воспроизведение);
- 2) право распространять экземпляры произведения любым способом: продавать, сдавать в прокат и так далее (право на распространение);
- 3) право импортировать экземпляры произведения в целях распространения, включая экземпляры, изготовленные с разрешения обладателя исключительных авторских прав (право на импорт);
- 4) право публично показывать произведение (право на публичный показ);
- 5) право публично исполнять произведение (право на публичное исполнение);
- 6) право сообщать произведение (включая показ, исполнение или передачу в эфир) для всеобщего сведения путем передачи в эфир и (или) последующей передачи в эфир (право на передачу в эфир);
- 7) право сообщать произведение (включая показ, исполнение или передачу в эфир) для всеобщего сведения по кабелю, проводам или с помощью иных аналогичных средств (право на сообщение для всеобщего сведения по кабелю);
- 8) право переводить произведение (право на перевод);
- 9) право перерабатывать, аранжировать или другим образом перерабатывать произведение (право на переработку);
- 10) право сообщать произведение таким образом, при котором любое лицо может иметь доступ к нему в интерактивном режиме из любого места и в любое время по своему выбору, - право на доведение до всеобщего сведения ("интернет-право" введено Федеральным законом от 20 июля 2004 г. N 72-ФЗ; вступает в силу с 1 сентября 2006 г.).

Закон "Об авторском праве и смежных правах" позволяет сторонам трудовых отношений относительно принадлежности исключительных имущественных прав установить в договоре иное.

В силу отсутствия в законодательстве требований об обязательной (тем более государственной) регистрации произведений и прав на них, имущественными правами на служебное произведение работодатель обладает в силу самого факта его создания. Чтобы в дальнейшем ни у кого не возникало вопросов по поводу того, что данное произведение действительно является служебным, работодатель должен иметь на руках следующие доказательства: трудовой договор, в котором отражены служебные обязанности работника-автора, его должностные инструкции, в которых фигурировала бы обязанность работника создавать объекты авторского права с указанием их конкретных видов.

Как показывает судебная практика, факт использования работником для создания произведения материалов и оборудования работодателя не является прямым доказательством того, что он создал

служебное произведение. Чтобы полностью исключить возможность работника-автора присвоить свои творческие наработки, работодателем должна быть предусмотрена система, которая отражала бы что конкретно, кем, в какие сроки разрабатывается. Это может быть оформлено приказом или распоряжением о проведении творческих изысканий, докладные записки с описанием промежуточных этапов работы, акты сдачи-приема результатов и так далее.

8.2. Права и обязанности работодателя и работника по охране конфиденциальности информации

Вопросы, касающиеся прав и обязанностей работодателя и работника по охране конфиденциальности информации, необходимо рассматривать применительно к двум возможным вариантам правового закрепления их взаимоотношений по поводу исполнения трудовых функций - при отсутствии трудового договора с работником и при наличии такового.

Рассмотрим сначала первый вариант. Если для развитых зарубежных стран отсутствие трудового договора является скорее исключением, причем весьма редким, то в нашей стране подобная практика - обычное явление. Хотя в последнее время наметилась явная тенденция к сокращению количества работников на безконтрактной основе. Ситуация, когда трудовой договор с работником заключен, однако, в нем отсутствуют положения о сохранении им коммерческой тайны, равно как и иным образом оформленные обязательства работника о соблюдении конфиденциальности, по правовым последствиям идентична рассматриваемому нами случаю. Это связано с тем, что при таком подходе права работодателя и работника приобретают нечеткий характер. Неопределенность прав работодателя особенно проявляется в вопросе о пределах действия законодательства об охране коммерческой тайны.

В отечественном трудовом законодательстве отсутствуют положения, прямо устанавливающие или хотя бы позволяющие вывести общую обязанность работников по сохранению конфиденциальности сведений, составляющих коммерческую тайну их работодателя. Это исключает возможность применения к работникам, разгласившим или иным образом способствовавшим утечке конфиденциальной информации, каких-либо санкций, и предъявление претензий к третьим лицам, получившим от работников закрытую информацию.

Наличие заключенного трудового контракта между работником и работодателем со специальным разделом, посвященным регулированию вопросов, связанных с обращением с информацией, составляющей коммерческую тайну, позволяет работодателю создать надежный механизм защиты "фирменных секретов" от посягательств со стороны персонала компании. И здесь очень важно найти эффективный баланс интересов работодателя - обладателя коммерческой тайны и работников (в том числе бывших). В случае чрезмерного расширения прав работодателя в сфере защиты своих прав на коммерческую тайну условия трудового договора могут вступить в противоречие с трудовым законодательством, имеющим целью охрану прав трудящихся.

Не следует забывать, что в соответствии с трудовым законодательством положения контракта (трудового договора), ограничивающие возможности работника в использовании им трудовых навыков и приемов, приобретенных по прежнему месту работы, включая и те, что достигнуты за счет его рационализаторских предложений, могут быть признаны незаконными. Работодателю следует исходить из того, что ограничения, принимаемые на себя работником на добровольной основе (но не навязанные ему), не должны вести к ограничению его право- и дееспособности. Согласно пункту 3 статьи 22 Гражданского кодекса РФ, полный или частичный отказ от правоспособности или дееспособности и другие сделки, направленные на ограничение право- и дееспособности, ничтожны, за исключением случаев, когда такие сделки допускаются законом. В связи с тем, что не всегда возможно в случае рассмотрения в судебном порядке законности тех или иных положений договора предсказать позицию суда, работодателю целесообразно предусмотреть в нем специальную оговорку, согласно которой действие трудового договора остается в силе во всем остальном, что не касается оспоренных положений.

В нашей стране появление требований в трудовых договорах о неразглашении информации, составляющей коммерческую тайну, и ставшую известной лицу в силу выполнения им своих трудовых функций, было связано с началом перестройки во второй половине 80-х годов. Таким образом, практика применения правовых механизмов защиты возникла еще до законодательного закрепления самого понятия коммерческой тайны и до того, как были внесены соответствующие изменения в Трудовой кодекс. Это произошло только в 1998 г. после принятия Закона РФ от 6 мая 1998 г. "О внесении изменений и дополнений в ст. 15 КЗоТ РФ". Законодательные новеллы о защите права на коммерческую тайну получили дальнейшее развитие в Трудовом кодексе РФ 2001 года.

Хотя обязанность не разглашать и не использовать информацию, составляющую коммерческую тайну, обладателем которой является работодатель, не входит в перечень основных обязанностей работника, который предусмотрен статьей 21 Трудового кодекса РФ (далее - Трудового кодекса РФ),

работник в любом случае обязан соблюдать правила внутреннего трудового распорядка организации и добросовестно исполнять обязанности, возложенные на него трудовым договором (контрактом), в котором, как правило, и регламентируется порядок обращения с конфиденциальной информацией. Кроме того, Трудовой кодекс РФ содержит целый ряд норм по вопросу защиты коммерческой тайны на предприятии. Согласно статье 37 Трудового кодекса РФ, участники коллективных переговоров, другие лица, связанные с ведением коллективных переговоров, не должны разглашать полученные сведения, если эти сведения относятся к охраняемой законом тайне (государственной, служебной, коммерческой и иной). Лица, разгласившие указанные сведения, привлекаются к дисциплинарной, административной, гражданско-правовой, уголовной ответственности в порядке, установленном федеральными законами. Статья 57 Трудового кодекса РФ предусматривает, что в трудовой договор могут быть включены условия об испытании, о неразглашении охраняемой законом тайны (государственной, служебной, коммерческой и иной), об обязанности работника отработать после обучения не менее установленного договором срока, если обучение производилось за счет средств работодателя, а также иные условия, не ухудшающие положение работника по сравнению с настоящим Кодексом, законами и иными нормативными правовыми актами, коллективным договором, соглашениями. Под условиями, ухудшающими положение работника, в частности, следует понимать возложение на него обязанностей, введение дополнительных мер ответственности, не предусмотренных трудовым законодательством.

Федеральный Закон "О коммерческой тайне" предусматривает, что в целях охраны конфиденциальности информации, составляющей коммерческую тайну, работодатель обязан:

- 1) ознакомить в письменной форме работника, доступ которого к информации, составляющей коммерческую тайну, необходим для выполнения им своих трудовых обязанностей или конкретного задания работодателя, с перечнем сведений, которые составляют коммерческую тайну работодателя и (или) его контрагентов;
- 2) ознакомить в письменной форме работника с установленным работодателем режимом коммерческой тайны и с ответственностью за его нарушение;
- 3) создать работнику необходимые условия для выполнения им установленного работодателем режима коммерческой тайны.

Доступ работника к информации, составляющей коммерческую тайну, осуществляется с его согласия.

В целях охраны конфиденциальности информации, составляющей коммерческую тайну, работник обязан:

- 1) выполнять установленный работодателем режим коммерческой тайны;
- 2) не разглашать информацию, составляющую коммерческую тайну работодателя и (или) его контрагентов, и без их согласия не использовать ее для собственных нужд в период действия трудового договора, а также в течение трех лет после его окончания, если соглашением между работником и работодателем, предусмотренным трудовым договором, не установлен иной срок. Вместе с тем Закон "О коммерческой тайне" предусматривает возможность заключения в период действия трудового договора специального соглашения между сторонами трудовых отношений (именно "соглашения", так как работник вправе отказаться от его заключения, тогда срок неразглашения составляет три года, как это установлено законом), в котором срок сохранения информации в режиме коммерческой тайны может быть изменен как в сторону увеличения так и уменьшения.

Какие же обязательства необходимо включить работодателю в договор, чтобы максимально обеспечить сохранность коммерческой тайны предприятия? Практика выработала типовые положения, позволяющие предусмотреть все аспекты правовой защиты конфиденциальности сведений, представляющих коммерческую ценность. Работник обязан:

- 1) не разглашать информацию, составляющую коммерческую тайну, обладателем которой является работодатель, которая будет ему доверена или станет известна в ходе выполнения трудовых функций;
- 2) не передавать третьим лицам и не раскрывать публично сведения, составляющие коммерческую тайну компании, без согласия уполномоченных лиц администрации;
- 3) сохранять информацию, составляющую коммерческую тайну организаций-контрагентов работодателя;
- 4) выполнять в части его касающейся требования приказов, инструкций, положений и других локальных нормативных актов по обеспечению сохранности коммерческой тайны работодателя;
- 5) не использовать информацию, составляющую коммерческую тайну работодателя, для занятия другой деятельностью, которая в качестве конкурентного действия может нанести ущерб организации;
- 6) при попытке третьих лиц получить от работника конфиденциальную информацию, незамедлительно сообщить об этом соответствующему должностному лицу;
- 7) в случае утраты, недостачи носителей информации, составляющей коммерческую тайну, удостоверений, пропусков, ключей от помещений в которых хранятся носители или идет обработка

"секретных" сведений, хранилищ, сейфов, личных печатей и о других событиях, которые могут привести к разглашению коммерческой тайны хозяйствующего субъекта, а также о причинах и условиях возможной утечки информации, незамедлительно сообщать уполномоченному должностному лицу;

8) при переходе на другой участок работы или при увольнении сдать уполномоченному лицу все носители, содержащие коммерческую тайну организации (документы, чертежи, рукописи, магнитные носители, видео- и фотоматериалы, изделия и так далее), которые находились в распоряжении работника в связи с выполнением им служебных обязанностей.

Трудовой договор с руководителем фирмы может дополнительно предусматривать его обязательство и ответственность по обеспечению охраны конфиденциальности информации, составляющей коммерческую тайну организации и (или) ее контрагентов. Согласно статье 273 Трудового кодекса РФ 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.

Все вышеперечисленные условия могут быть включены либо непосредственно в трудовой договор, либо они могут быть возложены на работника посредством оформления отдельного письменного обязательства (например, подписки о неразглашении и тому подобное), которое может быть заключено не только при приеме на работу, но и в последующем, в том числе при увольнении. Если работодатель использовал второй из вышеперечисленных способов оформления, то ему необходимо в обязательном порядке прямо указать в тексте обязательства о неразглашении на то, что оно является неотъемлемой составной частью трудового договора. Это связано с тем, что в статье 57 Трудового кодекса РФ фигурирует именно "трудовой договор" как документ, содержащий условия о неразглашении охраняемой законом тайны (государственной, служебной, коммерческой и иной).

Работодателю необходимо обратить особое внимание на то, что наличия в трудовом договоре (или иным образом оформленного соглашения между сторонами трудовых отношений) только общего условия о сохранении конфиденциальности информации, составляющей коммерческую тайну, недостаточно для того, чтобы "секреты фирмы" получили надежную правовую защиту от недобросовестных работников. Без четко закрепленного в локальных нормативных актах перечня сведений, отнесенных к категории коммерческой тайны, регламента безопасности и так далее работодателю будет весьма затруднительно привлечь к ответственности нарушителя режима коммерческой тайны.

8.3. Ответственность за разглашение коммерческой тайны в рамках трудовых отношений

Часть 3 статьи 11 Закона "О коммерческой тайне" в качестве общего правила устанавливает, что работник, виновный в разглашении служебной коммерческой тайны, обязан возместить работодателю причиненный ущерб. Данная норма должна толковаться расширительно - ясно, что ответственность работника должна быть предусмотрена не только за разглашение коммерческой тайны, но и за ее незаконное использование самим работником.

Какая ответственность предусмотрена для недобросовестного работника действующим законодательством*[^])?

Пунктом "в" части 6 статьи 81 Трудового кодекса РФ предусмотрена возможность расторжения трудового договора по инициативе работодателя в случае разглашения работником охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей.

В соответствии с требованиями частей 4 и 5 статьи 11 Закона "О коммерческой тайне" работник, нарушивший режим коммерческой тайны в период действия трудового договора, возмещает работодателю ущерб (подразумевается "реальный ущерб", который согласно ст. 15 Гражданского кодекса РФ не включает в себя упущенную выгоду). В том же случае, если нарушение допущено со стороны бывшего работника организации, то он возмещает своему бывшему работодателю убытки. Это связано с тем, что отношения между работодателем и работником после прекращения трудовой деятельности переходят из разряда трудовых и приобретают черты гражданско-правовых.

Как мы видим, в законе установлена ограниченная имущественная ответственность для действующих работников, нарушивших режим коммерческой тайны. Такой подход опирается на требования трудового законодательства, в частности - статьи 243 Трудового кодекса РФ, согласно которой в случаях разглашения сведений, составляющих коммерческую тайну, на работника возлагается материальная ответственность в полном размере причиненного ущерба. Согласно пункту 1 статьи 400 Гражданского кодекса РФ ограниченная ответственность не может быть увеличена договором. Как правило, в результате утраты фактической монополии на закрытые сведения коммерческого характера обладатель коммерческой тайны несет убытки в виде упущенной выгоды. Реальный ущерб

присутствует, в основном, только если работодатель, являясь стороной гражданско-правового договора, предусматривающего в качестве обязательного условия сохранение конфиденциальности переданных по договору сведений, сам оказывается должен возместить убытки пострадавшей стороне. Таким образом, зачастую работник, по вине которого фирма недополучила миллионы рублей возможной прибыли, сам может избежать материальной ответственности. Остается только надеяться, что либо сами законодатели, либо судебная практика исправят этот недочет, признав соответствующие положения статьи 11 Закона противоречащими статье 139 Гражданского кодекса РФ.

Несколько иного подхода придерживается отечественное законодательство в отношении "работников высшего звена" - руководителей организации. В соответствии со статьей 277 Трудового кодекса РФ, в случаях, предусмотренных федеральным законом, руководитель организации возмещает организации убытки, причиненные его виновными действиями. В отличие от положений, устанавливающих ограниченную ответственность рядовых работников за нарушение режима коммерческой тайны, Закон "О коммерческой тайне" предусматривает, что "руководитель организации возмещает организации убытки, причиненные его виновными действиями в связи с нарушением законодательства Российской Федерации о коммерческой тайне". Согласно части 1 статьи 11 указанного закона "убытки определяются в соответствии с гражданским законодательством". Это означает, что ответственность руководителя организации в данном случае является не ограниченной, а полной. В остальном же к руководителю организации должны применяться все положения, содержащиеся в частях 1-5 и 8 статьи 11 Закона "О коммерческой тайне".

В случае если разглашение работником информации, составляющей коммерческую тайну, обладателем которой является работодатель (его контрагенты), стало возможным в результате неисполнения работодателем обязанности по обеспечению режима коммерческой тайны, то убытки, причиненные разглашением этой информации, работником не возмещаются, также как и в случае, если разглашение конфиденциальных сведений явилось следствием непреодолимой силы или крайней необходимости.

Согласно статье 401 Гражданского кодекса РФ 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.

В соответствии со статьей 1067 Гражданского кодекса РФ вред, причиненный в состоянии крайней необходимости, то есть 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.

В заключение рассмотрения проблем, связанных с охраной информации, составляющей коммерческую тайну, хотелось бы обратить внимание отечественных работодателей на тот факт, что менее всего страдают от утечки информации японские компании. Это объясняется широким применением японским бизнесом системы "пожизненного найма" и воспитанием у работников чувства патриализма, когда все служащие компании, включая руководство, считают себя членами одной семьи. Российским предпринимателям есть смысл прислушаться к словам руководителя одной из крупнейших японских компаний, который утверждает, что когда нет преданности, которая приходит с долгосрочной занятостью, то даже самая современная техника не сможет положить конец утечкам информации и воровству, от которых повседневно страдает бизнес на Западе.

* (1) Гаврилов О.А. Курс правовой информатики: Учебник для вузов. М.: НОРМА, 2000. С. 2.

* (2) В российской судебной практике не раз возникал вопрос о возможности отнесения к коммерческой тайне опубликованных программ теле- и радиопередач и запрете на публикацию таких программ третьими лицами. Окончательную точку в данном вопросе поставил Высший Арбитражный Суд Российской Федерации (постановление Пленума ВАС РФ от 24.11.1998 г. N3900/98), признав невозможным распространение правового режима коммерческой тайны на теле- и радиопрограммы на основании несоответствия условию неизвестности.

* (3) Соловьев Э.Я. Коммерческая тайна и ее защита. М.: Ось-89, 2001. С. 26-27.

* (4) Смирнов В. Ноу-хау в российском законодательстве//Интеллектуальная собственность. 2000. N 1. С. 36.

* (5) Согласно Указу Президента РФ N 188 от 6 марта 1997 г. "Об утверждении перечня сведений конфиденциального характера" к конфиденциальной информации относятся "сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о

них"; эта группа сведений приобретает конфиденциальный характер с момента подачи документов в федеральный орган исполнительной власти по интеллектуальной собственности, независимо от того, обладают ли эти сведения тремя признаками коммерческой тайны.

*(6) Согласно статье 1 Федерального закона "О банках и банковской деятельности", небанковская кредитная организация - кредитная организация, имеющая право осуществлять отдельные банковские операции, предусмотренные указанным Законом. Допустимые сочетания банковских операций для них устанавливаются Банком России.

*(7) Постановлением Правительства РФ от 26 июня 1995 г. N608 "О сертификации средств защиты информации" утверждено Положение о сертификации средств защиты информации".

*(8) Решение Высшего Арбитражного Суда РФ от 3 марта 2004 г. N 15527/03.

*(9) Согласно действующей редакции Федерального конституционного закона о Правительстве РФ от 19 июня 2004 г. управление федеральной собственностью также относится к полномочиям Правительства РФ в сфере экономики.

*(10) Постановление Пленума Высшего Арбитражного Суда РФ от 22 декабря 1992 г. N 23.

*(11) В ряде случаев обладатель коммерческой тайны раскрывает конфиденциальную информацию потенциальным партнерам до заключения лицензионного договора с целью продемонстрировать коммерческую ценность "секрета фирмы". В этом случае стороны могут договориться о выплате обладателю компенсации на тот случай, если партнер после ознакомления с информацией откажется от заключения договора. Эта компенсация называется "паушальный" взнос.

*(12) Соловьев Э.Я. Коммерческая тайна и ее защита. М.: Ось-89, 2001. С. 23.

*(13) Погуляев В.В. Правовые аспекты применения химических ловушек//Защита информации. Конфидент. 2004. N 3 (57). С. 26-28.

*(14) Э. Гаврилов. Вопросы правовой охраны коммерческой тайны//Хозяйство и право. 2004. N 11. ст. 27.

*(15) Применение уголовно-правовых санкций было рассмотрено в предыдущей [главе](#).