

Коваль Игорь Александрович

Магистрант

Направление: Юриспруденция

Магистерская программа: Гражданское право, семейное право, международное частное право

Правовая концепция режима коммерческой тайны

Аннотация. Охрана коммерческой тайны является одним из актуальнейших вопросов в сфере обеспечения информационной безопасности. Большинство мер по защите конфиденциальной информации сводится к ее технической, а иногда даже физической защите. В данной статье рассматривается правовая основа защиты коммерческой тайны. Особое внимание уделено проблемам установления режима правовой охраны в организациях, а также привлечения работников и контрагентов к ответственности за его нарушение. Рассматриваются также особенности правовой защиты коммерческой тайны от посторонних лиц, не связанных с правообладателем договорными отношениями.

Ключевые слова: коммерческая тайна; информационная безопасность; режим правовой охраны; ответственность.

Коммерческая тайна – предмет правового регулирования Гражданского кодекса Российской Федерации, Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [1], Федерального закона от 29.07.2004 г. № 98-ФЗ «О коммерческой тайне» (далее – Закон № 98-ФЗ) и иных федеральных законов.

Согласно закрепленному в статье 3 Закона № 98-ФЗ определению, коммерческая тайна – это режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов,

сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду [3]. К информации, которая «требуется тишины», относятся имеющие коммерческую ценность сведения не только экономического, но также организационного и производственного характера. Секретная информация может храниться в организации на совершенно разных носителях – от простой бумаги до жестких дисков компьютеров.

Поскольку информационная система любой крупной компании представляет собой достаточно сложную структуру, приоритетная задача при внедрении новых подсистем – не нарушать ее функциональность. Исходя из этого, формирование системы информационной безопасности любой компании должно происходить поэтапно. Следует отметить, что защита одной из разновидностей конфиденциальной информации, такой как коммерческая тайна, не должна нарушать общей концепции информационной безопасности, выработанной на предприятии [4].

Юридическое оформление защиты коммерческой тайны в рамках общей защиты информации предприятия оформляется наиболее целесообразно следующим пакетом документов:

1. Типовое положение об информации на предприятии.
2. Положение о коммерческой тайне предприятия и правила ее хранения.
3. Приказ о присвоении сведений, составляющих коммерческую тайну предприятия.
4. Методика определения сведений, составляющих коммерческую тайну предприятия.
5. Служебная записка о включении информации в «Перечень сведений, составляющих коммерческую тайну предприятия».
6. Приказ об утверждении «Перечня сведений, составляющих коммерческую тайну предприятия».
7. Положение о разрешительной системе доступа сотрудников предприятия и представителей сторонних организаций к сведениям, составляющим коммерческую тайну предприятия.

8. Договор о защите коммерческой информации (о конфиденциальности).

9. Обязательства сотрудника предприятия о сохранении коммерческой тайны.

10. Обязательства (предупреждение) о сохранении коммерческой тайны при увольнении с предприятия.

11. Соглашение о конфиденциальности с посетителем предприятия.

12. Инструкция по организации и ведению на предприятии делопроизводства документов, содержащих коммерческую тайну.

Направления формирования эффективной системы защиты информационной безопасности компании будут недееспособными, если не будет учитываться человеческий фактор, который, как правило, и является угрозой для сохранения коммерческой тайны. Сотрудник компании является основной силой обеспечения действенности такой системы и, одновременно, ее основным разрушителем.

Для человека умение хранить секреты – одно из самых ценных качеств. Для компании в той же мере, критическое свойство сохранять корпоративные секреты.

А в масштабах общества сохранность коммерческой тайны равноценна глобальной безопасности. Информация имеет неограниченную ценность, именно поэтому каждый этап ее использования требует скрупулезной защиты [5]. Угрозы информационным системам подобны айсбергу. Его вершина – внешние угрозы: вирусы, хакерские атаки и спам, защиту от которых необходимо осуществлять практически на каждом предприятии. Однако под водой остается невидимая часть – внутренние угрозы: саботаж, похищение конфиденциальных данных, небрежное отношение к своим обязанностям. Около 80 % потерь, связанных с нарушением информационной безопасности, вызванной утечкой конфиденциальной информации, допущены внутри компании.

Стремительный рост риска утечки информации вызван серией корпоративных скандалов в связи с разглашением конфиденциальных данных.

Большинство таких инцидентов показало, что пробелы в физической безопасности бизнеса не являются результатом злонамеренной активности. В частности, чаще всего угрозу представляют сотрудники компании.

Итак, первый шаг, который необходимо сделать предусмотрительному бизнесмену, – разработать единое «Положение об охране коммерческой тайны» и ввести его в действие. К данному этапу нельзя подходить формально и лишь в общих фразах доводить до сведения сотрудников, какие данные могут стать достоянием общественности, а какие – нет. В этом случае при наступлении, так сказать, «страхового» события доказать, что тот или иной работник организации предоставил секретные сведения конкурентам, более чем затруднительно, а иногда просто невозможно [6]. Работник может избежать ответственности, заявив о своей неосведомленности о перечне данных, составляющих коммерческую тайну. Поэтому залог успеха – в четкости формулировок положения. В документе следует установить порядок доступа к конфиденциальной информации отдельных групп лиц, в том числе и представителей госструктур, имеющих законное право на ознакомление с «секретами фирмы». Совсем не лишним будет отразить в документе все мероприятия, касающиеся категорий учета, хранения и использования тайных сведений.

Ознакомить сотрудников с грамотно составленным «Положением о коммерческой тайне» – это полдела. Их знания необходимо перенести в правовое поле, т.е. предложить им подписать внимательно прочитанный документ.

Казалось бы, можно удовлетвориться и автографом работника в положении, однако некоторые компании предпочитают укрепить «броню». С этой целью в соответствии с положениями статьи 57 Трудового кодекса РФ они включают пункт, обязывающий сохранять конфиденциальные сведения в тайне, в трудовой договор сотрудника. В нем же следует прописать и обязанность нанятого специалиста вернуть при увольнении все документы, с помощью которых можно раскрыть коммерческую тайну [7].

Все бумажные документы, в которых содержатся сведения, составляющие коммерческую тайну, следует пометить специальным грифом «Коммерческая тайна» (или сокращенно КТ). Он располагается в правом верхнем углу и дополняется номером экземпляра. Аналогичную пометку необходимо разместить на электронных носителях конфиденциальных документов.

У определившей «правила игры» фирмы появляются все необходимые рычаги для того, чтобы привлечь к ответственности или заставить возместить ущерб сотрудников, нарушивших положение о коммерческой тайне. Незаконными можно считать те действия, которые были направлены на умышленное преодоление мер, принятых обладателем секретов по охране конфиденциальных сведений, если информацию получило лицо, знающее или предполагающее, что в его распоряжении оказались сведения, составляющие коммерческую тайну, а также если сотрудник предприятия, не имея полномочий на передачу данных, все же разглашает их.

В силу статьи 11 Закона № 98-ФЗ работник обязан выполнять установленный работодателем режим коммерческой тайны, не разглашать информацию, составляющую коммерческую тайну, обладателями которой являются работодатель и его контрагенты, и без их согласия не использовать эту информацию в личных целях, передать работодателю при прекращении или расторжении трудового договора, имеющиеся в пользовании работника материальные носители информации, содержащие информацию, составляющую коммерческую тайну.

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

Трудовой кодекс Российской Федерации указывает способы, которые организация может применять для защиты коммерческой тайны по отношению

к своим работникам. Например, в статье 81 ТК РФ указано, что работодатель имеет право разорвать трудовые отношения в случае, когда сотрудник разгласил охраняемую законом коммерческую тайну. Помимо Трудового кодекса РФ, информацию об ответственности за сбор, хранение и распространение сведений, составляющих коммерческую тайну, содержит Уголовный кодекс РФ. В частности, статья 183 УК РФ «Незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну» предусматривает наказание в виде лишения свободы на срок до 10 лет.

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

Организация не имеет права считать всю информацию, находящуюся в ее распоряжении, коммерческой тайной. Перечень информации, которая не может быть объявлена коммерческой тайной, закреплен в статье 5 Закона № 98-ФЗ. Так, в число общедоступной попала информация о численности или составе работников, системе оплаты и условиях труда на предприятии. Кроме того, свободный доступ должен быть обеспечен к данным о перечне лиц, имеющих право действовать без доверенности от имени юридического лица, к сведениям, изложенным в учредительных документах фирмы, а также к информации, обязательность раскрытия которой установлена соответствующими федеральными законами. Все данные, которые не попали в этот черный список, при желании владельцев бизнеса могут быть объявлены конфиденциальными [3].

Наличие заключенного трудового контракта между работником и работодателем со специальным разделом, посвященным правовому регулированию вопросов охраны сведений, составляющих коммерческую тайну, позволяет работодателю создать надежный механизм защиты фирменных секретов от посягательств со стороны действующего персонала

компании, а также бывших работников, прекративших свою деятельность по различным обстоятельствам.

Имея такие письменные договорные отношения, работодатель при возникновении конфликтов будет иметь возможность разрешить ситуацию, требуя привлечения к ответственности виновных за нарушение положений ФЗ «О коммерческой тайне». Согласно статье 14 указанного закона, за нарушение права на коммерческую тайну лицо, совершившее противоправное деяние, может быть привлечено к дисциплинарной, гражданско-правовой, административной или уголовной ответственности.

Следует также отметить, что для эффективного функционирования установленного режима коммерческой тайны необходимо вести учет всех лиц, имеющих доступ к информации, составляющей коммерческую тайну. В техническом обеспечении необходимо установить различный уровень доступа к информации, в том числе на уровне программного обеспечения организации.

Следует установить следующий порядок работы с конфиденциальными документами. Конфиденциальные документы должны обрабатываться в конфиденциальном делопроизводстве фирмы специально назначенным должностным лицом, ответственным за конфиденциальные документы. Конфиденциальные документы должны храниться в отдельном помещении в запираемых и опечатываемых шкафах. При этом допускается хранение конфиденциальных документов в общем делопроизводстве, но они обязательно должны находиться отдельно от других дел делопроизводства. Важными в данном случае также является архивное хранение таких документов и их уничтожение.

Вступая в деловые взаимоотношения с контрагентом, следует отдельным пунктом в соглашении оговорить условие неразглашения данных, составляющих коммерческую тайну.

В данном направлении хотелось бы отметить такую особенность при регулировании установленного режима коммерческой тайны, как взаимодействие с «внешними силами». Практически все коммерческие

организации сталкиваются с необходимостью взаимодействия с внешними персоналиями, например, это может быть потенциальный клиент. У организации нет трудового договора с ним о неразглашении коммерческой тайны или подписанного соглашения, как с контрагентом.

Как же защитить в этом случае коммерческую тайну?

Значение выражения «записанный разговор» известно многим по сюжетам сериалов о «лихих 90-х» и шпионским блокбастерам. Какая техника требуется для записи голосовых переговоров? Между прочим, этот прибор сейчас есть практически у всех – это сотовый телефон. Возможности сотового телефона, конечно, не безграничны, но достаточно широки – он дает устойчивый канал для связи с удаленным собеседником, имеется фото и видеокамера с неплохим разрешением, практически во всех моделях есть диктофоны, а емкость его памяти превышает десятки гигабайт. Сотовый телефон – идеальное устройство для хищения информации, именно по этой причине его изымают при входе в государственные объекты повышенной секретности.

Однако изъять частную собственность, а именно таковой является чей-то телефон, не имея на то законных оснований – чревато судебным разбирательством.

Никакие внутренние правила и распорядки частной организации не смогут повлиять на использование сотовых телефонов – пользоваться ими будут, а значит, вероятность кражи информации сохраняется постоянно [8]. Есть лишь один способ полностью исключить эту угрозу – подавитель сотовых телефонов. Это генератор помех, трансляция которых делает невозможной любую попытку связи по сотовому телефону. То есть в данном случае меры информационной безопасности сводятся только к техническим мерам.

С некоторого времени промышленный шпионаж стал приносить колоссальные доходы, практически все мировые корпорации готовы купить информацию о разработках конкурентов. Они прекрасно понимают, что эти расходы обернутся значительной прибылью в будущем. Необходимо прийти к

пониманию, что в бизнесе нет друзей и партнеров, которым можно было бы полностью доверять. Бизнес – это постоянное противостояние, а в этом деле, как известно, все средства хороши. Регулирование режима коммерческой тайны – одна из важнейших задач для любой солидной компании. В период экономического кризиса важность сохранения в тайне даже незначительных «секретов фирмы» значительно возрастает.

Установление правовых основ защиты коммерческой тайны и иной конфиденциальной информации, имеющей коммерческую ценность, является важным элементом юридического обеспечения предпринимательской деятельности.

В большинстве экономически развитых зарубежных стран законодательство, регулирующее правовой режим коммерческой тайны и устанавливающее ответственность за ее неправомерное использование, представляет собой весьма развитый нормативный массив, формирование которого осуществлялось на основе национальных правовых традиций, эволюционировавших в ходе развития правовых институтов.

В заключение хотелось бы отметить, что установление режима коммерческой тайны не должно стать самоцелью. Показателем эффективности установленного режима, грамотно осуществленного всеми возможными правовыми и техническими средствами, является не только исключение возможности утечки ценной информации, но и гарантия привлечения виновного лица к ответственности, если это все таки произошло. Необходимо помнить, что режим коммерческой тайны должен стать одним из элементов действующей политики информационной безопасности, занять свое место в системе защиты информации, не вступая в противоречие с общей системой функционирования организации. С этой целью при разработке и внедрении системы мер режима коммерческой тайны должны быть максимально учтены особенности и ресурсы организации, а также достигнуто оптимальное сочетание экономичности и результативности режима.

Литература

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Российская газета. 2006. № 165. 29 июля.
2. Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» // Российская газета. 2004. № 166. 5 августа.
3. Иванов Д.В. Источники правового регулирования конфиденциальной информации как условия трудового договора // Трудовое право. 2008. № 12.
4. Кауров В. Информационная безопасность в трудовых отношениях // Кадровик. Трудовое право для кадровика. 2009. № 8.
5. Колебошин Г.М. Обязанности работника в отношении коммерческой тайны работодателя // Трудовое право. 2007. № 5.
6. Коломиец А. Условие о неразглашении коммерческой тайны в трудовом договоре // Хозяйство и право. 2008. № 5.
7. Станскова У. Условие трудового договора об обеспечении секретности и конфиденциальности информации // Кадровик. Трудовое право для кадровика. 2010. № 10.
8. Шевердяев С.Н. Конституционно-правовой режим информации ограниченного доступа // Конституционное и муниципальное право. 2007. № 1.

© Бюллетень магистранта 2015 год № 6