**Министерство Образования Ростовской Области**

**Южный Федеральный Университет**

**Таганрогский Радиотехнический Университет**

**Реферат**

**на тему: "Защита коммерческой информации"**

**г. Таганрог**

**2011**

**Понятие и источники коммерческой информации**

Коммерческая информация представляет собой сведения о сложившейся ситуации на рынке различных товаров и услуг.

Назначение коммерческой информации состоит в том, что она позволят торговым фирмам проводить анализ коммерческой деятельности, планировать ее и осуществлять контроль над результатами этой деятельности.

Источниками коммерческой информации могут служить маркетинговые исследования по конкретным товарам. Однако, перед тем, как вкладывать денежные средства в проведение исследований, сбор и анализ информации, необходимо провести сравнительную оценку затрат и значимости возможных результатов. Если прирост прибыли от использования коммерческой информации превысит прирост затрат на ее получение, то проведение маркетинговых исследований является целесообразным.

Важнейшим источником коммерческой информации являются также внутренние материалы и документы торговой формы, в частности, сведения об объемах товарооборота, затратах на продажу, товарных запасах, прибыли предприятия, расходах на рекламу.

Еще одним из источников коммерческой информации являются данные внешней статистики и публикуемые в средствах массовой информации сведения о состоянии рынка.

***Общие вопросы защиты коммерческой информации***

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 коммерческой информации необходимо руководствоваться такими критериями (свойствами), как:

♦ полезность;

♦ своевременность;

♦ 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 ее 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) источником 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 коммерческой деятельности этот критерий особой роли не играет.

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

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) коммерческой информации, как интеллектуальной собственности, могут быть граждане России, граждане иностранных государств, лица без гражданства, а также объединения граждан - коллективных предпринимателей.

Обширны и направления коммерческой 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 коммерческой 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 передачу, а равно сбор и хранение сведений, составляющих государственную тайну, с целью передачи ее иностранному государству предусмотрена ст. 276 Уголовного кодекса РФ

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

Обеспечение безопасности государственной интеллектуальной собственности под грифом “совершенно секретно”, “секретно” не имеет прямого отношения к защите частной коммерческой информации. Однако следует указать на некоторые исключения. В случае, если спецслужба иностранного государства проявит интерес к получению определенной коммерческой информации, то наряду с другими мерами оказывать ей противодействие будет и контрразведка. Под защиту специальных органов государства может быть взята коммерческая 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 коммерческой информации, то она подобной уголовно-правовой, оперативно-следовательской и режимной защитой не обладает и не пользуется.

В гражданском законодательстве, тем не менее, предпринята попытка узаконить 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.

1. 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-правовому договору”.

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

Подводя итоги изложенному, 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;
* коммерческая 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.

***Специальные вопросы защиты коммерческой информации***

Коммерческая 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 общеуголовных 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. 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. Коммерческая информация, рекламируемая в газетах, в журналах, по телевидению, радио помогает преступникам выйти на объект 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).

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 коммерческая информация надежно защищена.

***Коммерческая тайна. Промышленный шпионаж***

К коммерческой тайне могут быть отнесены самые разнообразные сведения, связанные с производством, технологией, управлением, финансами и другими вопросами деятельности предприятия. На практике наряду с термином “коммерческая тайна” широко используются такие термины, как “конфиденциальная информация”, “ноу-хау”, “секреты производства”. Все они, в сущности, обозначают одно и те же понятие, которое в Гражданском кодексе РФ именуется “коммерческой тайной”.

В соответствии со ст.139 Гражданского кодекса РФ коммерческая тайна - это информация, имеющая 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.

Из данного определения вытекают следующие обязательные признаки коммерческой тайны.

Первый признак - информация должна иметь действительную или потенциальную коммерческую ценность. Поэтому из числа сведений, составляющих коммерческую тайну, исключаются те из них, которые не представляют никакого интереса для окружающих. При отнесении предприятием информации к кругу сведений, составляющих коммерческую тайну, действительная или потенциальная коммерческая ценность таких сведений предполагается и не нуждается в доказывании. Однако в случае возникновения судебного спора (например, по иску к контрагенту о возмещении убытков, причиненных разглашением коммерческой тайны) перед предприятием встанет необходимость доказывать суду наличие у информации коммерческой ценности.

Второй признак - к информации, составляющей коммерческую тайну, не должно быть свободного доступа на законном основании. Если информация может быть получена законным образом любым заинтересованным лицом (путем изучения печатных изданий, просмотра открытых баз данных и т.п.), то такая информация коммерческой тайной не является. Даже если информация стала известной неограниченному круги лиц в результате чьих-либо неправомерных действий, то и в этом случае информация автоматически утрачивает статус коммерческой тайны, поскольку лишается одного из необходимых критериев - отсутствие к информации свободного доступа.

Третий признак - для того, чтобы информация считалась коммерческой тайной, требуется, чтобы обладатель такой информации принимал меры к охране ее конфиденциальности. Меры по охране коммерческой тайны могут быть организационными (например, утверждение внутренних документов, регулирующих порядок доступа персонала к коммерческой тайне), техническими (использование сигнализации, защита телефонных переговоров и т.п.) и юридическими (например, включение в трудовые контракты с персоналом и договоры с контрагентами положений о неразглашении конфиденциальной информации). При этом простое определение круга информации, составляющей коммерческую тайну, не может рассматриваться в качестве охранной меры.

Коммерческая тайна, как разновидность информации, может являться объектом интеллектуальной собственности. При соблюдении необходимых условий (информация приносит доход и может быть использована в течение периода, превышающего 12 месяцев) права на указанную информацию могут отражаться в бухгалтерском учете в виде нематериальных активов. В то же время законодательство не рассматривает факт отражения в бухгалтерском учете прав на информацию в качестве одного из признаков коммерческой тайны. Поэтому отсутствие в учете указанных прав не может свидетельствовать об отсутствие самой коммерческой тайны.

Коммерческая тайна не требует для признания ее таковой какой-либо государственной регистрации или выполнения каких-либо иных формальностей. В то же время следует отметить, что не любая информация, соответствующая всем перечисленным выше критериям, может быть отнесена к коммерческой тайне. Государство вправе осуществлять контроль (в том числе налоговый) за деятельностью предприятий. Для этих целей законодательство определяет круг сведений, которые не могут составлять коммерческую тайну.

Так, например, Постановлением Правительства РФ от 05.12.91г. № 35 установлен перечень таких сведений, к которым, в частности, относятся:

♦ учредительные документы (решение о создании предприятия или договор учредителей) и устав;

♦ документы, дающие право заниматься предпринимательской деятельностью (регистрационные удостоверения, лицензии, патенты);

♦ сведения, необходимые для проверки правильности исчисления и уплаты налогов;

♦ документы о платежеспособности;

♦ сведения о численности работающих и их заработной плате; документы об уплате налогов;

♦ сведения об участии должностных лиц предприятия в других организациях.

В соответствии с п.89 Положения по ведению бухгалтерского учета (утверждено Приказом Минфина РФ от 29.07.98г. № 34), годовая бухгалтерская отчетность организации является открытой для заинтересованных пользователей: банков, инвесторов, кредиторов, покупателей, поставщиков и др., которые могут знакомиться с указанной отчетностью.

Под коммерческой тайной предприятия (фирмы) следует понимать сведения, не являющиеся государственными секретами, но связанные с производством, технологией, управлением, финансами и другой деятельностью предприятия, разглашение которых может нанести ущерб его интересам. Защищаемые сведения дают определенные преимущества в конкурентной борьбе. Коммерческой тайной предприятия не может быть информация, сокрытие которой способно нанести ущерб обществу.

В соответствии с Законом РФ "О предприятиях и предпринимательской деятельности" перечень сведений, составляющих коммерческую тайну, определяется руководителем предприятия. Предприятие имеет право не предоставлять информацию, содержащую коммерческую тайну.

Законом предусматривается, что порядок, организация защиты коммерческой тайны с учетом действующего законодательства устанавливается руководителем предприятия (фирмы).

Сведения, отнесенные к коммерческой тайне, должны иметь следующие признаки:

♦ не являться государственным секретом;

♦ относиться к производственной деятельности предприятия;

♦ не наносить ущерб интересам общества; иметь действительную или потенциальную коммерческую ценность и создавать преимущества в конкурентной борьбе;

♦ иметь ограничения в доступе, устанавливаемые руководителем предприятия на законном основании (предприятием (фирмы) должны приниматься меры по их охране).

Методика отнесения тех или иных сведений к коммерческой тайне в нашей стране еще окончательно не разработана, поэтому ограничимся лишь некоторыми.

К коммерческой тайне могут быть отнесены:

♦ технология производства; технологические приемы и оборудование;

♦ модификации ранее известных технологий и процессов;

♦ перспективные методы управления;

♦ ценовая и сбытовая политика;

♦ сравнительные характеристики собственного ассортимента и товаров конкурентов с точки зрения качества, внешнего вида, упаковки и т.д.;

♦ производственные, коммерческие и финансово-кредитные отношения с партнерами;

♦ планы предприятия по расширению (свертыванию) производств;

♦ факты проведения переговоров по вопросам купли-продажи;

♦ данные, которые могут быть использованы для нанесения ущерба репутации предприятия (фирмы);

♦ информация о кадрах (текучесть кадров, ведущие специалисты и места их работы по совместительству);

♦ сил и условий для защиты коммерческой тайны, а также другие сведения.

В повседневной жизни коммерческая тайна всегда выступает в форме коммерческих секретов. Поскольку всякая тайна есть секрет, но не всякий секрет есть тайна.

Коммерческие секреты – форма проявления коммерческой тайны. Представляют собой сведения в виде документов, схем, изделий, относящиеся к коммерческой тайне фирмы и подлежащие защите со стороны службы безопасности от возможных посягательств путем похищения, выведывания, утечки информации.

Они различаются по следующим признакам:

♦ по природе коммерческой тайны (технологические, производственные, организационные, маркетинговые, интеллектуальные, рекламные)

♦ по принадлежности собственности (собственность предприятия, группы предприятий, отдельного лица, группы лиц);

♦ по назначению коммерческих секретов.

Носитель коммерческого секрета – лицо, осведомленное о коммерческих секретах предприятия или фирмы (руководители и допущенные к коммерческим секретам исполнители).

Носители коммерческих секретов следует отличать от источников закрытой коммерческой информации («ноу-хау», схемы, документы, технологии, изделия, образцы).

Секретность в условиях рыночного хозяйствования защищает производителя от недобросовестной конкуренции, к которой относятся различные противоправные действия в виде скрытого использования торговой марки, подделки продукции конкурента, обманной рекламы, подкупа, шантажа и т.п. Не последнее место в этом ряду занимает промышленный 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 взаимосвязано 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.

Рассмотрим признаки, характеризующие промышленный (коммерческий) 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.

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. 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.

Адресатами (заказчиками) получения 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.

***Обеспечение защиты коммерческой тайны***

Разглашение коммерческой тайны может ухудшить экономическое положение предприятия или фирмы. Чтобы этого не произошло, следует перевести такую информацию в разряд охраняемой. Это делается приказом руководителем фирмы, в котором перечисляются сведения, относящиеся к коммерческой тайне.

Методика отнесения тех или иных сведений к коммерческой тайне в нашей стране еще не разработана, поэтому, опираясь на опыт зарубежных стран, ограничимся лишь некоторыми рекомендациями.

При засекречивании информации надо исходить из принципа экономической выгоды и безопасности фирмы. Причем, объявляя ту или иную информацию коммерческой тайной, важно соблюсти “золотую середину”. Чрезмерное засекречивание деятельности фирмы может обернуться потерей прибыли, так как условия рынка требуют широкой рекламы производимой продукции и услуг. Те же результаты может вызвать пренебрежительное отношение к коммерческой тайне, так как рынок это всегда конкуренция. Американские предприниматели считают, что утрата 20 % информации приводит к разорению фирмы в течение месяца в 60 случаях из 100

Информация типа “ноу-хау”, безусловно, должна быть отнесена к разряду коммерческой тайны. Ее надо охранять и от собственного персонала, ибо всегда существует опасность, что тот или иной сотрудник уволится и устроится на работу в конкурирующую фирму. Сведения же, которыми он владеет, не могут быть у него изъяты.

За рубежом существует практика подписания с сотрудником соглашения, по которому ему после увольнения запрещается работать в конкурирующей фирме. Правда, такого рода соглашения действуют лишь в течение определенного срока после расторжения договора о найме. Кроме того, во время действия подобного ограничения этому лицу должно выплачиваться вознаграждение. В нашей практике такие соглашения пока неизвестны.

Информация о рационализаторском предложении, изобретении и т. п., находящиеся на стадии разработки, несомненно, относится к коммерческой тайне. Рационализаторское предложение даже после его оформления и выдачи авторского свидетельства может оставаться коммерческой тайной, поскольку представляет собой техническое решение задачи, новое для данной фирмы. Изобретение после выдачи на него патента имеет специальную правовую охрану и поэтому не нуждается в защите как коммерческая тайна. Другое дело, если по соглашению с автором изобретения фирма примет не подавать заявку в Госпатент Российской Федерации. Тогда охрана информации полностью возлагается на фирму. Следует подчеркнуть, что решение не подавать заявку на изобретение на патентоспособное техническое решение, возможно только по договоренности с автором, так как по существующему правилу, если работодатель в течение трех месяцев с момента уведомления его автором, о сделанном изобретении не подаст заявку на него, автор вправе сам подать заявку и получить патент. До недавнего времени 90 % авторских свидетельств получали гриф “для служебного пользования”. Вместо авторских свидетельств теперь выдают патент. Основным принципом патента является его обязательная открытость, что способствует ускорению научно- технического прогресса. Патент- тот же товар изобретателя, но государство продолжает засекречивать патенты, т.е. нарушает права изобретателей. Государство же должно не отбирать у человека право на его интеллектуальную собственность, а выкупать его, причем по рыночной стоимости.

Особое внимание следует уделить охране договоров, заключаемым предприятием. Большая их часть, безусловно, относится к коммерческой тайне. Причем в определенных случаях охране подлежит не только текст договора, но и сам факт его заключения.

Разрабатывая меры по защите коммерческой тайны фирмы, необходимо экономически обосновать целесообразность засекречивания той или иной информации. В первую очередь выделяется информация, утечка которой может привести вашу фирму к банкротству. Это строго конфиденциальная информация. В мире бизнеса, это как правило, “ноу-хау”. К конфиденциальной информации относятся сведения о перспективах развития фирмы, ее клиентах, сроках и сумме кредитования. Огласка этих сведений, конечно же, не приведет к краху, но лишит фирму на какое-то время устойчивой прибыли. Также не подлежит огласке информация, раскрытие которой может привести к неблагоприятным последствиям. К ней относятся: номера домашних телефонов, адреса руководителей и сотрудников фирмы, текущие планы работы, информация о конфликтных ситуациях и т.п. Остальные сведения относятся к открытым, то есть доступным всем. Но следует иметь в виду, что неправильно поданная информация может помочь аналитикам из конкурирующей фирмы обнаружить ваши уязвимые места. Руководитель фирмы должен установить строгий порядок хранения первых экземпляров договоров и работы с ними. Их следует хранить в определенном месте у ответственного лица и выдавать только под расписку с письменного разрешения руководителя фирмы.

На лица, ответственные за хранение договоров и работу с ними, возлагается персональная ответственность за утерю договоров или утечку информации из них. Все это необходимо потому, что деятельность коммерческих структур строится в большей степени на договорных началах, и конкурент или партнер по переговорам, обладая информацией в этой сфере, может составить довольно полную картину производственного и финансового положения фирмы. Пропажа (похищение) первых экземпляров договоров ведет к значительным затруднениям, и даже невозможности доказывать те или иные положения при возникновении спора и его решении в судебном порядке. При подписании договора рекомендуется, чтобы представители сторон ставили подписи не только в конце договора, но и на каждом листе во избежание замены одного текста другим. Следует отметить, что затраты зарубежных фирм на охрану своей коммерческой тайны составляют 10-15 % всех расходов на процесс производства. Поэтому наиболее расчетливые предприниматели пытаются на этом сэкономить, переложив затраты на плечи государства. Каким образом? Путем получения госзаказов оборонного характера. Помимо прочих преимуществ, госзаказы позволяют пользоваться защитой государственных правоохранительных органов и, в первую очередь, контрразведки.

Главное место в организации надежной защиты секретной информации должно отводиться работе с кадрами. Эта работа должна начинаться со дня приема человека на работу.

Вторым по важности мероприятием должно быть ограничение доступа к секретной информации. Работа должна быть организована таким образом, чтобы сотрудник имел доступ только к той информации, которая необходима ему в процессе выполнения прямых служебных обязанностей.

Третьим направлением в работе с кадрами является проведение воспитательной работы, соблюдение режима секретности, вознаграждение в успехе выполнения этого режима, а также учить правилам соблюдения режима секретности, разъяснять ценность секретных материалов.

Такие подходы к работе с кадрами дают неплохие результаты и могут применяться на предприятиях разного профиля деятельности.

Что можно рекомендовать руководителю, начинающему создавать систему безопасности на своей фирме? Прежде всего знать, что обойдется это недешево. Поручить создание системы безопасности профессионалам, только им и не кому более. Сразу же следует подумать о безопасности наиболее важных секретов, утечка которых может нанести ущерб, значительно превышающий на их защиту. При этом надо установить :

♦ какая информация нуждается в защите;

♦ кого она может заинтересовать;

♦ каков “срок жизни” этих секретов;

♦ во что обойдется их защита.

Затем следует подготовить план по охране коммерческой тайны. Основываясь на зарубежном опыте, он должен состоять из двух разделов:

♦ предотвращение похищения секретной информации;

♦ предотвращение утечки секретной информации.

Для этого требуется:

♦ определить, какая коммерческая информация является секретом фирмы;

♦ установить места ее накопления;

♦ выявить потенциальные каналы утечки информации;

♦ получить консультацию по перекрытию этих каналов у специалистов;

♦ проанализировать соотношение затрат по использованию различных систем, обеспечивающих защиту секретной информации, и выбрать наиболее приемлемую;

♦ назначить людей, ответственных за каждый участок этой системы;

♦ составить график проверки состояния дел на участках.

Система обеспечения безопасности фирмы включает в себя следующие организационные мероприятия:

♦ контроль помещений и оборудования (обеспечение безопасности производственных и конторских помещений, охрана фото- и иного копировального оборудования, контроль за посетителями);

♦ работа с персоналом (беседы при приеме на работу, ознакомление вновь принятых с правилами защиты информации, обучению сохранению коммерческой тайны, работа с сотрудниками, подозреваемыми в хищении секретной информации, беседы с увольняющимися);

♦ организация работы с конфиденциальными с конфиденциальными документами (установление порядка делопроизводства, контроль за прохождением секретных документов, контроль за публикациями, рассекречивание и уничтожение конфиденциальных документов, охрана секретов других фирм);

♦ работа с конфиденциальной информацией, накопленной в компьютерах фирмы (создание систем защиты электронной информации от несанкционированного к ней доступа, обеспечение контроля за пользованием ЭВМ);

♦ защита коммерческих тайн фирмы в процессе заключения контрактов (здесь важно четко определить круг лиц, имеющих отношение к этой работе).

Вышеизложенный план является примерным. Однако во всех случаях защиты коммерческой тайны необходимо обратить особое внимание на документы, поскольку в нашей стране основные объемы коммерческой информации хранят в документах.

Руководитель должен упорядочить процессы фиксации секретной информации в деловых бумагах и организовать их движение таким образом, чтобы похищение конфиденциальных документов было бы затруднено на столько, что оно станет невыгодным для похитителя.

При работе с документами, содержащими коммерческую тайну, следует соблюдать определенные правила, которые сводятся к следующему:

♦ строгий контроль (лично или через службу безопасности) за допуском персонала к секретным документам;

♦ назначение ответственных лиц за контролем секретного делопроизводства и наделения их соответствующими полномочиями;

♦ разработка инструкции (памятки) по работе с секретными документами, ознакомление с ней соответствующих сотрудников фирмы;

♦ контроль за принятием служащими письменных обязательств о сохранении коммерческой тайны фирмы;

♦ введение материального и морального поощрения сотрудников, имеющих доступ к секретной информации;

♦ внедрение в повседневную практику механизмов и технологий защиты коммерческой тайны фирмы;

♦ личный контроль со стороны руководителя фирмы служб внутренней безопасности и секретного делопроизводства.

При работе с документами нельзя отлучаться из комнаты, а если приходится выходить, то необходимо закрыть дверь. Посторонних к документам допускать не следует. Документы, которые правомерно могут потребовать сотрудники налоговой инспекции или правоохранительных служб, следует держать отдельно от остальных конфиденциальных бумаг.

По окончании работы наиболее важные документы убираются в сейф, менее важные в специальные контейнеры. Те и другие следует опечатывать и сдать на хранение сотрудникам службы безопасности фирмы.

При пересылке документов следует иметь в виду, что использование телемониторов-игл позволяет через непроклееные уголки конвертов прочитать содержимое делового письма, не вскрывая его. Поэтому конверты с документами целесообразно дополнительно проклеить скотчем.

Доверяя свои бумаг почте необходимо отправлять их заказными письмами и письмами с уведомлением о вручении адресату.

Перемещения документов внутри фирмы также следует держать под контролем.

Организация защиты документов - обязанность руководителей фирмы и ее службы безопасности. Следует быть уверенным, что с момента появления до уничтожения документ к посторонним не попадал. Если документ утерян (украден), специалисты из службы безопасности должны провести расследование.

Подготовку документов, содержащих важные сведения, следует доверять проверенным людям. Количество экземпляров должно быть строго ограниченным. Для разделения документов по степени важности можно использовать яркие цветные наклейки. При необходимости следует определять степень конфиденциальности документа, а также срок действия ограничительных грифов. При этом необходимо помнить: чем больше секретной информации в нем отражено, тем больше потребуется затрат для его защиты.

Копирование документов - один из способов получения сведений, составляющих тайну фирмы. Множительная техника должна находится под надежным контролем. Количество копий должно строго учитываться, а их уничтожение - контролироваться. Следует придерживаться правила: наиболее ценные документы руководители фирм копируют сами.

Если документы размножаются на принтерах ЭВМ, то следует позаботиться о защите информации на магнитных носителях. Если это пишущая машинка, то следует принять меры по хранению перфоленты, позволяющей повторно печатать один и тот же текст в автоматическом режиме. По стуку клавишей пишущей машинки специалист с помощью электроники получит текст, аналогичный оригиналу, находясь вне помещения офиса.

Для работы с секретными документами должны отводиться специальные помещения с хорошей звукоизоляцией. В эти помещения не должны допускаться не только посторонние лица, но и сотрудники, не имеющие разрешения (допуска) на работу с секретами фирмы. Эти помещения должны иметь капитальные стены, надежные перекрытия, прочные двери с замками и запорами, защиту на окнах от проникновения посторонних лиц. Эти помещения должны надежно охраняться, в том числе системой охранной сигнализации, электронно-механическими приспособлениями, кабельным телевидением, и т.п.

Черновики секретных документов должны готовиться в тетрадях с пронумерованными листами. После подготовки документов “набело” черновики должны уничтожаться уполномоченными на это сотрудниками. Число копий секретных документов должно строго учитываться, а копировальные машины снабжаться счетчиком копий и колючем, запускающим машины в действие.

Копировальная бумага и красящая лента пишущих машин- предмет особых забот, так как с них можно снять секретную информацию. Поэтому использованная копировальная бумага и лента уничтожается под контролем ответственных лиц.

Вероятность утечки секретной информации из документов особенно велика в процессе их пересылки. Если нет возможности пользоваться услугами военизированной фельдсвязи, доставку секретных документов и ценностей следует организовать своими силами с привлечением сотрудников собственной службы безопасности или же обратиться в специализированные фирмы, которые такие услуги оказывают за плату.

Служащие фирмы, отвечающие за ее сохранность, использование и своевременное уничтожение секретных документов, должны быть защищены от соблазна торговли секретами фирмы простым, но весьма надежным способом - хорошей зарплатой.

В процессе хранения информации и пересылки секретных документов могут быть применены средства защиты и сигнализации при несанкционированном доступе к ним. Одна из новинок - светочувствительное покрытие, наносимое на документы, которое может проявиться под воздействием света, указывая тем самым на факт ознакомления с документами или их фотографирование посторонними лицами.

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

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

**Список использованной литературы**

коммерческий информация защита шпионаж

1. Гражданский кодекс Российской Федерации. Части первая и вторая.- М., 1999.

2. Уголовный кодекс Российской Федерации. М., 1998.

3. Долгополов Ю.Б. “Предпринимательство и безопасность”. М, 1991.

4. Казакевич О.Ю. и др. “Предприниматель в опасности: способы защиты (практическое руководство для предпринимателей и бизнесменов)”.- М., 1992.

5. Кавеладзе И.Т. Практика защиты коммерческой тайны в США (руководство по защите вашей деловой информации). М., 1992.

6. Раевский Г. “Угрозы экономической безопасности предприятия и задачи службы безопасности по их нейтрализации”, журнал “Частный сыск” №4, М., 1994.

7. Прашкевич Г.М. Шпион против алхимиков: Фант. Повести. - Екатеринбург: Тезис, 1994.-544 с.

8. Э.Я. Соловьева, проф. МГУ, “Коммерческая тайна и ее защита”.

9. Панкратов Ф.Г., Серегина Т.К. «Коммерческая деятельность». Москва 1998 г.