

*Dr.iur. Александр Байков, ассоциированный профессор
Балтийская международная академия
Латвия*

Проблемы функционирования правового механизма защиты коммерческой тайны на предприятии

Аннотация. В статье рассматриваются организационные, административные (управленческие) и правовые меры обеспечения сохранности коммерческой тайны. Последовательно анализируются условия обеспечения конфиденциальности коммерческой информации, методика выделения сведений, составляющих коммерческую тайну, мероприятия по защите информации. Автором дается оценка роли управленческой информации в конкурентной борьбе, разрешительной системы доступа к информации. Достаточно подробно исследуется правовая природа и виды соглашений о конфиденциальности, содержание некоторых из них, способы защиты от разглашения коммерческой тайны, среди которых основное место занимают применяемые к правонарушителям меры ответственности, а также основные вопросы охраны коммерческой тайны после прекращения трудовых отношений с работником.

Ключевые слова: информация, закрытая информация, коммерческая тайна, государственная тайна, перечень относимых к коммерческой тайне сведений, режим конфиденциальности, формы конфиденциальных отношений, режим коммерческой тайны, механизм защиты коммерческих секретов.

Вместо введения

Проблематика правового регулирования информационно-правовых отношений, связанная с процессами становления и развития информационного общества, приобрела особую актуальность и стала предметом научных изысканий, начиная с 70-х годов прошлого века. Справедливо было замечено, что в определенных формах информация является элементом любых общественных отношений [1, 93], да и сами правовые нормы – это, прежде всего, информация о возможном и должном поведении, о позитивных или негативных последствиях правомерного и, соответственно, неправомерного поведения, т.е. правовые нормы содержат правовую информацию [2, 15].

В этой связи, более чем оправданно, то внимание, которое сегодня уделяется анализу информационно-правовых отношений в целом, информации как объекту права интеллектуальной собственности [3, 461 – 474], правовых режимов различных видов информации, в том числе

коммерческой тайны, несанкционированный доступ к которой нередко используется в конкурентной борьбе. Поэтому нельзя не согласиться с известным утверждением Уинстона Черчилля – «кто владеет информацией, тот владеет миром».

Формы и способы защиты права на коммерческую тайну, факторы и организационно-правовые мероприятия, влияющие на обеспечение сохранности и неразглашения конфиденциальных сведений, неоднократно анализировались, как в правовом, так и в экономическом и управленческом аспектах, такими учеными, как Т.Ю. Базаров [Т.У. Bazarov, 1998], М.И. Брагинский, В.В. Витрянский [М.И. Braginsky, V.V. Vitryansky, 1998], В.А. Лапач (V.A. Lapach, 2002), В.Ф. Попондопуло [V.F. Popondopulo, 2004], А.П. Сергеев [A.P. Sergeyev, 2003], Э. Я. Соловьев [E. J. Solovyov, 1996] и многими другими авторами.

Цель настоящей работы – провести анализ методики выделения сведений, составляющих

коммерческую тайну, основных направлений, методов и способов её защиты и на этой основе разработать порядок ее организационно-юридической защиты, т.е. режим конфиденциальности в контексте обеспечения эффективной деятельности предприятия в условиях конкуренции. Данная статья является логическим продолжением предпринятого автором исследования, опубликованного ранее в «Балтийском юридическом журнале» в статье «Коммерческая тайна: понятие и правовой режим» (№1 (22), 2011), где были рассмотрены понятие, конститутивные признаки, правовая природа, содержание коммерческой тайны, правовой статус ее владельцев, содержание субъективного права на коммерческую тайну, его правовой режим.

Проблема защиты информации от несанкционированного доступа к ней возникла не сегодня. Так еще Геродот отмечал, что уже в V веке до нашей эры использовалось преобразование информации методом кодирования. В виде криптограмм (по-гречески — тайнопись) коды появились в глубокой древности. Например, спартанцы использовали специальное устройство, дававшее возможность особым способом, обеспечивающим сохранение тайны, писать важные сообщения. Секретной азбукой пользовался Юлий Цезарь. В эпоху Возрождения, над созданием тайных шифров, трудились известный философ Ф.Бэкон и крупные математики Ф.Виет, Д. Кардано.

В 1817 году в Великобритании, а в США в 1837 году, впервые, в судебных заседаниях появилось упоминание «коммерческой тайны», и эти судебные решения стали важными прецедентами.

Впервые, законодательный акт, направленный на защиту коммерческой тайны, был принят во Франции в 1844 году. Годом позже, в России «Уложением о наказаниях общего определения» было введено наказание за разглашение коммерческой тайны. К началу XX века, коммерческая тайна защищалась уже во всех европейских странах.

Основным фактором, способствующим защите циркулирующей на предприятии информации, остаются режимные, т.е. специальные меры, направленные на предотвращение утечки конкретных сведений. Принятие специальных мер, направленных на защиту интеллектуальной собственности, зависит, прежде всего, от вла-

дельца (владельцев) информации, складывающейся в их среде деятельности конкурентной обстановки, ценности, которую представляет для них производственная или коммерческая информация, и других факторов.

Безусловно, хранить секрет, если он больше никому кроме владельца не известен, не представляет большой сложности и не требует больших затрат. Носитель информации (документ, дискета, предмет) должен иметь соответствующее место хранения (сейф или другое недоступное для других лиц место). Несколько усложняется охрана этих сведений, когда об их наличии становится известно заинтересованным лицам. Возникает необходимость ограничить доступ посторонних лиц к месту хранения секретных материалов.

Предприятия, фирмы, объединения, где имеется не один, а несколько владельцев информации, к тому же ещё и работают сотрудники, не допущенные к производственным, коммерческим секретам, представляют собой более сложный объект защиты. Возникает вопрос о необходимости обеспечения внешней и внутренней безопасности. Для его решения можно использовать коммерческие фирмы, предоставляющие услуги по обеспечению безопасности и, безусловно, собственные службы безопасности.

Важное место в системе организационных, административных, правовых и других мер, позволяющих качественно решать задачи информационного обеспечения научно-производственной и коммерческой деятельности, физической сохранности материальных носителей закрытых сведений, предотвращения их утечки, сохранения коммерческой тайны, занимает разрешительная система доступа исполнителей к классифицированным документам и сведениям. Под доступом понимается получение письменного разрешения руководителя предприятия (или, с его санкции, других руководящих лиц) на выдачу тому или иному сотруднику конкретных закрытых сведений, с учетом его служебных обязанностей (должностных полномочий).

Обеспечение сохранности конфиденциальной коммерческой информации требует соблюдения следующих условий: (1) определение (выявление) сведений, составляющих коммерческую тайну предприятия; (2) разработка порядка их охраны; (3) обеспечение соблюдения этого порядка.

Методика выделения сведений, составляющих коммерческую тайну

Порядок выделения, из всего объема собственной информации предприятия (фирмы), ее наиболее ценных частей, для последующей защиты, тесно связан с процессом производства товаров (услуг) и вытекает из практики конкурентной борьбы. Факторы, определяющие конкурентоспособность предприятия, способны давать позитивные результаты, только при условии их сокрытия от экономических соперников. Поэтому, отнесение таких сведений к коммерческой тайне, является формой защиты экономической безопасности предприятия (фирмы), оформляемой распоряжением руководителя. В этом распоряжении перечисляются сведения, относящиеся к коммерческой тайне. Сущность формирования методики выделения ценных сведений заключается в отыскании логики действий и признаков, характеризующих коммерческую тайну.

Исключив из информационных потоков информацию, составляющую государственную тайну, а также общеизвестную информацию, в оставшемся информационном объеме можно выделить два вида сведений: (1) технология, управление; (2) деловая (финансово – коммерческая) информация.

Часть информации, с учетом целесообразности и коммерческой выгоды, защищается нормами закона Латвийской Республики от 15 февраля 2007 года «Патентный закон» [4] и закона Латвийской Республики от 06 апреля 2000 года «Об авторском праве» [5], а также основных международных конвенций, регулирующих эти положения.

После последовательного выполнения вышеназванных действий, предметом анализа и оценки остается лишь часть, незащищенных с помощью патентов и авторского права, сведений, а также коммерческо-финансовые данные. Ключом к пониманию того, какие сведения целесообразно, в тот или иной период, защищать как коммерческую тайну, является конкуренция (ценовая и неценовая). Именно поэтому, к коммерческой тайне целесообразно относить сведения, которые дают (могут дать) значимые преимущества в конкурентной борьбе. Разглашение же этой информации наносит

экономический ущерб, вследствие снижения конкурентоспособности товаров и услуг предприятия. Американские бизнесмены считают, что утрата 20% информации приводит к разорению фирмы в течение месяца в 60 случаях из 100 [6, 4].

Далее осуществляется анализ и проводится оценка сфер и циклов производства товаров, в которых возможны нововведения: товар, сервис, маркетинг, производство, распределение, финансирование, управление, социальная сфера. В каждой из этих сфер, на основе анализа, определяется объем нововведений в процентах, необходимый для успешной деятельности [7]. Наибольший объем сведений (нововведений, влияющих на конкурентоспособность), составляющих коммерческую тайну, приходится на следующие сферы: товар, маркетинг, производство, сервис, управление.

Рассматривая цикл производства с позиции охраны коммерческой тайны, следует учитывать, что большинству фирм удается добиться динамического роста и финансово-коммерческого успеха, путем последовательных усовершенствований. С учетом особенностей рынка, к коммерческой тайне должны относиться сведения об усовершенствованиях выпускаемых изделий, включая технологию и другие вопросы (а не только значительные инновации).

В мероприятиях по защите информации должна найти отражение проблема дифференциации качества товаров, относительно товаров конкурентов. На стадии разработки товара, определенную ценность как раз и будут представлять сведения (информация) о его свойствах, обеспечивающих существенное отличие от уже имеющихся на рынке изделий. Это наиболее ценные сведения предприятия (фирмы), составляющие коммерческую тайну. При покупках руководствуются не только ценой, но и показателями дифференциации товаров, достигнутой в результате эффективного дизайна. Усилия предприятий направляются на повышение ценностной значимости собственных товаров в глазах клиента и на углубление разницы между своими товарами и товарами конкурента. В этой связи, целесообразно сначала составить исчерпывающий перечень свойств своего товара, а затем задаваться вопросом, какое из этих свойств, будучи усовершенствованным, обеспечит ему

наиболее конкурентное отличие. Именно эти сведения, с большей вероятностью, могут быть отнесены к коммерческой тайне.

Оценка роли управленческой информации в конкурентной борьбе, за получение преимуществ перед экономическими соперниками, позволяет включить ряд сведений, из этой сферы деятельности предприятия, в перечень данных, составляющих коммерческую тайну. Ощутимый экономический ущерб может нанести разглашение коммерческой тайны, на этапе испытания разработанного товара рынком. Главное в процессе рыночных испытаний – оценить привлекательность товара для потребителя. Необходимо обеспечить защиту таких сведений, которые облегчили бы принятие конкурентами соответствующих контрмер. Как правило, охране на этой стадии подлежат: торговая марка продукта, название фирмы, которая проводит испытания, результаты испытаний, время вывода продукта в серийное производство и т.п.

Для удержания или завоевания позиций на рынке, предприятия активно используют рекламу, в которой важно не допустить разглашения ценной информации, так как, получив ее, конкуренты могут внести необходимые коррективы в процессе конкурентной борьбы. Испытанный метод рекламы, обеспечивающий защиту коммерческой тайны – это, так называемый, метод черного ящика. При этом описывается проблема, показываются достигнутые результаты, полученные преимущества, но как это достигнуто, сообщается в урезанном виде, с крайней осторожностью. В последние годы, в промышленно развитых странах, службы безопасности стали принимать меры по защите информации, которую соперничающие фирмы могут получить в анализе отходов продукции, поступающих в утилизацию или на рынок. Главной формой защиты является содержание в тайне фирмами, специализирующимися на продаже отходов производств, сведений о предприятиях-поставщиках этого сырья.

Особое внимание следует уделять охране заключенных коммерсантом договоров. Большая часть их относится к коммерческой тайне. Причем, в определенных случаях, охране подлежит не только текст договора, но и сам факт его заключения. Не подлежит огласке информация, раскрытие которой может привести

к неблагоприятным последствиям (номера домашних телефонов, адреса сотрудников, планы работы, информация о конфликтных ситуациях в коллективе) [8, 283].

Первый шаг, который должен сделать коммерсант, желающий сохранить свои производственные или технологические секреты, – разработать перечень сведений, составляющих коммерческую тайну предприятия, а также утвердить Положение о порядке обеспечения сохранности коммерческой тайны предприятия. Документально оформленная коммерческая тайна предприятия, выраженная в определенном объеме сведений, приобретает согласно части 1-й статьи 83-й Трудового Закона Латвии (в дальнейшем – ТЗ) [9] статус «сведений, составляющих коммерческую тайну работодателя», и является собственностью работодателя.

Для того, чтобы принять решение о включении тех или иных данных о деятельности предприятия в перечень сведений, составляющих коммерческую тайну, целесообразно, на первом этапе, определить возможные отрицательные последствия, в случае их разглашения. К отрицательным последствиям относятся: разрыв деловых отношений с партнерами; срыв переговоров; утрата возможности заключения выгодного договора; снижение уровня сотрудничества с деловыми партнерами; невыполнение договорных обязательств; необходимость проведения дополнительных рыночных исследований; отказ от решений, ставших неэффективными в результате разглашения информации и необходимость принятия дополнительных мер, связанных с финансовыми затратами; использование конкурентами полученных сведений для повышения эффективности экономического соперничества; потеря возможности патентования и продажи лицензии; совершенствование технологии; снижение цен на продукцию или снижение объемов продаж; нанесение ущерба авторитету фирмы; снижение уровня экономической безопасности; опережение конкурентом вывода аналогичного товара на рынок; ухудшение условий получения кредитов; появление трудностей в снабжении, приобретении оборудования; увольнение ведущих специалистов предприятия [10, 42].

Чтобы избежать ошибок, необходимо учитывать дополнительные критерии отнесения информации к коммерческой тайне. Наиболее

общими из них являются: выигрыш во времени для предприятия в сравнении с конкурирующими фирмами; уникальность разработки; новизна (новая функция потребления, новая технология, применение в новых областях); преимущества в технико-экономических характеристиках товара перед изделиями конкурента; оригинальное применение материалов, технологий; преимущества в ценовой конкуренции; значительные трудозатраты в получении информации; монополия предприятия на информацию по данному направлению производственно-коммерческой деятельности; степень очевидности использования информации конкурентами в случае ее опубликования; перспектива самостоятельного получения сведений, закрываемых конкурентами; появление возможности выхода на международный рынок; степень влияния на формирование у потребителя положительного представления о фирме; возможность обеспечения сохранности на предприятии информации, в случае ее отнесения к коммерческой тайне [11, 65].

Структура и содержание перечня сведений, относимых к коммерческой тайне, зависят от характеристики предприятия. В перечне, по возможности, указываются сроки пересмотра сведений, отнесенных к коммерческой тайне, и перевода их в разряд общедоступных. Составив список технологий и деловой информации по приемлемой схеме, прежде всего, необходимо обеспечить защиту ценной информации, утечка которой способна нанести ущерб, превышающий затраты на ее защиту.

Практика показывает, что данный вопрос лучше решать коллегиально. Для разработки перечня, распоряжением руководителя предприятия, создается комиссия из наиболее квалифицированных и компетентных специалистов основных подразделений и представителей службы безопасности. Нельзя использовать отнесение каких-либо сведений к категории коммерческой тайны в целях уклонения от уплаты налогов, сокрытия фактов нанесения ущерба здоровью людей, а также других противозаконных действий. Результатом работы экспертов должен стать перечень сведений, составляющих коммерческую тайну предприятия. Вполне естественно, что по мере необходимости этот перечень должен пересматриваться, изменяться и дополняться. В перечне,

если возможно, желательно указать конкретный срок, на который те или иные сведения отнесены к коммерческой тайне.

Перечень доводится до структурных подразделений и соисполнителей в части, их касающейся, для руководства в работе и приведения в соответствие с ним грифа работ (целесообразно применять гриф «коммерческая тайна»), документов и изделий. Исполнитель и руководитель, подписывающий документ, оценивают при его подготовке содержащиеся в нем сведения, составляющие коммерческую тайну предприятия.

Разработка порядка охраны коммерческой тайны

Организационно-юридическая защита коммерческой тайны реализуется путем установления на предприятии режима конфиденциальности. Конфиденциальные отношения являются фундаментальной категорией, характеризующей механизм защиты коммерческих секретов. Можно выделить три формы конфиденциальных отношений:

- между сотрудниками и самим работодателем, как юридическим лицом, возникающие с момента трудоустройства конкретного лица и продолжающиеся в течение всего периода его работы на данном предприятии;
- между конкретным сотрудником и другими сотрудниками этого предприятия, складывающиеся и развивающиеся как по вертикали, так и по горизонтали;
- между заказчиком и исполнителем, порожденные договором на выполнение работ или оказание каких-либо услуг.

Как отмечалось выше, право установления режима коммерческой тайны имеет обладатель коммерческой тайны. Конфидент коммерческой тайны обязан соблюдать режим коммерческой тайны, установленной ее обладателем или же установить режим коммерческой тайны, если это следует из обязательств, содержащихся в договоре, заключенном с обладателем коммерческой тайны. Оформление доступа к коммерческой тайне может производиться в соответствии с утвержденным руководителем положением о разрешительной системе

доступа, где юридически закрепляются полномочия должностных лиц предприятия по распределению информации и пользованию ею. Руководитель предприятия может разрешить пользование любой охраняемой информацией любому работнику данного предприятия или лицу, прибывшему на объект из другой организации для решения каких-либо вопросов, если в отношении этих сведений не установлены ограничения на ознакомление со стороны производственно-коммерческих партнеров по совместному производству и т.п. [12, 47].

На небольших предприятиях, с ограниченным объемом закрытых работ (документов и изделий), руководитель имеет возможность лично распределять всю закрытую информацию, поступающую извне и создаваемую внутри предприятия, между работниками, независимо от занимаемых ими должностей. В этом случае осуществляется, так называемое, прямое распределение классифицированной информации. Однако прямое распределение становится невозможным на предприятии с большим объемом закрытых работ, рассредоточенным по различным подразделениям и участкам, в которых задействованы сотрудники различных должностных категорий. В целях качественного выполнения управленческих функций руководитель предприятия часть своих прав, распоряжаться движением классифицированных сведений, может передать руководителям нижестоящих уровней. Руководитель, как правило, оставляет за собой право распоряжаться наиболее ценными сведениями, составляющими коммерческую тайну (конфиденциальные договоры с фирмами, отчеты о результатах работ по перспективным изделиям и т.п.).

Эффективная работа разрешительной системы возможна только при соблюдении определенных правил:

- дифференцированный подход к разрешению доступа, учитывающий важность классифицированных сведений, в отношении которых решается вопрос о доступе;
- документальное отражение выданного разрешения на право пользования теми или иными защищаемыми сведениями. Это означает, что руководитель, давший разрешение на право пользования, должен его, в обязательном порядке, зафиксировать

в письменном виде на соответствующем документе или в действующей на предприятии учетной форме. Никакие устные указания и просьбы о доступе кого бы то ни было (за исключением руководителя предприятия) не имеют юридической силы и не обязательны для работников службы безопасности. Это требование относится и к руководителям всех уровней, работающих с классифицированной информацией и ее носителями;

- соблюдение принципа контроля со стороны службы безопасности. Это означает, что любое разрешение на ознакомление с закрытыми документами, сведениями и объектами должно быть согласовано с начальником службы безопасности. В разрешении должны быть указаны: дата его оформления и выдачи, фамилии, должности лиц, конкретные классификационные документы и изделия, к которым они могут быть допущены (ознакомлены) [13, 199].

Эффективно функционирующая разрешительная система должна отвечать следующим требованиям:

- распространяться на все виды классифицированных документов и изделий, имеющих на предприятии, независимо от места их нахождения и создания;
- определять порядок доступа всех категорий сотрудников, получивших право работать с коммерческой тайной, а также специалистов, временно прибывших на предприятие и имеющих отношение к совместным закрытым заказам;
- устанавливать простой и надежный порядок оформления разрешений на доступ к охраняемым документам и изделиям, позволяющий незамедлительно реагировать на изменения в области информации на предприятии;
- четко разграничивать права руководителей различных должностных уровней, в оформлении доступа соответствующих категорий исполнителей;
- исключать возможность бесконтрольной и несанкционированной выдачи документов и изделий кому бы то ни было;
- не разрешать лицам, работающим с классифицированной информацией и объекта-

ми, вносить изменения в учетные данные, а также подменять учетные документы.

Соблюдение вышеперечисленных требований важно, хотя бы в силу того, что, как показал опрос крупнейших российских компаний, причинами разглашения коммерческих секретов являются: (1) болтливость сотрудников, особенно связанная с употреблением алкоголя и общением в дружеских компаниях – 32%; (2) стремление сотрудников заработать деньги любым способом, по принципу «деньги не пахнут» – 24%; (3) отсутствие службы безопасности фирмы – 14%; (4) «советская» привычка персонала делиться опытом, давать советы – 12%; (5) бесконтрольное использование информационных и копировальных средств на фирме – 10%; (6) психологические конфликты между сотрудниками, между сотрудниками и руководством – 8% [14]. Как видно из вышесказанного, все причины самым непосредственным образом связаны с человеческим фактором.

Гриф коммерческой тайны, которым помечают те или иные документы, обычно содержат словосочетание «Коммерческая тайна», свидетельствующее о принадлежности информации к коммерческой тайне. Указанный гриф проставляется на носителе информации или сопроводительном документе. В правом верхнем углу документа пишется: «КТ» (или полностью – «Коммерческая тайна»), «Конфиденциально». Такая пометка не является грифом секретности, а лишь показывает, что право собственности на данную информацию охраняется законодательством. На документах, содержащих коммерческую тайну и передаваемых в органы государственной власти, иные государственные органы и органы местного самоуправления, гриф «Коммерческая тайна» проставляется на носителях информации в обязательном порядке.

Лицо, устанавливающее режим коммерческой тайны, самостоятельно определяет критерии отнесения вновь получаемой информации к коммерческой тайне. Им также определяется срок действия режима коммерческой тайны и совокупность мер по обеспечению режима коммерческой тайны, в отношении получаемой информации, в том числе, постановку и снятие грифа коммерческой тайны, порядок доступа к коммерческой тайне, выбор и использование средств и методов защиты, хранения и передачи

информации, составляющей коммерческую тайну, за исключением случаев, предусмотренных законом или договором.

При разработке разрешительной системы, особое внимание должно быть уделено выделению главных, особо ценных для предприятия сведений, что позволит обеспечить к ним строго ограниченный доступ. При наличии совместных работ с другими предприятиями (организациями), иностранными фирмами или их отдельными представителями, необходимо предусмотреть порядок доступа этих категорий к коммерческой тайне предприятия. В положении о разрешительной системе фирмы необходимо указать, что передача классифицированных документов и изделий от исполнителя к исполнителю возможна только в пределах структурного подразделения и с разрешения его руководителя. Передача, возврат таких документов, изделий производится по установленному на фирме порядку и только в течение рабочего времени данного дня.

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

Как уже отмечалось выше, сотрудники других фирм могут участвовать в закрытых совещаниях только с персонального разрешения руководства фирмы. Готовит списки, как правило, лицо, ответственное за организацию совещания в контакте с заинтересованными руководителями структурных подразделений. Список является основанием для организации контроля за допуском на данное совещание. Перед началом совещания сотрудник службы безопасности предупреждает присутствующих, что обсуждаемая информация носит закрытый характер и не подлежит распространению

за пределы, установленной фирмой, сферы обращения, и выдает инструкции по порядку ведения записей.

Срок действия режима коммерческой тайны устанавливается и определяется сроком действия условий, необходимых и достаточных для признания определенной информации коммерческой тайной. Обязательной мерой по обеспечению режима коммерческой тайны, является заключение обладателем и конфиденнтом коммерческой тайны, должным образом оформленных, соглашений о конфиденциальности или иных, подтверждающих обязательства о неразглашении коммерческой тайны, договоров.

Конфидент коммерческой тайны, получивший коммерческую тайну в силу гражданско-правового договора и допустивший ее разглашение, обязан незамедлительно известить об этом обладателя коммерческой тайны. При отсутствии в его действиях состава преступления, конфидент коммерческой тайны несет гражданско-правовую ответственность, в соответствии с действующим законодательством.

Необходимым условием установления режима коммерческой тайны, при заключении и выполнении гражданско-правового договора, является заключение сторонами в письменной форме соглашения о конфиденциальности наряду с договором или включение соответствующих условий в трудовой договор. Согласно части 1-й статьи 83-й ТЗ, работник обязан хранить в тайне попавшие в его распоряжение сведения, составляющие конфиденциальную информацию предприятия.

Соглашение о конфиденциальности может быть односторонним или взаимным, т. е. связывающим обязательством хранить молчание либо только одну его сторону, либо одновременно и работника и работодателя. Одностороннее соглашение о конфиденциальности наиболее часто встречается на практике. Именно односторонним является обычно соглашение о конфиденциальности, заключаемое с наемным работником. Взаимное соглашение о конфиденциальности заключается, как правило, в том случае, когда работник, чаще руководитель высокого уровня или ведущий технический специалист, приходит в крупную компанию с уже готовым бизнес-планом или разработкой, а компания предоставляет данные о своих мар-

кетинговых, финансовых и иных возможностях. В любом соглашении о конфиденциальности должен быть, прежде всего, четко и с максимально возможной степенью детализации и конкретизации определен его предмет и полный перечень той информации, которую стороны впредь будут рассматривать как конфиденциальную.

При этом необходимо учитывать, что далеко не любая хотя бы и секретная, исходя из локальных нормативных документов данного предприятия, информация может быть признана таковой в рамках соглашения о конфиденциальности, заключаемого с конкретным работником. Так, например, если в компанию поступает разработчик, создавший некую новую технологию, аналогичную уже используемой на вашем производстве, вряд ли можно распространить его обязательства о неразглашении и на информацию о данной разработке.

Важнейшим условием любого соглашения о конфиденциальности является срок его действия. Наиболее насущным является вопрос о том, действует ли соглашение о конфиденциальности и после прекращения действия трудового договора.

Соглашения о конфиденциальности служат для предотвращения утечки любой конфиденциальной информации, от производственных секретов до персональных данных. Его использование предусмотрено законодательством большинства развитых стран, а иски, с ним связанные, принимаются судами безоговорочно.

Характерной чертой конфиденциальных отношений является их документальное оформление. Отсюда возникает еще одна проблема – это вопрос о присвоении тому или иному документу соответствующего грифа конфиденциальности и разработке системы режимных мер, обеспечивающих защиту конфиденциальной информации. Анализ имеющихся отечественных и зарубежных публикаций позволяет ряду авторов рекомендовать применительно к предпринимательским структурам следующий подход. Ввести два грифа обозначения информации, относящейся к коммерческой тайне:

- «строго конфиденциально» – в случае, когда утрата (разглашение) информации создает предпосылки для возможных катастрофических последствий, чаще всего банкротства;

- «конфиденциально» – в случае, когда утрата (разглашение) информации наносит экономический или моральный ущерб предприятию, но не может привести к его гибели.

Вместе с тем, следует учитывать, что использование договоров о неразглашении коммерческой тайны – вовсе не самостоятельная мера по ее защите. Предложив сотруднику подписать такой договор, руководство фирмы предупреждает сотрудника, что в дело вступает целая система мероприятий по защите информации: правовых, организационных, технических. Договор, хотя и не исключает вовсе, тем не менее, закладывает правовую основу недопущения возможных противоправных действий. Принципиальным представляется также отражение вопросов соблюдения коммерческой тайны в договоре, заключаемом с руководителем фирмы при его избрании в установленном законом порядке на должность. Законом, руководителю предоставлены исключительные права в определении состава и содержания сведений, составляющих коммерческую тайну, и порядка их защиты. Вместе с тем, на него возлагаются определенные обязанности по надлежащему обеспечению сохранности коммерческой тайны и ответственность за состояние дел на этом участке.

Поэтому в договоре с руководителем предприятия целесообразно отразить следующее:

- необходимо обязать его строго хранить коммерческую тайну предприятия и не использовать ее для занятия любой деятельностью в ущерб предприятию;
- следует подчеркнуть, что руководитель предприятия несет персональную ответственность за создание необходимых условий для обеспечения сохранности коммерческой тайны предприятия;
- как и члены коллектива работников, руководитель предприятия должен быть предупрежден, что нарушение им требований, в части организации защиты коммерческой тайны и порядка ее защиты, может повлечь расторжение договора, а также уголовную, административную, гражданско-правовую ответственность в соответствии с действующим законодательством.

Наличие вышеперечисленных документов дает возможность говорить о наличии на предприятии юридически закрепленного порядка защиты коммерческой информации. Это открывает возможность принимать на себя обязанности по сохранению коммерческой тайны заказчика, относя ее к закрытой информации. При этом в договорах с заказчиком необходимо четко и однозначно указывать сведения, относящиеся к защищаемой информации. Владелец коммерческой тайны имеет право изменить или отменить режим коммерческой тайны, если это не нарушает принятых им на себя, при заключении соглашения о конфиденциальности или иного договора, обязанностей. При изменении или отмене режима коммерческой тайны, владелец коммерческой тайны обязан в письменной форме известить об этом конфиденцента коммерческой тайны, с которым имеется соответствующее соглашение или соответствующий договор. При ликвидации юридического лица – владельца коммерческой тайны, ликвидационная комиссия (ликвидатор) принимает решение о возможности и порядке дальнейшего использования и охраны информации, составляющей коммерческую тайну ликвидируемого юридического лица.

Основные результаты исследования

(I) Включению тех или иных данных о деятельности предприятия в перечень сведений, составляющих коммерческую тайну, должно предшествовать определение возможных отрицательных последствий их разглашения.

(II) Формами конфиденциальных отношений являются:

- отношения между сотрудниками и работодателем как юридическим лицом, возникающие с момента трудоустройства конкретного лица и продолжающиеся в течение всего периода его работы на данном предприятии;
- отношения между конкретным сотрудником и другими сотрудниками этого предприятия, складывающиеся и развивающиеся как по вертикали, так и по горизонтали;
- отношения между заказчиком и исполнителем, порожденные договором на выполнение работ или оказание каких-либо услуг.

(III) Разрешительная система должна отвечать следующим требованиям:

- распространяться на все виды классифицированных документов и изделий, имеющих на предприятии, независимо от их места нахождения и создания;
- определять порядок доступа всех категорий сотрудников, получивших право работать с коммерческой тайной, а также специалистов, временно прибывших на предприятие и имеющих отношение к совместным закрытым заказам;
- устанавливать порядок оформления разрешений на доступ к охраняемым документам и изделиям, позволяющий незамедлительно реагировать на изменения в области информации на предприятии;
- четко разграничивать права руководителей различных должностных уровней в

оформлении доступа соответствующих категорий исполнителей;

- исключать возможность бесконтрольной и несанкционированной выдачи документов и изделий кому бы то ни было;
- не разрешать лицам, работающим с классифицированной информацией и объектами, вносить изменения в учетные данные, а также подменять учетные документы.

(IV) Эффективная работа разрешительной системы, соответствующей ряду требований, возможна только при соблюдении определенных правил.

(V) Использование договоров о неразглашении коммерческой тайны – не самостоятельная мера по ее защите. Вместе с ними должна быть разработана система правовых, организационных и технических мероприятий по защите информации.

Список использованных источников:

1. Бачило И.Л., Лопатин В.М., Федотов М.А. Информационное право // СПб.: Юридический центр Пресс, 2001. – 789 с.
2. Кудрявцев Ю.В. Нормы права как социальная информация // М.: Юридическая литература, 1981. – 144 с.
3. Сергеев А.П. Право интеллектуальной собственности в Российской Федерации / Учеб. – 2-е изд., перераб. и доп. // М.: ООО «ТК Велби», 2003. – 752 с.
4. 15.02.2007. likums «Patentu likums» // Latvijas Vēstnesis, 34 (3610), 27.02.2007. [в силе с 01.03.2007.]
5. 06.04.2000. likums «Autortiesību likums» // Latvijas Vēstnesis, 148/150 (2059/2061), 27.04. 2000. [в силе с 11.05.2000.] с дальнейшими изменениями и дополнениями;
6. Соловьев Э. Коммерческая тайна и её защита // М.: ИВФ «Антал», 1996. – 64 с.
7. Методика выделения связей, составляющих коммерческую тайну предприятия // <http://www.dvgu.ru>
8. Договорное право / Под ред. проф. Брагинского М.И. и проф. Витрянского В.В. // М.: «Статут», 1998. – 480 с.
9. 20.06.2001. likums „Darba likums» // Latvijas Vēstnesis, 105 (2492), 06.07.2001., Ziņotājs, 15, 09.08.2001. [в силе с 01.06. 2002.] с дальнейшими изменениями и дополнениями;
10. Шаваев А.Г. Безопасность корпораций. Криминологические, уголовно-правовые и организационные проблемы // М.: Концерн «Банковский Деловой Центр», 1998. – 240 с.
11. Ярочкин В.И. Секьюритология – наука о безопасности жизнедеятельности // М.: Ось-89, 2000. – 399 с.
12. Уткин Э.А., Кочеткова А.И. Управление персоналом в малом и среднем бизнесе // М.: «Акалис», 1996. – 206 с.
13. Базаров Т.Ю., Ерёмкина Б.Л. Управление персоналом // М.: ЮНИТИ, 1998. – 560 с.
14. Мохорев А. Коммерческая тайна: понятие, режим, защита, ответственность за разглашение // доступно: http://kppn.avо.ru/index.php?option=com_content&view=article&id=43&Itemid=84

References:

1. Bachilo, I., Lopatin, V., Fedotov, M. Information law // St. Petersburg: Legal Center Press, 2001. – 789 p.
2. Kudryavtsev, Y. The rule of law as a social information // Moscow: Legal Books, 1981. – 144.p
3. Sergeev, A. Intellectual property rights in the Russian Federation: Study aid – 2nd ed., revised and enlarged edition // Moscow: Ltd. «TK Welby», 2003. – 752.p.
4. 15.02.2007. Patent Law // Latvijas Vēstnesis, 34 (3610), 27.02.2007. [in force from 01.03.2007] with further amendments;
5. 06.04.2000. Copyright Law // Latvijas Vēstnesis, 148/150 (2059/2061), 27.04. 2000. [in force from 11.05.2000] with further amendments;
6. Solovyov, E. Commercial secret and its protection // Moscow: IVF «Antal», 1996. – 64 p.
7. Method for detecting relations related to the company commercial secret // Available: <http://www.dvgu.ru>
8. Contract law / Edited by prof. Braginsky M. and prof. Vitryansky V. // Moscow: Statut, 1998.– 480p.
9. 20.06.2001. Labour Law // Latvijas Vēstnesis, 105 (2492), 06.07.2001., Ziņotājs, 15, 09.08.2001. [in force from 01. 06. 2002.] with further amendments;
10. Shavaev, A. Corporations safety. Criminological, legal and organizational problems // Moscow: Concern «Banking Business Center», 1998. – 240 p.
11. Yarochkin, V. Securitology – the science of safety // Moskow: Os-89, 2000. – 399 p.
12. Utkin. E., Kochetkova, A. Human resource management in small and medium business. // Moscow: «Akalis», 1996. – 206 p.
13. Bazarov, T., Eremina, B. Human resource management // Moscow: UNITY, 1998. – 560 p.
14. Mohorev, A. Commercial secret: conception, regime, protection, responsibility for disclosure // http://kppn.avо.ru/index.php?option=com_content&view=article&id=43&Itemid=84