О.В. Мосин.

Предпринимательская тайна и правовая защита информации

ПЛАН:

1. ВВЕДЕНИЕ.

По мнению западных теоретиков-экономистов, успешное развитие предпринимательство существенно зависит от той политико-экономической среды (командно-административной или рыночно-конкурентной), в которой оно осуществляет свою деятельность. Представляется, что подобный взгляд в сфере предпринимательского права и хозяйствования следует признать в качестве основополагающего фактора.

Однако не менее важным фактором, постоянно сопутствующим определенной экономической среде, является криминогенная и иная, затрудняющая или сводящая на нет действия предпринимателя, обстановка. Наличие условий, при которых создается реальная угроза причинения вреда (ущерба) субъектом хозяйствования, ставит в ряд первоочередных и долговременных задач, требующих оперативного решения, проблему обеспечения экономической безопасности.

Многие вопросы предпринимательской деятельности регулируются и обеспечиваются гражданским, административным, трудовым, авторским, уголовным и другим законодательством. Вести же речь о том, что с помощью только правового регулирования и охраны можно решить все проблемы, связанные с обеспечением безопасности предпринимательства, не только преждевременны, но и, как показывает практика, не осуществимы в обозримом будущем.

В рыночно-конкурентных условиях возникает масса проблем, связанных с обеспечением безопасности не только физических и юридических лиц, их имущественной собственности, но и предпринимательской (коммерческой) информации, как вида интеллектуальной собственности. Для защиты предпринимательских информационных потоков от различного рода посягательств используются как правовые, так и специальные меры, а в необходимых случаях комплексное их применение.

Совокупность сведений, циркулирующих в предпринимательской деятельности, в целях их уяснения, можно условно сгруппировать по направлениям:

1. Предпринимательская (коммерческая) информационная система (сведения о состоянии экономической системы, факторах, положительно или отрицательно влияющих на ту сферу хозяйствования и коммерции, в которой действует предприниматель);

2. Правовая информационная система (сведения о действующем законодательстве, регулирующем и охраняющем деятельность предпринимательских (коммерческих) структур);

3. Специально-оперативная информационная система (сведения о

способах, силах и средствах обеспечения безопасности предпринимательской информации от доступа третьих лиц).

Структура. Первые две информационные системы рассмотрены в разделе “Общие вопросы защиты предпринимательской информации”, а третью - в разделе “Специальные вопросы защиты предпринимательской информации”.

2. ОБЩИЕ ВОПРОСЫ ЗАЩИТЫ ПРЕДПРИНИМАТЕЛЬСКОЙ ИНФОРМАЦИИ.

Предпринимательская (коммерческая) деятельность тесно взаимосвязана с получением, накоплением, хранением, обработкой и использованием разнообразных информационных потоков. Возникает вопрос: вся ли эта информация подлежит защите или только отдельные ее группы? Если же для защиты выделяется только определенная группа информации, то по каким критериям (свойствам) ?

Отвечая на поставленные вопросы, следует подчеркнуть, защите подлежит не вся информация, а только та, которая представляет ценность для предпринимателя. При определении ценности предпринимательской информации необходимо руководствоваться такими критериями (свойствами), как полезность, своевременность и достоверность поступивших сведений.

Полезность информации состоит в том, что она создает субъекту выгодные условия для принятия оперативного решения и получения эффективного результата.

В свою очередь, полезность информации зависит от своевременного их доведения (получения) до субъекта предпринимательства. Например, из-за несвоевременного поступления полезных по своему содержанию сведений упускается возможность заключить выгодную торговую или иную сделку. Результат - время упущено, информация теряет свою полезность.

Критерии полезности и своевременности тесно взаимосвязаны и взаимозависимы с критерием достоверности оцениваемой информации. Недостоверные сведения сводят к нулевому эффекту своевременность и кажущуюся их полезность для субъекта предпринимательства. При этом сам факт (например, желание конкретного лица заключить договор купли-продажи) может существовать реально, тогда как сведения о нем содержат искаженное представление. Причины возникновения недостоверных сведений различны: неправильное восприятие (в силу заблуждения, недостаточного

опыта или профессиональных знаний) источникам факта или умышленное, с определенной целью, искажение о нем сведений. Как правило, сведения, представляющие интерес для предпринимателя, а также источник их поступления должны подвергаться перепроверке.

Можно сослаться еще и на такой критерий, как полнота информации. Однако вести речь о том, насколько полна информация о конкретном объекте (факте) и где ее границы, довольно затруднительно и, к тому же, малоэффективно. В предпринимательской деятельности этот критерий особой роли не играет.

В итоге, субъект оценки предпринимательской информации, ее владелец (собственник), на основании совокупности перечисленных критериев, определяется ценность поступивших сведений для своей хозяйственной деятельности и принимает по ним оперативное решение.

Кстати, в зарубежной экономической литературе предпринимательская информация рассматривается не в качестве средства достижения положительного результата (прибыли), а прежде всего условия, способствующего или препятствующего его наступлению. Особо подчеркивается наличие стоимостного фактора предпринимательской информации, т.е. выступать в качестве предмета купли-продажи. Например, отдельные ведомства командно-административной системы достаточно профессионально учитывали и использовали фактор стоимости информации в своих интересах.

Определение стоимости тех или иных сведений требует дифференцированного подхода. В одних случаях, дешевле обойдется метод собственных проб и ошибок, в других же, целесообразнее получить (купить) информацию о том, как избежать подобных ошибок, а в-третьих, как сохранить ценную информацию от доступа посторонних лиц, чтобы не потерять ее стоимость, а следовательно, ожидаемую от нее результативность. Факт утечки информации напрямую связан с падением ее ценности для лица, из владения которого она вышла.

Важное значение в условиях развития многообразных форм собственности имеет вопрос определения принадлежности информации на правах интеллектуальной собственности конкретному субъекту предпринимательства, а в итоге наличия у него правомочий на ее защиту.

Закон РФ регламентирующий предпринимательскую деятельность предусматривает, что владельцами (собственниками) предпринимательской информации, как интеллектуальной собственности, могут быть граждане России, граждане иностранных государств, лица без гражданства, а также объединения граждан -

коллективных предпринимателей.

В области внешнеэкономической деятельности предпринимательство осуществляется в форме смешанных предприятий (СмП) - участвуют предприятия двух и более стран на долевом формировании капитала; совместные предприятия на территории Российской Федерации (СП) - участвуют одно или несколько отечественных предприятий и одна или несколько иностранных компаний. Предполагаются и другие формы совместного предпринимательства.

Обширны и направления предпринимательской деятельности. Это внутренние и внешние экономические сферы производственной, посреднической, коммерческой, научно-технической, инвестиционной, сервисной деятельности.

Если подвести итог краткому анализу, то можно убедиться, что субъекты предпринимательства, формы и направления их деятельности далеко не равнозначны, а следовательно, и информационные потоки, циркулирующие в этих сферах, не равноценны. Так, государственные предприятия, занимающиеся предпринимательской деятельностью, могут обладать сведениями, определяемыми как государственные или служебные секреты.

Информация государственных режимных предприятий (учреждений), в зависимости от степени важности (ценности), подразделяется на сведения, составляющие:

- ***государственную тайну;***
- ***военную тайну;***
- ***служебную тайну;***
- ***иные сведения, не составляющие тайны, но представляющие интерес для иностранных спецслужб.***

Наряду с режимными мерами, безопасность государственных секретов обеспечивается также нормами уголовного закона.

Уголовная ответственность за расглашение государственной тайны преедусмотрена в новом Уголовном Кодексе РФ 1996 г.

Защита государственной секретной информации возложена на сотрудников режимных служб и правоохранительных органов (ст. 126 УПК РФ).

Обеспечение безопасности государственной интеллектуальной собственности под грифом “сов. секретно”, “секретно” не имеет прямого отношения к защите частной предпринимательской информации. Однако следует указать на некоторые исключения. В случае, если спецслужба иностранного государства проявит интерес к получению определенной предпринимательской информации, то наряду с другими мерами оказывать ей противодействие будет и контрразведка. Под защиту специальных органов государства

может быть взята предпринимательская информация, оцененная как особо важная не только для ее частного собственника, но государства, когда не исключено, что к ней может проявить интерес иностранная спецслужба. Вопрос о подобной защите должен решаться на договорной основе между предпринимателем и органом федеральной безопасности с обозначением пределов и функций профессиональной деятельности последних.

Что касается основной массы предпринимательской информации, то она подобной уголовно-правовой, оперативно-следовательной и режимной защитой не обладает и не пользуется.

В гражданском законодательстве, тем не менее, предпринята попытка узаконить предпринимательскую (коммерческую) информацию в качестве защищаемой.

Воспроизведем статью 139 части первой Гражданского кодекса Российской Федерации, называющейся: ***“Служебная и коммерческая тайна”:***

1. 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. Сведения, которые не могут составлять служебную или коммерческую тайну, определяются законом и иными правовыми актами.

2. Информация, составляющая служебную или коммерческую тайну, защищается способами, предусмотренными настоящим Кодексом и другими законами.

Лица, незаконными методами получившие информацию, которая составляет служебную или коммерческую тайну, обязаны возместить причиненные убытки. Такая же обязанность возлагается на работников, разгласивших служебную или коммерческую тайну вопреки трудовому договору, в том числе контракту, и на контрагентов, сделавших это вопреки гражданско - правоввому договору.

По существу в пункте 1 вышеизложенной статьи законодатель дал определение понятию “коммерческая тайна”.

Таким образом, можно сделать следующие выводы:

- ***субъектом оценки предпринимательской (коммерческой) информации является ее владелец (собственник);***
- ***поступившие сведения и их источник подлежат обязательной перепроверке;***
- ***ценность информации определяется с помощью таких критериев (свойств), как полезность, своевременность и достоверность;***

- ***предпринимательская информация в зависимости от ценности имеет свою стоимость;***
- ***информация подлежит защите при условии, что ценность информации зависит от сохранности в тайне от третьих лиц, доступ к информации закрыт на законном основании, обладатель информации принимает надлежащие меры по ее охране;***
- ***использование правовой системы позволяет предпринимателю правильно отделять частную информацию от сведений, составляющих государственные секреты, и не допустить конфликта с действующим уголовным правом.***

3. СПЕЦИАЛЬНЫЕ ВОПРОСЫ ЗАЩИТЫ ПРЕДПРИНИМАТЕЛЬСКОЙ ИНФОРМАЦИИ.

Приступая к рассмотрению третьей группы сведений, относящихся к специально-оперативной (т.е. наличия способности быстро что-либо осуществить на практике) информационной системе, следует отметить, что она направлена на защиту не всей предпринимательской информации, как отмечалось уже выше, а только к особо выделенным, ценным сведениям.

Предпринимательская информация, циркулирующая в рыночно-конкурентной сфере деятельности, подразделяется на

- ***техническую,***
- ***организационную,***
- ***коммерческую,***
- ***финансовую,***
- ***рекламную, о спросе-предложении, конкурентах, криминальной обстановке и др.***

Прежде чем принимать меры к защите определенной информации, необходимо уточнить следующие вопросы:

1. ***Какие сведения нельзя скрывать, защищать от доступа к ним (от кого?);***
2. ***Какие сведения невыгодно скрывать (почему?);***
3. ***Какие сведения подлежат охране (кем и от кого ?).***

Ответ на первый вопрос дало российское правительство в своем постановлении ***"О перечне сведений, которые не могут составлять коммерческую тайну".*** К ним относятся:

- ***организационные сведения (устав и учредительные документы предприятия, регистрационные удостоверения, лицензии, патенты);***
- ***финансовые сведения (документы об исчислении и уплате налогов, других платежей, предусмотренных законом, документы о состоянии платежеспособности);***
- ***сведения о штате и условиях деятельности (число и состав работающих, их заработная плата, наличие свободных мест, влияние производства на природную среду, реализация продукции, причиняющей вред здоровью населения, участие должностных лиц в предпринимательской деятельности, нарушение антимонопольного законодательства);***
- ***сведения о собственности (размерах имущества, денежных средствах, вложениях платежей в ценные бумаги, облигации, займы, в уставные фонды совместных предприятий).***

Не вполне определенным остается вопрос о том, кому предприниматель обязан предъявлять по требованию перечисленные сведения? Вместе с тем, исходя из характеристики информации, можно предполагать, что претендовать на ознакомление с этими сведениями могут в пределах своей компетенции:

- ***прокурор в порядке надзора и в других случаях, предоставленных ему законом;***
- ***правоохранительные органы по возбужденному уголовному делу;***
- ***налоговые службы (управления);***
- ***аудиторские фирмы (по просьбе самого владельца);***
- ***профсоюзы;***
- ***государственные предприятия (учреждения);***
- ***санэпидемстанции;***
- ***экологические организации;***
- ***предпринимательские предприятия и частные лица, вступающие с ним в сделку.***

Данный перечень не является исчерпывающим.

Указанные сведения не являются предметом защиты от ознакомления с ними третьих лиц, но это не исключает их охраны от уголовных преступлений.

Вторая группа сведений характеризуется тем, что ее невыгодно скрывать от

окружения самому предпринимателю. Это касается прежде всего рекламной информации. Без рекламы в хозяйственной деятельности трудно добиться эффективного результата, особенно в условиях жесткой конкуренции. Практически реклама широко начинает входить в нашу жизнь. Однако пропаганда и широкое распространение рекламы имеют не только положительную, но и отрицательную сторону для предпринимателя. Суть в том, что рекламная информация становится достоянием не только законопослушных граждан (на которых она и рассчитана), но и преступных элементов. Предпринимательская информация, рекламируемая в газетах, в журналах, по телевидению, радио помогает преступникам выйти на обьект будущего посягательства, изучить его слабые (уязвимые, например, для закона отдельные виды деятельности, различного рода махинации) стороны, а затем принять решение, каким способом получить для себя от него выгоду.

Предприниматель, рекламирующий свою деятельность, должен быть готов к возможному посягательству и своему ответному действию. Некоторые из них, в подобных ситуациях, пытаются найти защиту от преступников у таких же преступников, но из другой группировки. В итоге, запутавшись с преступным миром, попадают под их полное влияние, а иногда лишаются своих предприятий (фирм).

Целесообразнее все же защиту искать не у тех же преступников, а в службах по борьбе с организованной преступностью (милиции или органов госбезопасности), частных сыскных организациях.

Что касается предпринимательства в сыскной сфере деятельности, то она начинает получать достаточное освещение в прессе, включая интервью отдельных сотрудников об оказываемых услугах (кому и в каких случаях).

Кстати, в Великобритании частным детективным службам запрещается рекламировать оказываемые ими услуги в средствах массовой информации. Единственным источником, рекламирующим их деятельность, является, специально издаваемый в этих целях, справочник.*

Итак, предприниматель, рекламирующий свою деятельность, должен знать, с какими препятствиями он может столкнуться, и как он сможет их преодолеть в своей конкретной ситуации. Не выход из данного положения и конспирация предпринимательской деятельности, как пытаются это делать некоторые фирмы. Без клиентуры, в зависимости от видов хозяйствования, они не будут иметь необходимой прибыли. Выход один - обеспечить свою безопасность с помощью государственных и частных форм защиты.

К третьей группе сведений относятся те, которые представляют хозяйственную ценность для предпринимателя, и на них не распространяется законный доступ третьих

лиц. С понятием ценной информации мы уже определились. Проблема состоит в том, кто и как должен обеспечить сохранность информации.

Если обратиться к законодательным актам, то ни один из них не ставит прямо под свою защиту данный вид собственности. Если допустить, что такая норма имелась бы, например, в уголовном кодексе, то это еще не говорило бы о том, что предпринимательская информация надежно запрещена. Наличие нормы предполагает, что в случае нарушения содержащегося в ней запрета, виновный понесет соответствующее наказание. Положительным в плане предупреждения такого преступления служил бы еще сам факт наличия такой нормы, т.е. запрет на совершение указанного действия, ибо за него наступит ответственность. Действующее законодательство подобных условий пока не создает.

4. ПОРЯДОК ОТНЕСЕНИЯ СВЕДЕНИЙ К КОММЕРЧЕСКОЙ ТАЙНЕ ПРЕДПРИЯТИЯ.

В данном разделе мы будем употреблять только термин “коммерческая тайна”, так как действующее законодательство оперирует именно им и не упоминает термина “предпринимательская тайна”.

Первым вопросом, который необходимо решить при организации охраны коммерческой тайны, является определение круга сведений, составляющих коммерческую тайну, а также возможное распределение их по категориям важности в зависимости от их ценности для предприятия, характера и размера ущерба, который может быть нанесен предприятию при разглашении этих сведений. К решению этой проблемы следует подходить особенно тщательно. Если какие-либо данные, прямые или косвенные, будут упущены из внимания, то все принимаемые меры могут оказаться неэффективными. С другой стороны, излишние меры по ограничению доступа к информации осложнят работу и приведут к неоправданным экономическим издержкам. Правильная организация выделения и защиты коммерческой тайны должна не только не мешать работе предприятия, но даже способствовать его прибыльной деятельности.

При этом сведения, составляющие коммерческую тайну предприятия, отражаются в ***“Перечне сведений, составляющих коммерческую тайну предприятия”*** (далее Перечень), утверждаемом руководителем предприятия. При разработке Перечня необходимо учитывать требования ***постановления Правительства Российской***

Федерации от 5.12.91г. №35 "О передаче сведений, которые не могут составлять коммерческую тайну".

Юридическая практика показывает, что данный вопрос лучше решать коллегиально. Для разработки Перечня приказом руководителя предприятия создается комиссия из наиболее квалифицированных и компетентных специалистов основных подразделений и представителей службы безопасности (или РСО).

Для подготовки перечня сведений, относящихся к коммерческой тайне предприятия, целесообразно привлечь наиболее компетентных специалистов, знакомых как с деятельностью предприятия в целом, так и с работой отдельных подразделений. Создается группа в составе не более 4-5 человек, в которую желательно включить:

- ***специалиста, владеющего финансовыми вопросами, конъюнктурой рынка и данными в отношении конкурирующих фирм;***
- ***специалиста, полностью представляющего систему организации работы предприятия, ее особенности;***
- ***специалиста, по связям с другими предприятиями, а также по вопросам заключения контрактов, договоров;***
- ***специалиста, обладающего всеми сведениями о выпускаемой продукции, технологическом цикле ее практикования и производства, о прохождении всех видов информации (устной, документальной, в виде образцов, узлов, блоков, готовой продукции).***

Если предприятие достаточно велико или производимая продукция имеет разнородный характер, можно создать несколько таких групп: одну - главную, в целях координации и обобщения результатов работы, остальные в зависимости от необходимости по каждому отдельному участку.

С другой стороны, не исключено, что предприятие может состоять лишь из нескольких человек, особенно на первых этапах. Тогда, действительно, указанную задачу способен решить один руководитель, при условии, что он будет владеть перечисленной выше информацией. Но все же, во избежание субъективных ошибок, лучше рассматривать эти вопросы как минимум вдвоем.

Как уже сказано, в группе должны быть руководящие специалисты, обладающие полным объемом данных, которые могут быть отнесены к коммерческой тайне. Однако это не означает, что следует обязательно знакомить всех привлекаемых экспертов с конкретными сведениями, могущими представлять коммерческую тайну, если ранее они эти сведения не знали. В большинстве случаев достаточно, если хотя бы один из них осведомлен в деталях по отдельному рассматриваемому вопросу, а остальные

представляют себе общий характер. Такой подход сделает работу группы более рациональной и исключит уже на первом этапе возможные предпосылки к необоснованному распространению коммерческой тайны.

Далее, перед группой экспертов необходимо поставить комплекс вопросов в следующей последовательности:

а) выделить все виды деятельности предприятия, приносящие прибыль на данный момент;

б) исходя из имеющихся данных о рынке сбыта, оценить превышает ли уровень прибыли для данного вида деятельности аналогичные показатели у других предприятий;

в) определить вероятную перспективу рентабельности этой деятельности.

Если с экономической точки зрения вид деятельности устраивает предприятие в данный момент и в перспективе, а прибыль выше, чем у конкурирующих фирм, то предприятие располагает определенной коммерческой тайной и необходимо продолжить анализ.

В этом случае эксперты должны определить, что именно в данном виде деятельности позволяет получать прибыль. Примеры могут быть самыми различными.

Так, для сведений научного характера - это, как правило:

- ***идеи, изобретения, открытия;***
- ***отдельные формулы;***
- ***новые технические проекты;***
- ***новые методы организации труда и производства;***
- ***программное обеспечение ЭВМ;***
- ***результаты научных исследований.***

Для сведений технологического характера:

- ***конструкторская документация, чертежи, схемы, записи;***
- ***описания технологических испытаний;***
- ***“ноу-хау”;***
- ***точные знания конструкционных характеристик создаваемых изделий и оптимальные параметры разрабатываемых технологических процессов (размеры, обьемы, конфигурация, процентное содержание компонентов, температура, давление, время и др.);***
- ***сведения о материалах, из которых изготовлены отдельные детали, условиях экспериментов и оборудовании, на котором они проводились и т.д.;***

- ***используемые предприятием отдельные новые, либо уникальные измерительные комплексы и приборы, станки, оборудование.***

Для сведений делового характера:

- ***сведения о заключенных или планируемых контрактах;***
- ***данные о поставщиках и клиентах;***
- ***обзоры рынка, маркетинговые исследования;***
- ***информация о конфиденциальных переговорах;***
- ***калькуляция издержек производства предприятия, структуры цен, уровень прибыли;***
- ***планы развития предприятия и его инвестиций.***

Если в выделении узловых сведений возникают проблемы, то можно изучить рассматриваемый вид деятельности по отдельным технологическим этапам, по логическому алгоритму действий, по временным отрезкам. В любом случае полезными будут аналогичные примеры организации защиты секретов западными фирмами.

Так, крупнейшие в мире производители прохладительных напитков фирмы “Кока-Кола” и “Пепси-Кола” выделяют в качестве главных секретов специальные добавки в концентрат, из которого изготавливаются напитки. Американские машиностроительные и приборостроительные фирмы, широко рекламируя высокие качественные характеристики своей продукции, держат в глубоком секрете технологические особенности изготовления основных узлов, определяющих данные характеристики.

Следует учесть и другие факторы. Например, предприятие может применять широко известные методы организации производства, технологические приемы, оборудование и т.п. и при этом достигать высокой прибыли. Несмотря на общедоступность таких данных, сам факт их применения может являться коммерческой тайной.

Некоторые предприятия получают прибыль за счет монопольного положения на рынке, т.е. отсутствия производителей такого же вида товара в данном регионе. Не следует в этом случае пренебрегать своевременными мерами по защите коммерческой тайне, т.к., используя свободный доступ к необходимым данным, даже небольшое предприятие способно быстро организовать аналогичное производство и составить конкуренцию.

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.

При наличии таких сведений на первом, титульном листе в правом верхнем углу должен быть поставлен гриф. Например, “коммерческая тайна”.

Исключение сведений из категории составляющих коммерческую тайну предприятия производится по окончании контрольного срока, на который она устанавливалась или ранее, в связи с наступлением определенных обстоятельств (появление нового образца, утечка информации к конкуренту и т.п.).

Решение о досрочном исключении сведений из категории составляющих коммерческую тайну предприятия производится по окончании контрольного срока, на который она устанавливалась или ранее, в связи с наступлением определенных обстоятельств (появление нового образца, утечка информации к конкуренту и т. п.).

Решение о досрочном исключении сведений из категории, составляющих коммерческую тайну, принимаются теми же лицами, которые утвердили Перечень.

В основе этой системы должна лежать заинтересованность исполнителей работ как в выявлении новых обьектов защиты, так и в определении оптимального момента снятия ограничений на распространение ранее защищаемой информации.

В тех случаях, когда публикация необходима для закрепления приоритета или поддержания престижа советской науки, вместо конкретных приводятся сведения более общего характера. Например, точные значения характеристик и параметров могут быть заменены на диапазоны, в которых они находятся.

При открытом опубликовании сведений рекомендуется уделять больше внимания рекламной привлекательности ее результатов, чтобы заинтересовать в их использовании потенциальных потребителей внутри страны и за рубежом. Вместе с тем обьем публикуемых данных не должен быть достаточным для самостоятельного внедрения без дополнительной информации разработчика, которая именно и подлежит защите.

5. РЕЖИМНЫЕ МЕРЫ, НАПРАВЛЕННЫЕ НА ПРЕДОТВРАЩЕНИЕ УТЕЧКИ СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ ПРЕДПРИНИМАТЕЛЬСКУЮ (КОММЕРЧЕСКУЮ) ТАЙНУ.

Основным фактором, способствующим защите информации, остаются пока режимные. т.е. специальные меры, направленные на предотвращение утечки конкретных сведений. Чем больше к ним может быть проявлен или уже фиксировался интерес, тем оперативнее должны приниматься меры по недопущению его удовлетворения.

Принятие специальных мер, направленных на защиту интеллектуальной собственности, зависит прежде всего от владельца (владельцев) информации, складывающейся в их среде деятельности конкурентной обстановки, ценности, которую представляет для них производственная или коммерческая информация, и других факторов.

Безусловно, хранить секрет его владельцу, если он больше никому не известен, не представляет большой сложности и затрат на его охрану. Он сам не должен допустить к нему третьих лиц. При этом не быть болтливым, доверчивым. Носитель информации (документ, дискета, предмет) должен иметь соответствующее место хранения (не письменный стол, а сейф или другое недоступное для других лиц место). Несколько усложняется охрана этих сведений, когда о ее наличии становится известно заинтересованным лицам. Возникает необходимость ограничивать доступ посторонних лиц к месту хранения секретных материалов.

Предприятия, фирмы, объединения, где имеется не один владелец информации, а несколько, к тому же работают сотрудники, не допущенные к производственным (коммерческим) секретам, представляют собой более сложный обьект защиты. Возникает вопрос о необходимости обеспечения внешней и внутренней безопасности структурных объединений предпринимательства. Для его решения можно использовать частные предпринимательские фирмы, частные службы безопасности (т.е. которые функционируют самостоятельно, принимая заказы от клиентов), собственные службы

безопасности.

Качественное же исполнение заказа негосударственными детективными службами во многом зависит от тех условий, которые создаются им органами власти. Например, Санкт-Петербургская мэрия своим решением запретила на территории города деятельность частных предпринимательских фирм, которые занимались также оказанием услуг по защите коммерческих тайн. Осуществление этих частных функций вменяется государственным правоохранительным органам. И это не смотря на то, как показывает зарубежный опыт, что частное предпринимательство охраняет частное детективное общество. Государственным же правоохранительным органам, при всем их желании и возможностях, с этой задачей в полном объеме не справиться.

Это один вопрос. Второй касается изучения самой частной фирмы перед тем, как обратиться к ней за помощью. Почему? Имеются данные, что некоторые частные детективные образования, вместо того, чтобы действовать в соответствии со своим уставом, занимаются вымогательством, шантажем представителей других предпринимательских фирм. В принципе здесь идет обоюдная проверка заказчика и клиента перед тем, как заключить договор. Игнорирование этим подходом может привести к серьезным ошибкам.

Специальные меры, которые осуществляются при защите информации, можно подразделить на внешние и внутренние.

К внешним мероприятиям относятся следующие. Изучение партнеров, клиентов, с которыми приходится вести хозяйственную, коммерческую деятельность, собирать информацию об их надежности, платежеспособности и другие данные. При необходимости производится изучение связей сотрудников частной фирмы. Выясняются лица, проявляющие интерес к фирме, ее деятельности, сотрудникам, не относятся ли они к конкурирующей фирме или к преступной группе. В случае установления, что эти лица допустили какие-либо противозаконные действия, необходимо информировать соответствующий правоохранительный орган. Тем самым пресекается преступная деятельность и, в том числе, интерес к частной фирме. По возможности желательно установить, в чем суть этого интереса и кому понадобилась та или иная информация. Не повторится ли он в будущем, т.е. что можно ожидать от конкурента (не исключено и преступных элементов).

В ходе осуществления внутренних мероприятий по обеспечению безопасности решаются следующие вопросы. Подбор, проверка лиц, желающих поступить на работу в частное предприятие. Изучаются их анкетные данные, поведение по месту жительства и прежней работы, личные и деловые качества, положительные и отрицательные стороны

изучаемого лица, межличностные отношения. Находился ли в конфликте с законом (судимость, административные задержания, связь с преступным миром). В ходе анализа собранных материалов выясняется, нет ли каких-либо в них противоречий. Дополнительно может проводиться тестирование лица для выяснения моральных или других качеств. Обращается внимание на возможную работу в конкурирующей фирме и причины ухода. После этого делается вывод о пригодности кандидата к работе в данной фирме. На этом этапе изучения сотрудника интерес к нему не заканчивается. Периодически или в зависимости от поведения продолжают изучаться и анализироваться его поступки, затрагивающие интерес (секреты) фирмы. Не исключено, что конкурент может специально направить своих людей для устройства на работу в интересующее его предприятие с целью получения о нем ценных сведений.

Как показывает зарубежная практика работы частных фирм, утечка информации зачастую происходит по инициативе их же сотрудников. В мотивационной основе совершаемых поступков лежит корысть(получить значительную сумму денег) или месть(не исключая заодно и материальную выгоду), например, со стороны уволенного работника, имевшего доступ к предпринимательской информации. В этой связи, целесообразно обращать внимание на лиц, которые в процессе хозяйственной или иной деятельности проявляют необоснованный интерес к информационным хранилищам, предполагаемым сделкам и партнерам. При возникновении серьезных подозрений о недобросовестности сотрудника по отношению к фирме, предпочтительнее с ним расстаться.

Компьютеризация предпринимательских структур, накопление с ее помощью различной информации привлекает как конкурентов, так и преступников. Зачастую лица, желающие воспользоваться этой информацией, находятся среди обслуживающего персонала, а это уже проблема внутренней безопасности. Задача службы безопасности своевременно выявить среди обслуживающего персонала тех сотрудников, которые вынашивают намерения использовать имеющиеся в их распоряжении сведения для продажи другим лицам или использовать в своих личных целях для получения выгоды. Помимо действия в интересах конкурента, могут совершиться и действия, преследуемые по закону: мошенничество, саботаж, повреждение ЭВМ.

Если исходить из зарубежного опыта, то с волной компьютерных преступлений, пока для нас новых и, не в полном объеме, пока урегулированных на законодательном уровне, нам придется столкнуться в недалеком будущем. Субъектами этих преступлений, как правило являются высокообразованные специалисты, имеющие доступ к секретным программам, шифрам, кодам. В банковских системах, например, совершается

мошенничество (снимаются деньги со счетов клиентов вымышленным лицом, занимаются спекуляцией, используя банковский капитал, на валютных биржах, оплачивают собственные счета и т. д.). Развитию данного вида преступлений способствует также и то, что фирмы и банки не стремятся оглашать факты компьютерных краж, чтобы не отпугнуть клиентов. Преступники, зная такое положение, шантажируют владельцев банков, угрожают раскрыть секретные коды и шифры, что может повлечь миллионы расходов для их замены. Только на расследование государственными, частными службами компьютерных ошибок банков приходится тратить около 20 млрд. долларов в год.

Предприятия, располагающие ценной информацией, должны хранить ее в специальных несгораемых шкафах или сейфах, не допускать утери ключей от них или передачи на хранение другим лицам, даже из числа особо доверенных.

Зарубежные фирмы, например, используют для хранения секретной информации сейфы (шкафы), открываемые с помощью специальной магнитной карты или других сложных сигнальных электронных устройств. Следует отметить, что и эта мера значительно затрудняет к ним доступ. Особенно при наличии комплекса защитных (физических и технических) мер здания, где расположен сейф, иное хранилище.

Осуществление специальных внутренних и внешних мер защиты ценных информационных систем должно возлагаться на специально подготовленных лиц. В этой связи, предпринимателю целесообразно обращаться за помощью к частным детективным фирмам, специализирующимся на сыске и охране собственности. Могут создаваться и собственные службы безопасности. Здесь предприниматель сам решает, что ему выгоднее: мириться с утечкой информации или привлекать частные службы безопасности к ее защите. Вопрос состоит в том, какой из убытков меньший: при утечке секретов или их охране.

Зарубежные крупные и состоятельные фирмы вводят в свой штат дополнительную должность - сотрудника, занимающегося противодействием хищению ценной информации. Другие же фирмы постоянно или периодически пользуются услугами частных служб, специализирующихся на сыске и охране. Штатная численность этих служб насчитывает десятки тысяч сотрудников. Тенденция роста их рядов не сокращается. В действиях частных служб и полиции возникают противоречия, но их пытаются уладить с помощью закона или на паритетной основе. Существует договоренность об обмене информацией, если на охраняемой территории совершается преступление.

В Российской Федерации принят Закон “О частной детективной и охранной деятельности в Российской Федерации”, который содержит положения о сыскной и

охранной частной деятельности. Оценивая данный закон с критических позиций, следует указать и на такие положения, заслуживающие внимания, как оказание детективами на возмездной договорной основе помощи гражданам и организациям независимо от их форм собственности. Перечисляются виды разрешаемых и запрещаемых услуг, которые могут оказывать субъекты негосударственной детективной и охранной деятельности: сыщики и охранники.

В частности, Закон предусматривает возможность создания акционерными обществами собственных служб безопасности, которые, среди других задач, призваны вести "...изучение рынка, сбор информации для деловых переговоров выявление некредитоспособных или ненадежных деловых партнеров;...установление обстоятельств...недобросовестной конкуренции..., а также разглашение сведений, составляющих коммерческую тайну...". (ст. 3.).

Подводя итоги, следует отметить, что защита специальными мерами ценной информации должна осуществляться как против конкурентов, так и преступных элементов, пытающихся овладеть ею. Меры защиты зависят от тех способов и приемов, которые применяют похитители. Использование для защиты секретов частных фирм самых сложных электронных устройств позволяет только сдерживать их утечку, но не останавливать этот вид деятельности, широко получивший в мировой практике название промышленный (коммерческий) шпионаж. В экономической литературе, исследующей развитие предпринимательской деятельности, обращается внимание на поддержание этики честной коммерческой деятельности. В ходе же конкурентной борьбы как неотъемлемого элемента рыночного хозяйствования использование промышленного шпионажа нельзя отнести к этическим видам деловых взаимоотношений предпринимателей. Однако рыночно-конкурентная деятельность немыслима, как показывает зарубежная практика, без экономического, производственного, научно-технического и других видов шпионажа. Самый благоприятный общественно-экономический климат для развития предпринимательства не сможет предотвратить банкротства, если в результате удачной шпионской акции будут похищены секретные для фирмы (компании) сведения. Шпионаж - это тень рыночно-конкурентной деятельности, двигатель для одних фирм и тормоз для других.

6. КОММЕРЧЕСКИЙ ШПИОНАЖ.

Лицо, пожелавшее заняться предпринимательством, как правило, уже имеет определенные познания в избранной области, а в случае недостаточности может их получить из обширного ассортимента отечественной и зарубежной литературы. Предпринимательство тесно взаимосвязанно с конкуренцией. Осуществление последней может принимать самые различные формы, в том числе и такие, как хищение или сбор чужой информации, которая носит общеизвестное название шпионаж. Об этой области деятельности у подавляющего большинства людей сложилось довольно стереотипное представление, основанное на художественной литературе, кино- и телефильмах. И не возникало необходимости в более глубоком изучении этого явления. Тем не менее подходы к такому общественному явлению, как шпионаж, в условиях рыночно-конкурентной деятельности резко меняются, ибо лицам, занимающимся предпринимательством, уже приходится, ибо лицам, занимающимся предпринимательством, уже приходится сталкиваться с этой проблемой. С одной стороны, они вынуждены защищать свои секреты (ценную информацию), а с другой - пытаться завладеть секретами конкурента, чтобы выжить в рыночном противоборстве. Цель данного раздела, хотя бы в очень краткой форме, изложить отдельные вопросы, характеризующие понятие шпионажа, его виды и способы осуществления и тем самым оказать практическое содействие лицам, прямо или косвенно причастным к предпринимательской деятельности.

Термин “шпионаж” (с прилагательными: “экономический”, “промышленный”, “коммерческий”, “научно-технический”) означает активные действия, направленные на сбор или хищение ценной информации, закрытой для доступа посторонних лиц.

Экономический шпионаж более широкое понятие, которое охватывает и такие его подвиды, как промышленный, производственный, научно-технический, коммерческий шпионаж. Обладание тайной одним лицом вызывает к ней интерес другого лица, для удовлетворения которого совершаются действия, направленные на завладение ею с целью получить определенную материальную или иную выгоду. Лицо, участвующее в подобной деятельности, имеет общеизвестное название “шпион”. В предпринимательстве конкурентная борьба невозможна без получения информации. Стремления получить сведения в условиях закрытого к ним доступа законным путем порождает неизбежно недобросовестную конкуренцию, т.е. объективную потребность шпионить за конкурентом. Без владения информацией о действиях конкурента, предполагаемом спросе на продукцию, перспективных научных разработках трудно, а порой и невозможно быть конкурентоспособным. Возникает два тесно взаимосвязанных обстоятельства:

1. Предприниматель вынужден выступать в качестве защитника своих

секретов (ценной информации);

2. Предприниматель вынужден в целях конкуренции добывать (воровать, покупать) чужие защищаемые секреты. То, что не защищается, особой ценности в рассматриваемом плане не имеет.

Возникает вопрос о том, как рассматривать промышленный (коммерческий) шпионаж с позиций действующего законодательства . В литературе о промышленном шпионаже за рубежом отмечается, что рассматриваемая деятельность вовсе не считается преступной и не влечет уголовной ответственности. Если в процессе хищения секретной информации предприятию, учреждению или сотрудникам причиняется ущерб, то уголовному наказанию виновное лицо повергается именно за последнее деяние, а не за сам факт хищения ценнейших сведений. В принципе такой поход является правильным, поскольку сам предприниматель не заинтересован в том, что когда он будет совершать хищение материалов, а заниматься этим он вынужден в силу рыночной деятельности, то будет находиться под угрозой применения к нему уголовного наказания. Предпочтительнее обратить внимание на охрану своих тайн, чем прибегать к уголовно-правовой защите.

В этих целях более подробно рассмотрим признаки, характеризующие промышленный шпионаж. К ним относятся:

- ***субъект (кто может заниматься данным видом деятельности);***
- ***предмет (на что посягается промышленный и иной шпионаж);***
- ***способ, средство (действия, с помощью которых осуществляется овладение закрытыми сведениями);***
- ***адресат (кто выступает заказчиком).***

Субъектами промышленного (коммерческого) шпионажа могут быть граждане России, иностранные граждане, лица без гражданства, относящиеся и не относящиеся к сотрудникам предпринимательских предприятий, учреждений, фирм. Исполнителем шпионажа может выступать непосредственно предприниматель, сотрудники собственной службы безопасности, частных детективных сыскных фирм или отдельные лица, действующие в частном порядке. Поиск и овладение промышленной, коммерческой информацией осуществляется, в одних случаях, по заданию заказчика, в других - по собственной инициативе для последующей ее продажи заинтересованным лицам.

Анализ зарубежной практики показывает, что у частных служб безопасности, специализирующихся на хищении чужих секретов, имеется значительная по числу клиентура заказчиков и покупателей. Например, в Великобритании одно из частных сыскных агентств, наряду с расследованием фактов о промышленном шпионаже,

обеспечением безопасности предприятий и фирм, занимается также добыванием (хищением) информации о конкурентных частных предприятиях. Подобные фирмы не стремятся особо конспирировать, скрывать свою деятельность. Их координаты имеются в специальных справочниках. В настоящее время в странах рыночной экономики действуют сотни и тысячи агентств и десятки тысяч промышленных шпионов.

Подобные агентства начинают образовываться и действовать и на территории Российской Федерации. Однако резкий рост таких служб следует ожидать только в условиях сформировавшейся рыночно-конкурентной экономики, аналогичной западным странам.

По вполне понятным причинам выдать секреты могут и сотрудники фирмы. Если лицам, не работающим на предприятии, необходимо преодолевать физические и технические препятствия для проникновения к секретам, то работникам фирмы не требуется прилагать подобные усилия. Тайной информацией они уже обладают или имеют возможности собрать ее. Мотивацией таких действий могут служить корысть, месть и т.д. Поэтому при формировании коллектива сотрудников необходимо учитывать, кому из них доверять свои тайны, а кому нет. Решают этот вопрос сами предприниматели. Так, сотрудники общеизвестного АНТа на страницах газет довольно подробно делятся информацией о том, как они занимались внутренней безопасностью своего кооператива. Вначале принимали к себе на работу только тех, кого знали лично и могли им доверять. Расширение штата сотрудников увеличивало опасность утечки информации. Поэтому руководством АНТа принимается решение о создании специального подразделения - департамента по проверке людей, поступавших к ним на работу. На кандидатов заводились досье, в которых концентрировались результаты их изучения и проверок. Проверяемые могли знакомиться с досье на себя. Трудно пока вести речь о том, что любой предприниматель может иметь такие же возможности или создать их. Но подход к защите своих секретов у них был правильный и их опыт может использоваться другими фирмами с учетом своих возможностей и потребностей.

Следующим признаком, характеризующим шпионаж, является предмет посягательства, т.е. информация, которая представляет ценность для ее обладателя и закрыта к доступу посторонних лиц. Носители такой информации самые разнообразные: документы, чертежи, схемы, патенты, дискеты, кассеты, в которых содержатся научные исследования. бухгалтерские материалы, контракты, планы и решения руководства предпринимательских фирм. Предметом промышленного шпионажа может быть не только информация предпринимательских фирм, но и государственных предприятий и учреждений.

Определенные трудности возникают при определении промышленной тайны предприятий, фирм, компаний со смешанным капиталом. Например, частный и государственный капитал; государственный и иностранный частный капитал; отечественный и иностранный частный капитал. Неизбежно столкновение интересов нашего и иностранного собственника как между собой, так и с государством. В последнем случае необходимо учитывать наличие государственной (военной) тайны, служебной тайны, иных сведений, определяемых уголовным законом, а также промышленную тайну. Сведения, составляющие государственные секреты, перечислены в специальных нормативных актах, утверждаемых Российским правительством. На их основании издаются ведомственные акты, определяющие виды секретов, подлежащих охране. Промышленная же тайна может включаться в перечни государственных секретов, а может и не относиться к ним. Посягательство на секреты государственных предприятий и учреждений преследуется уголовным законом, тогда как предпринимательские секреты уголовным законом не защищены. Например, способ производства и заварки чая для государства не представляет ценности, а для предпринимателя - это фирменный секрет, на котором держится все его предприятие.

Следующим признаком промышленного шпионажа является способ его осуществления. Действия по завладению информацией проходят скрытно (тайно) от окружения, путем их хищения, сбора, покупки, выдачи. Не исключается и уничтожение, искажение или саботирование по использованию информации. Цель - не дать владельцу возможности использовать ее для получения выгоды, быть конкурентоспособным.

К средствам получения секретов относятся различные технические системы. Если у нас пока основными владельцами разведывательных технических средств являются специальные государственные органы (службы), то на Западе они находятся в пользовании и частных лиц. Это позволяет предпринимателям широко использовать средства электронной разведки в получении необходимой информации. Снятие ее с телефонных переговоров, ЭВМ, помещений, где ведутся секретные беседы, и т.д. Применение тех или иных средств зависит от информации, которую намеревается получить субъект. Один вид информации может быть похищен, другой прослушан, третий - сфотографирован или сделаны зарисовки, четвертый записан на магнитофон, пятый - снят кинокамерой и т.д. Иногда используется комплекс специальных мер по ее получению. В зависимости от вида получения информации принимаются соответствующие меры защиты. Например, существуют приборы, с помощью которых можно с расстояния до 500 м лазерным лучом снимать речевую информацию за счет вибрации оконных стекол. В ответ, для предотвращения утечки информации таким

способом, немецкая фирма Сименс начала выпуск специальных оконных рам, ослабляющих на 110дБ проникновение электромагнитных излучений в определенных диапазонах.

Адресатами (заказчиками) получения промышленной (коммерческой) информации выступают предприниматели малого и крупного бизнеса, руководители государственных предприятий, а также правительства иностранных государств. Защита секретов промышленных и коммерческих фирм и проникновение к ним являются двумя сторонами одной медали. К ним в одинаковой мере проявляют интерес как частные лица, так и сотрудники государственных служб.

Один из руководителей американской разведки, выступая в 1998г. в Национальном пресс-клубе, заявил, *что "экономическая мощь является ключом к господству и власти во всем мире.*" В речи этого руководителя, произнесенной в Американском университете, прозвучало, что "в предстоящие годы мы станем свидетелями резкого возрастания напряженности в международных экономических отношениях. Объективная информация об экономике иностранных государств станет практически важной, и разведка обязана ее добывать". За рубежом считают, что не менее важная задача ложится на плечи контрразведывательных подразделений, которые обязаны пресекать все попытки иностранных спецслужб, не исключая и дружественные, осуществлять политический, промышленный и экономический шпионаж против США.

В нашей периодической печати также появляются заметки о том, что отечественная разведка (разведки) перенацеливает свои усилия на сбор торгово-экономической информации.

Как видим, новым приоритетом в современных условиях для разведывательных и контрразведывательных сообществ становятся сведения экономического характера. Поэтому напрашивается вывод о том, что интерес к определенным видам частной и государственной экономической информации на территории Российской Федерации (включая деятельность наших фирм и за рубежом) будет проявляться не только со стороны частных служб безопасности, но и иностранных спецслужб (разведок).

Может ли частный предприниматель противостоять посягательствам специальных государственных служб? Трудно что-либо утверждать в данных условиях, скорее всего нет. К тому же прямая защита предпринимательских структур не относится к функциям контрразведывательных служб. Западные фирмы тратят на защиту своей информации 15 % своих доходов. У нас вести речи о такой защите пока рано. Вместе с тем наш предприниматель не стремится в случае необходимости обращаться к государственным правоохранительным органам.

Попытаемся остановиться на проблеме отличия промышленного (коммерческого) шпионажа от государственных тайн и иных сведений, находящихся под охраной уголовного закона. В качестве основы разграничения этих понятий и принимаемых государственно-властных или иных решений лежат признаки, характеризующие промышленный шпионаж, а также признаки, характеризующие составы преступлений, содержащие запреты на завладение государственными структурами.

Итак, посягательства на частную информацию могут быть со стороны субъектов частного предпринимательства и спецслужб иностранного государства.

1. Проникновение к частным секретам фирмы, предприятия со стороны конкурирующей частной фирмы (сотрудники частного детективного агентства, собственной разведывательной службы) предотвращается собственными силами безопасности и техническими средствами. Лицо, задержанное в помещении (здании), может быть привлечено к уголовной ответственности за непосредственно причиненный ущерб: разбой; умышленное или неосторожное уничтожение или повреждение личного имущества граждан или как посягательство против собственности объединений и организаций; преступление против жизни и здоровья личности.

Завладение промышленным (коммерческим) секретом осуществляется также с помощью подкупа сотрудников конкурирующей фирмы, их шантажа, угроз и т.д. Если выяснится, что утечка секрета произошла по вине своего же работника, то предприниматель сможет только уволить его, чтобы предотвратить выдачу информации в будущем.

В таких случаях предпочтительнее всего для предпринимателя является не допустить утечки информации, создав надежную защиту, чем тратить силы и средства на поиск шпиона, похитившего секретные материалы.

2. Частный детектив, действуя в интересах отечественной предпринимательской фирмы, посягает на информацию государственного предпринимательского предприятия. В данной ситуации может быть несколько решений.

Если частное лицо овладевает ценной информацией, относящейся к сведениям, составляющим государственную или служебную тайну, то уголовная ответственность по УК РФ за это деяние не предусмотрена.

Похищенные сведения составляют государственную тайну. В данном случае также не усматривается состав преступления. Во-первых, если рассматривать по признакам

состава разглашения государственной тайны, то частное лицо не может быть субъектом данного преступления. Сведения ему не доверялись и не могли стать известными по службе или работе, так как он не работал на данном предприятии, учреждении.

Не попадает это действие и под признаки составов, предусматривающих измену Родине в форме шпионажа или шпионаж. По объективной стороне этих особо опасных государственных преступлений адресатами сбора и передачи информации выступают иностранное государство, иностранная организация или их агентура. Здесь же адресатом выступает отечественная предпринимательская фирма.

Отсутствует состав преступления в действиях частного лица и тогда, когда сведения, составляющие государственную тайну, он получит от работников режимного предприятия обманным путем, подслушиванием их разговоров и т.д. В то же время в поведении работников, допустивших утечку доверенной им (ставшей известной по службе или работе) секретной информации, содержатся признаки состава разглашения государственной тайны (неосторожная форма вины).

- В действиях частного лица, обнаружившего утраченные материалы, содержащие государственную тайну, передавшего их нашей частной фирме, также не содержится состава преступления.
- Сотрудник режимного предприятия совершает с частным лицом сделку, продает ему за деньги государственную тайну. При этом сознает, что покупателем является отечественная предпринимательская фирма.

Лицо, продавшее секретные материалы, должно нести уголовную ответственность за разглашение государственной тайны. Лицо, купившее эти сведения, уголовной ответственности не несет.

3. Частное лицо в интересах предприятия смешанного типа (частный и государственный отечественный капитал) посягает на промышленную (коммерческую) тайну аналогично по типу предприятия. Здесь могут быть различные подходы к решению вопроса ответственности. В частности, похититель информации в интересах отечественного СмП не попадает под признаки соответствующих норм УК РФ.

В то же время при наличии государственной или служебной тайны возникает вопрос об ответственности сотрудников данного предприятия, если будет установлено, что они продали, выдали (разгласили) частному лицу секретные сведения. В их поведении имеются, в зависимости от предмета посягательства, признаки состава разглашения государственной тайны. Разглашение же служебной тайны не является предметом данного преступления. Отсутствуют здесь также и признаки другого сходного преступления -

передачи иностранным организациям сведений, составляющих служебную тайну. Нет адресата, который предусмотрен составом преступления, а именно: иностранной организации, их представителей. Однако, если указанные действия совершает должностное лицо, вопреки интересам предприятия, то оно может нести уголовную ответственность за злоупотребление властью или служебным положением.

4. Частное лицо посягает на информацию предприятий смешанного типа (отечественный и иностранный капитал) в интересах отечественного предприятия.

В его действиях отсутствуют признаки составов преступления, за исключением тех случаев, когда в процессе хищения не будет совершено другое преступление (убийство или причинение телесных повреждений охраннику или другим лицам, уничтожение или повреждение имущества и т.п.).

5. Частное лицо действует в интересах иностранной частной или государственной фирмы, филиалы которой расположены как на территории Российской Федерации, так и за рубежом, против отечественных частных и государственных предпринимательских структур.

При посягательстве на промышленную (коммерческую) информацию частного предприятия признаки состава преступления отсутствуют. Некоторое внешнее сходство данная деятельность по приобретению информации имеет с признаками состава передачи иностранным организациям сведений, составляющих служебную тайну. Однако служебная тайна определяется нормативными актами только государственных и для государственных предприятий. Следовательно, отсутствует в рассматриваемом деянии такой признак, как предмет преступления - служебная тайна.

Несколько иную уголовно-правовую оценку получают действия частного лица (нашего гражданина, иностранного гражданина или лица без гражданства) в интересах иностранной организации (государственные - учреждения, органы, организации, т.е. относящиеся к правительственной структуре; негосударственно-посреднические, коммерческие, промышленные, страховые и другие, относящиеся к малому и крупнофирменному предпринимательству, а также компании промышленников, различные общественные организации) в случае завладения сведениями, составляющими служебную тайну государственных предприятий.

Уголовная ответственность виновного наступает за передачу иностранным организациям сведений, составляющих служебную тайну. При этом ответственность несут как лица, выдающие служебную тайну (работники предприятия), так и лица, собирающие (выведывание, хищение, купля) с целью передачи иностранным

государственным и негосударственным организациям или их представителям.

Под действие данной статьи могут попадать действия сотрудников частных детективных фирм, занимающихся добычей чужих секретов, при условии, что адресатам передачи сведений, составляющих служебную тайну, выступают иностранные организации.

Сотрудники негосударственных детективных фирм, которые намерены оказывать услуги в сборе определенной информации по инициативе заказчика или по собственной, с целью последующей продажи заинтересованному адресату, должны выяснять для себя, чтобы не вступить в конфликт с законом, кто выступает заказчиком или какой адресат ее приобретает.

Нельзя исключать и такой ситуации, когда услугами частных детективов пожелают воспользоваться иностранные спецслужбы. Частным бизнесом движут деньги, а такие услуги щедро могут оплачиваться.

Сознательное выполнение частным детективом, например, заказов представителя иностранного государства (сотрудника органов разведки, дипломата или иностранной негосударственной организации), направленных на получение сведений, составляющих государственную (военную) тайну, или иных сведений (экономического, научно-технического, военного или другого характера), как составляющих секреты, так и не относящихся к ним, но представляющих интерес для адресата, должно оцениваться и квалифицироваться как шпионаж или измена Родина в форме шпионажа (в зависимости от гражданства детектива).

Деятельность же на территории Российской Федерации частного лица по сбору сведений о третьих государствах (работе посольства, иностранных организаций и граждан) не попадает под признаки шпионажа.

6. Деятельность представителей спецслужб иностранных государств по сбору промышленной (коммерческой) информации отечественных частных предпринимательских предприятий, учреждений, фирм должна квалифицироваться как противозаконная, т.е. шпионаж. Предметом состава шпионажа (измены Родине в форме шпионажа), в данном случае, являются сведения, хотя и не составляющие государственную (военную) тайну, но представляющие интерес для иностранного адресата. Частнопредпринимательская информация, с учетом субъекта посягательства, попадает под уголовно- правовую защиту. Лица, занимающиеся ее сбором и передачей адресату, должны нести уголовную ответственность за шпионаж.

7. Частная иностранная фирма (компания, акционерное общество и т.д.)

через своих представителей собирает сведения, составляющие промышленную (коммерческую) тайну отечественного частнопредпринимательского предприятия (учреждения, фирмы).

В этой связи следует подчеркнуть, что активизация деятельности иностранных предприятий на территории России может затрагивать и интересы национальной безопасности. Разведки иностранных государств до 80 % разведывательной информации получаю из открытых источников - газет, журналов, научной политической и экономической литературы, т.е. за счет высококвалифицированной аналитической работы. Получить же таким путем промышленную (коммерческую) информацию не представляется возможным. Секреты частных фирм на страницы открытой печати и другой общедоступной литературы не попадают. Поэтому в сфере промышленного шпионажа действуют не разведчики аналитики, а разведчики, цель которых своим действием овладеть единовременно сведениями, составляющими тайну, а не собирать их длительное время по крупицам. Хотя подготовительная работа может и занимать определенное время.

Уголовно-правовая оценка такой деятельности с позиций действующего законодательства позволяет сделать вывод о том, что она противозаконна. Адресат, желающий получить информацию и предмет - иные сведения, в которых он заинтересован, являются, наряду с другими, признаками шпионажа, за который предусмотрена уголовная ответственность.

Краткое рассмотрение пределов возможной защиты и сбора промышленной (коммерческой) информации свидетельствует о недостаточной пока правовой проработке данной проблемы. Однако значение и учет в предпринимательской деятельности действующего законодательства позволяют избежать серьезных ошибок и не вступать в конфликт с законом.

СПИСОК ЛИТЕРАТУРЫ:

1. Долгополов Ю.Б.,“Предпринимательство и безопасность”, “Универсум”, М., 2001 г.

2. Казакевич О.Ю. и др. “Предприниматель в опасности: способы защиты (практическое руководство для предпринимателей и бизнесменов)”, Объединение УППИКС, М, 1998 г.

3. Кавеладзе И.Т., “Практика защиты коммерческой тайны в США (руководство по защите вашей деловой информации)”, “ЭКОконсалтинг”, М., 1999г.

4. Раевский Г. “Угрозы экономической безопасности предприятия и задачи службы безопасности по их нейтрализации”, журнал “Частный сыск” №4, “Ось-89”, М., 2001 г.

5. “Гражданский кодекс Российской Федерации”, часть первая, “ИНФРА-М”, М, 1997г.