ПРЕДОТВРАЩЕНИЕ ПОТЕРЬ КОММЕРЧЕСКИ ЗНАЧИМЫХ РАЗРАБОТОК И ПРЕЖДЕВРЕМЕННОГО РАСКРЫТИЯ ИЗОБРЕТЕНИЙ

Борис Прахов,
заведующий отделом промышленной собственности НИИ интеллектуальной собственности НАПрН Украины, главный редактор журнала «Теория и практика интеллектуальной собственности »

1. Предотвращение потерь коммерческих значимых разработок

Это разглашение сущности научно-технических разработок — совершение таких действий, после которых сущность объектов интеллектуальной собственности становится известной неограниченному числу лиц.

В связи с тем, что факты публикации приводят к разглашению новизны и утраты права на получение охранных документов должны осуществляться меры по предупреждению преждевременного разглашения.

Своевременное засекречивание созданной в компании информации на ранней стадии ее использования позволяет в дальнейшем при необходимости получить объект патентного или авторского права и иметь все преимущества, которые дает управление интеллектуальной собственностью. Поэтому предотвращение потерь коммерчески значимых секретов является важнейшим направлением политики компании в области интеллектуальной собственности.

В судебных спорах, связанных с коммерчески значимыми секретами, которые получают правовую охрану в Украине, как служебная и коммерческая тайна, суды во всех странах, проводя расследование, выясняют два основных вопроса:

1) существует ли служебная и коммерческая тайна;
2) действительно ли другая компания украла эту тайну или нечестно завладела ею.

При защите своих служебных и коммерческих тайн каждая компания должна иметь это в виду.

Процедуры и политика в области интеллектуальной собственности, тщательно спроектированные для компании, необходимы для того, чтобы удостовериться, что секреты оформлены согласно действующему законодательству, и чтобы помешать другим компаниям законными средствами узнать их.

Служебная и коммерческая тайны считаются существующими, когда объект охраны является секретным, ценным в силу его неизвестности за пределами компании и компания предпринимала формальные подтверждающие шаги для сохранения его в секрете.

Суды традиционно пользовались следующими критериями, чтобы определить, удовлетворяются ли эти юридические требования:

1) степень известности объекта охраны за пределами компании;
2) степень известности объекта охраны служащим и другим лицам, вовлеченным в компанию;
3) объем превентивных мер, принимаемых компанией для охраны секретности данного объекта;
4) ценность, которую объект представляет для самой компании и ее конкурентов;

5) объем усилий и денежных средств, затраченных компанией при разработке данного объекта;
6) степень легкости или трудности, с которой объект защиты может быть законно получен или дублирован другими компаниями.

Судебное разбирательство по делам о нарушении служебной или коммерческой тайны обычно включает в себя полемику о том, был ли объект охраны секретным и предпринимала ли компания формальные подтверждающие шаги для эффективного сохранения его в секрете. Объект охраны считается секретным, если он не является общеизвестным за пределами компании и не может легко стать известным конкурентам, пользующимся законными средствами. Абсолютная секретность здесь не требуется.

Чтобы сохранить объект в секрете, каждая компания обязана предпринимать формальные подтверждающие шаги. Что представляют собой эти шаги? Ответ на данный вопрос не столь очевиден. Простое «намерение» компании сохранить объект в качестве служебной и коммерческой тайн является недостаточным. Более того, не следование процедурам, установленным для охраны секретов, иногда может быть расценено хуже, чем отсутствие таких процедур вообще. По-этому формальные подтверждающие шаги должны состоять по крайней мере, в выполнении дополнительных мер предосторожности, помимо обыкновенных процедур использования. Примеры формальных подтверждающих шагов следующие:

1) ограничение доступа к ключевому оборудованию;
2) просвещение служащих на предмет существования секретов;
3) определение для каждого из служащих, какие фрагменты проектов, над которыми он работает, являются служебной и коммерческой тайнами;
4) предупреждение служащих о недопустимости раскрытия секретов;
5). закрытие доступа к инженерным записям и другой конфиденциальной информации;
6) требование, чтобы служащие подписывали соглашения о неразглашении;
7) выполнение требования, чтобы другие компании подписывали соглашения о неразглашении прежде, чем происходит раскрытие секретов;
8) гостевая политика.

Выполнение разнообразных процедур, предназначенных для предотвращения потери коммерческих секретов, является, возможно, лучшим формальным подтверждающим шагом, который компания в состоянии предпринять. Например, в одном случае было признано, что компания предпринимала достаточные формальные подтверждающие шаги по защите своих коммерческих секретов путем подписания служащими соглашений, соблюдения строгого режима секретности на предприятии, ограничения доступа к компьютерам.

Отсутствие таких шагов может привести к потере коммерческого секрета. Отсутствие формальных подтверждающих шагов для сохранения служебных и коммерческих тайн в секрете может быть проиллюстрировано на примере дела корпорации *Motorola* против корпорации *Fairchild.*

Пример

Motorola подала иск против *Fairchild* и своих бывших служащих, работавших позже на *Fairchild,* в связи с нечестным завладением коммерческими секретами. *Motorola* изначально заявила о похищении 140 коммерческих секретов, но позднее снизила это число до 10. Эти 10 коммерческих секретов имели отношение к производству двух дискретных транзисторных устройств — пластико-герме-

тичных TO-92 и TO-3 с алюминиевым корпусом.

Свидетельские показания выявили, что *Motorola* допускала проведение заводских экскурсий по всей производственной линии TO-92. На линии не было никаких знаков, предупреждающих о коммерческих секретах, не давалось никаких предупреждений тем людям, которые совершали экскурсии. *Motoro1a* ни от кого не требовала подписывать заявления или предоставлять расписки о неразглашении коммерческих секретов. Служащие *Motorola* иногда даже объясняли посетителям, как функционирует эта производственная линия. Другие свидетельства выявили, что *Motorola* позволяла репортерам из какого-то технологического журнала фотографировать производственную линию TO-92 для статьи. *Motorola* демонстрировала фильмы об этой производственной линии на коммерческих показах. Многие из коммерческих секретов также были раскрыты в патентах и публикациях.

Возможно, наиболее вредоносным в случае с *Motorola* был тот факт, что *Motorola* даже не знала, что именно она считает своими коммерческими секретами. Она никогда не имела записей, предметного указателя или списка, касающихся ее коммерческих секретов.

Основываясь на этих свидетельствах, суд отклонил иск *Motorola,* так как пришел к заключению, что корпорация не сделала никаких попыток к тому, чтобы определить свои коммерческие секреты и оберегать их.

Поэтому политика и процедуры в области интеллектуальной собственности необходимы еще и для того, чтобы подтвердить, что компания правильно определяет и документирует свои коммерчески значимые секреты, предпринимает формальные подтверждающие шаги к их сбережению. Это может очень пригодиться в судебном разбирательстве по данному поводу. После выяснения существования служебной и коммерческой тайн суд произведет исследование на предмет незаконности овладения коммерчески значимым секретом другой компанией. Считается, что компания нечестно овладела секретом, если она использовала для этого нечестные средства.

Овладение служебной и коммерческой тайнами нечестным способом предполагает такие действия, как кража, подкуп служащего в целях раскрытия коммерчески значимого секрета, мошенничество, электронный шпионаж и другие действия, например, нарушение контракта, которые являются недобросовестными в данных обстоятельствах.

Честные средства обнаружения служебной и коммерческой тайны следующие:

- разборка (вскрытие) изделия;
- независимое открытие;
- открытие после публичного рассекречивания (непреднамеренного или любого другого), произведенного владельцем коммерческого секрета.

В поиске ответа на вопрос, использовала ли компания честные или нечестные средства, суд выясняет, как обвиняемая компания фактически узнала о коммерчески значимом секрете, а не как она могла бы о нем узнать.

Компания обязательно должна проводить процедуры и политику в области охраны интеллектуальной собственности, коммерческих секретов, чтобы предотвратить кражу. К тому же, мероприятия по предотвращению потерь секретов могут способствовать уменьшению шансов для кого бы то ни было узнать об этих коммерческих секретах честными способами.

И все же, возможно, самую большую угрозу потери прав на служеб-

ную и коммерческую тайны представляют определенные действия владельца коммерчески значимого секрета, а не действия его конкурентов. Компания может потерять свои секреты, сделав их известными конкуренту вне зависимости от его поведения. Причиной может стать собственное поведение, например, когда один из служащих случайно раскрывает секрет, помещая его в публикуемую статью или распространяясь о нем на семинарах или выставках. В каждом таком случае неосторожность служащих, выражающаяся в публичном раскрытии коммерческого секрета, может привести к немедленной потере компанией его правовой охраны безотносительно к поведению конкурентов.

Еще один ключевой момент охраны коммерчески значимых секретов связан с увольняющимися служащими. Во многих отраслях служащие мигрируют от одного конкурента к другому, забирая с собой «багаж», полный частной информации. Часто они раскрывают, случайно или целенаправленно, своим новым работодателям секреты бывших работодателей. При этом новый работодатель часто является просто невинным получателем секрета. Поэтому, если какой-либо служащий увольняется, предотвращение раскрытия секретов становится трудновыполнимой задачей. Еще менее выполнимая задача — отстоять свои права на коммерчески значимый секрет перед новым работодателем. Общее правило гласит: невиновен новый работодатель, который получает коммерчески значимые секреты бывшего работодателя от своих новых служащих, не подозревая об этом. В таком случае новый работодатель не несет ответственности перед бывшим работодателем.

Процедуры и политика компании в области интеллектуальной деятельности должны осуществляться и для того, чтобы предостеречь бывшего служащего, а также его нового работодателя о том, что этому бывшему служащему известны служебные и коммерческие тайны компании. Такие процедуры и политика нацелены на прорыв линии защиты невиновного получателя секрета путем обоснования того, что обвиняемая сторона знала о существовании статуса служебной и коммерческой тайны у секретной информации.

Любое раскрытие служебных и коммерческих тайн партнеру или третьей стороне в деловых отношениях должно происходить под завесой конфиденциальности. Как правило, это достигается посредством выдвижения к другой компании требования подписать соглашение о конфиденциальности. Отсутствие вообще какого бы то ни было требования секретности по отношению к перспективному деловому партнеру может привести к потере компанией права на служебную и коммерческую тайну.

В одном из реальных случаев компания установила прототип блока для тестирования и предоставила инженерные чертежи этого блока одному из своих клиентов. Компания не предупредила клиента о том, что сам прототип и чертежи были конфиденциальными, а также не пометила чертежи знаком конфиденциальности. Кроме того, другим людям, не вовлеченным в деловые отношения, было позволено видеть данный прототип без каких-либо ограничений. Исходя из свидетельств, суд пришел к заключению, что компания не обладает никакими правами на служебную и коммерческую тайны, содержащиеся в технологии, воплощенной в прототипе и чертежах, так как эта компания никогда не обходилась с ними как с коммерчески значимыми секретами и не предпринимала никаких мер к охране их конфиденциальности.

Процедуры и политика в области интеллектуальной собственности необ-

ходимы, чтобы удостовериться в том, что соответствующее конфиденциальное соглашение было достигнуто прежде, чем произошло раскрытие материалов, относящихся к служебной и коммерческой тайнам.

Минпромполитики Украины разработало методические рекомендации по охране конфиденциальной информации, которые помогли собственнику такой информации создать детально проработанную программу, являющуюся частью общей системы превентивных мер по обеспечению экономической безопасности. В рекомендациях установлен следующий минимально возможный комплекс мероприятий, включаемых в программу по защите конфиденциальной информации:

1) наличие соглашений с работниками, в частности предусматривающих обязанность работников не разглашать конфиденциальную информацию работодателя;
2) наличие соответствующих соглашений или специальных положений в контрактах, предусматривающих защиту конфиденциальной информации, в договорах с заказчиками, исполнителями, консультантами и другими юридическими и физическими лицами, состоящими в договорно-правовых отношениях с собственником конфиденциальной информации и/или не являющихся его работниками;
3) наличие у собственника конфиденциальной информации инструкций, определяющих принципы отнесения информации к разряду конфиденциальной, порядок работы с конфиденциальной информацией и контроля за соблюдением установленного режима работы с конфиденциальной информацией.

В рекомендациях приводятся примерные соглашения, заявления работников и иные документы, содержащие обязательства по защите конфиденциальной информации. В подавляющем большинстве промышленно развитых стран соглашения подобного рода являются эффективным инструментом защиты конфиденциальной информации. Подобные соглашения между работником и работодателем заключаются либо параллельно с установлением трудовых отношений, либо с момента, когда работник получает доступ к конфиденциальной информации работодателя.

В Украине обязательства работников по неразглашению конфиденциальной информации могут быть оформлены либо в виде отдельных документов, включающих в себя любые не противоречащие законодательству условия соглашения, либо в трудовом договоре в соответствии с Кодексом законов о труде Украины, допускающий включение в трудовой договор условия о неразглашении охраняемой законом тайны (государственной, служебной, коммерческой и иной).

Следует иметь в виду, что соглашения такого типа обычно заключаются с работниками, которые в ходе выполнения своих трудовых (служебных) обязанностей на предприятии (в организации, учреждении и т. д.) имеют или получают доступ к технической, коммерческой или финансовой информации со статусом конфиденциальной либо сами создают такую информацию.

Ключевым элементом процесса передачи и использования конфиденциальной информации является договор о конфиденциальности и неразглашении, который позволяет применять самые различные подходы и их многочисленные комбинации с учетом целей договора, позиций сторон, специфики раскрываемой информации и особенностей национального законодательства.

Определяющим критерием необходимости заключения соглашения о конфиденциальности является тот факт, что в процессе выполнения трудовых

(служебных) обязанностей или определенных в договоре работ работник получает доступ к конфиденциальной информации или синтезирует информацию, которую необходимо сохранить в качестве конфиденциальной.

Российское законодательство не устанавливает каких-либо специфических условий, которые должны быть отражены в соглашениях о конфиденциальности. Работодатели и работники свободны в определении любых не противоречащих законодательству условий соглашения.

Соглашение о конфиденциальности может иметь достаточно простые структуру и содержание. Однако, принимая во внимание некоторую противоречивость законодательной базы данной области, предпочтительно достаточно подробно определить в трудовом договоре и соглашениях о конфиденциальности (неразглашении) взаимоотношения работника и работодателя по поводу конфиденциальной информации. При подготовке соответствующих положений трудового договора и соглашения о конфиденциальности следует принимать во внимание существующее законодательство, в частности общие положения о сделках и договорах.

Приведенные в рекомендациях примерные соглашения содержат лишь основные положения, направленные на урегулирование отношений между работодателем и работником с целью обеспечения необходимых мер по конфиденциальности информации. При приеме работника на работу с ним, помимо трудового договора, подписывается целый пакет самостоятельных соглашений, в частности соглашение о конфиденциальности.

Первым шагом в создании системы защиты коммерческой тайны на предприятии является составление документа (приказа или положения), устанавливающего границы коммерческой тайны во всех сферах деятельности организации, ответственных лиц, сроки актуальности секретной информации и меры наказания в случае разглашения секретов фирмы. После составления такого документа со всех работников предприятия нужно взять подписку о том, что сотрудник с ним ознакомлен и обязуется не разглашать секретные сведения в течение установленного срока актуальности информации.

Следующим шагом является выработка и реализация мер по предотвращению утечки информации. Они могут варьировать в зависимости от рода деятельности предприятия и строгости охраны коммерческой тайны. Необходимо:

- Подготовить приказ о хранении информации на общедоступном диске, регламентирующий правила хранения информации на электронных носителях и степень доступности информации для менеджеров различных уровней.
- Закрепить за всеми менеджерами, занятыми в продажах, конкретную область деятельности, в которой они обслуживают имеющихся и ищут новых клиентов. Все сведения о потенциальных клиентах (контактные лица, телефоны, даты и результаты встреч и телефонных разговоров, а также личные примечания менеджеров) должны заноситься в специальную базу данных, хранящуюся на сети. Ежемесячно менеджеры должны готовить отчеты о поиске новых клиентов в напечатанном виде, эти отчеты следует хранить в кабинете начальника отдела для обеспечения сохранности информации (клиентской базы данных) при увольнении персонала.
- Интегрированную программу по выписке счетов, наличию продукции на складе и т. п. написать

под интерфейс, несовместимый с Windows, для того чтобы обеспечить защиту информации от трансфера данных в другие программы MS Office, от копирования информации с базы данных и т. д. Или обеспечить эту защиту другим программным способом.

- Проследить за тем, чтобы на рабочих станциях (терминалах) продавцов не были установлены дисководы, для предотвращения копирования информации из базы данных.
- При увольнении менеджера или начальника отдела проводить сдачу-приемку дел. Причем передавать не только клиентскую базу, но и информацию обо всех неформальных отношениях, установленных с клиентом. Кроме того, увольняющийся менеджер должен не только в присутствии преемника обзвонить своих клиентов и представить им нового человека, но в некоторых случаях даже лично объехать VIP-клиентов и познакомить их с новым менеджером.
- При увольнении менеджера или начальника отдела конфисковать у него визитные карточки других организаций, полученные им во время работы на предприятии, и телефонные записные книжки.
- Для сотрудников, которым были предоставлены ноутбуки, создать специальные механизмы синхронизации данных. На все ноутбуки предприятия силами IT-отдела установить системы защиты от взлома и криптования информации. В результате даже потерянный или украденный ноутбук не станет источником утечки конфиденциальных данных: расшифровка информации, закрытой с использованием современных криптотехнологий (например, PGP), конечно, возможна, но требует очень серьезных материальных и технических ресурсов и под силу в настоящее время лишь государственным ведомствам и очень крупным корпорациям.

2. Предотвращение преждевременного раскрытия изобретений

Когда компании теряют свои патентные права, это происходит, как правило, по одной причине — из-за несоблюдения юридических требований, предъявляемых к патентоспособности согласно действующему законодательству. Многие компании без надобности утрачивают свои патентные права лишь из-за того, что они не разработали правильную политику и процедуры патентования.

Требование новизны при получении патента выявляет многочисленные препятствия для патентоспособности. Эти препятствия носят фатальный характер для попыток запатентовать изобретение, не позволяя выдать патент или делая недействительным патент, ошибочно предоставленный Патентным ведомством.

Препятствия для патентоспособности можно разделить на две группы:

- препятствия, причиной которых являются другие изобретатели;
- препятствия, причиной которых является компания-правообладатель.

Первая группа препятствий не позволяет компании получить патент, потому что изобретение уже было открыто в прошлом кем-то другим. В этом случае компания ничего не может изменить, так как сам ход событий «ставит крест» на патентовании.

Однако компания может предотвратить возникновение препятствий второй группы, называемых самовозведенными препятствиями для патентоспособности. Самовозведенные препятствия подконтрольны компании

и могут возникнуть из-за ее неосторожности или по причине отсутствия знаний о том, как функционирует патентное законодательство.

Например, патентный закон препятствует получению патента, если заявитель демонстрировал на выставке свое техническое решение более чем за полгода до подачи патентной заявки на изобретение. Сама компания создает во вред себе это препятствие для патентоспособности. Как не может компания позволять служащим добровольно овладевать собственностью, принадлежащей компании (например, компьютерами, мебелью, офисными принадлежностями), точно так же она должна защищаться от неосторожного «отбрасывания» или присвоения служащими прав интеллектуальной собственности, представляющих ценность для компании. Предотвращение возникновения непреднамеренных самовозведенных препятствий является основным видом предосторожности.

Первым самовозведенным препятствием для патентоспособности является печатная публикация, описывающая какую-либо технологию и в достаточной степени доступная публике, интересующейся этой технологией.

Печатная публикация состоит не только из напечатанного и опубликованного документа. Она включает в себя компьютерное хранение данных на диске и другие технологии хранения информации, восстановления и распространения данных. К печатным публикациям относятся:

- статьи в профессиональных или коммерческих журналах;
- дипломные работы;
- диссертации;
- газетные статьи;
- брошюры;
- микрофильмы;
- фотографии;
- данные, хранящиеся на компьютерном диске;
- производственные каталоги;
- рекламная информация.

Вторым препятствием для патентоспособности, которое может стать самовозведенным, является ***публичное использование,*** что определяется как любое использование изобретения, которое происходит без каких-либо ограничений или обязательств секретности перед изобретателем. Компания утрачивает патентные права на новую технологию, если она публично использует эту новую технологию или позволяет другой компании использовать ее без ограничения до подачи заявки на патент.

С другой стороны, компания может использовать эту новую технологию в секрете или позволить другой компании использовать эту же технологию, наложив ограничения секретности, не инициируя возникновения препятствий публичного использования.

Тот факт, что изображение спрятано от публики внутри механизма, не предотвращает наличия публичного использования, достаточно одного факта использования

Примеры ситуаций публичного использования:

- демонстрация прототипа группе потенциальных потребителей;
- предоставления образцов нового товара потребителю;
- испытание потребителями нового продукта;
- показ изобретения на коммерческих шоу;
- попытки продать товар, который подлежит патентованию;
- распространение рекламных брошюр, описывающих изобретение;
- показ фотокопий или фотографий перспективным покупателям;
- детальное обсуждение изобретения во время коммерческих показов;
- контрактное предложение, которое детализируется изобретением.
- распространение образцов;

- продажа товара, изготовленного с помощью патентоспособной технологии, даже если эта технология не является публично известной.

В большинстве стран патентное законодательство предъявляет строгие требования к новизне, и патентоспособность в этих странах заранее исключается, если любое публичное раскрытие имело место до подачи патентной заявки, в отличие от патентного законодательства Соединенных Штатов Америки, которое предоставляет изобретателю 12-месячный льготный период для подачи патентной заявки после публичного использования или продажи. Одни страны предоставляют более короткий срок после раскрытия содержания патентной заявки, другие страны вообще не предоставляют такого льготного срока, в большинстве стран любое публичное раскрытие до подачи патентной заявки автоматически уничтожает возможность получения иностранных патентных прав.

Случайно возникают ситуации, когда две компании независимо друг от друга разрабатывают одну и ту же новую технологию. Если ни одна компания не знает о разработках другой компании, то каждая из них может подать патентную заявку на свою технологию, заявляя эту технологию как свою собственную. Однако патентное законодательство допускает предоставление только одного патента на одно изобретение. Таким образом, лишь одна компания получит патентные права. В Украине получит та компания, которая первой подаст заявку на изобретение в Патентное ведомство. В США Патентное ведомство решает, какая из компаний первой изобрела эту новую технологию, и присваивает первенство в изобретении той компании, которая докажет, что ее изобретение сделано раньше, чем у компании-конкурентки. ◆

Список использованной литературы

1. *Андрощук Г.О. Захист комерційної таємниці / Г.О.Андрощук [та ін.]. — К., 2000*
2. *Андрощук Г.А. Какие сведения могут составлять коммерческую тайну / Г.А. Андрощук, Л. Вороненко. — Бизнес информ, 1999. — № 9–10*
3. *Беляков Е.Б. Защитить действительного творца.*
4. *Гасанов Р.М. Промышленный шпионаж на службе монополий. // М.:Вопросы изобретательства, 1990.*
5. *Меньшиков А.А. Правовые вопросы передачи ноу-хау в международной торговле / А.А.Меньшиков — М. : МИГПАН, 1993.*
6. *Максименко В.Г. Предприниматель в опасности: способы защиты (практическое руководство для предпринимателей бизнесменов) / В.Г.Максименко, Н.И.Шиян — М., 1992.*
7. *Прахов Б.Г. Последствия нарушений прав патента-владельца / Б.Г.Прахов // Предпринимательство, хозяйства и право —1997 — № 6.*
8. *Свинсон Б. Экономическая преступность / Б.Свинсон. — М. : Прогресс, 1997.*
9. *Тыцкая Г.И. Споры о недействительности патента в праве зарубежных стран / Г.И. Тыцкая — М. : ВНИИПИ, 1998.*