Министерство науки и образования Республики Казахстан

Колледж экономики и информационных технологий

**Курсовая работа**

На тему: "Предпринимательская тайна и механизм её защиты"

Выполнил: студент гр.9-521 Сабргалиева Д. М.

Проверил: преподаватель Филонова М. Е.

Уральск 2010г.

Оглавление

Введение

Сущность и значение предпринимательской информации

Понятие предпринимательской тайны

Защита предпринимательской тайны

Механизм и способы защиты предпринимательской информации

Заключение

Список использованной литературы

# 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 области 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.

В связи с развитием рыночных отношений предпринимательскую деятельность в нашей стране приходится осуществлять в условиях нарастающей неопределенности ситуации и изменчивости экономической среды. Значит, возникает неясность и неуверенность в получении ожидаемого конечного результата, а следовательно, возрастает риск, то есть опасность неудачи, непредвиденных потерь. В особенности это присуще начальным стадиям освоения предпринимательства.

Подобная обстановка несколько необычна и непривычна для нашего хозяйственника или просто гражданина, которому предстоит пройти тернистый путь, прежде чем он превратится в подлинного предпринимателя.

В условиях командно-административной экономики все мы привыкли к тому, что экономическая обстановка формируется “сверху" в приказном порядке в виде набора правил и норм. Планы, программы, постановления, инструкции, государственные цены, фонды, лимиты, наряды, тарифы формировали ту экономическую систему координат и хозяйственную среду, в которой вынуждены были действовать предприятия и люди.

Конечно, жесткая система централизованных установок и предписаний сковывала инициативу, подавляла интерес и творческое начало. Но она вносила явную или по крайней мере кажущуюся четкость, обеспечивала навязанный “порядок”.

Для ужесточения контроля на не национализированных предприятиях в 1917 году был принят декрет "О рабочем контроле". Отменяющий право собственности трудовых коллективов на производственную информацию (т.е. отменяющий понятие "предпринимательская тайна"). Однако в рыночной экономике информация становится товаром и должна подчиняться законам товарно-денежных отношений. Каждый собственник имеет право изменять свои интересы, согласованные с интересами других собственников и общества.

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.

Рынок есть прежде всего экономическая свобода. Над предпринимателем могут возвышаться только закон и устанавливаемые им ограничения. Государственное регулирование в условиях рынка сводится преимущественно к установлению норм осуществления предпринимательской деятельности и к налоговой системе. Все остальное определяется производителем и потребителем, их волей, а в какой-то степени складывается случайным образом.

За экономическую свободу приходится платить. Ведь свободе одного предпринимателя сопутствует одновременно и свобода других предпринимателей, которые вольны покупать или не покупать его продукцию, предлагать за нее свои цены, продавать ему по определенным ценам, диктовать свои условия сделок.

При этом естественно, что те, с кем приходится вступать в хозяйственные отношения, стремятся прежде всего к своей выгоде, а выгода одних может стать ущербом для других. К тому же предприниматель-конкурент вообще склонен вытеснить своего оппонента с рынка.

В новых рыночно-конкурентных условиях возникает масса проблем, связанных с обеспечением безопасности не только физических и юридических лиц, их имущественной собственности, но и предпринимательской (предпринимательской) 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:

* предпринимательская (коммерческая) информационная система (сведения о состоянии экономической системы, факторах, положительно или отрицательно влияющих на ту сферу хозяйствования и коммерции, в которой действует предприниматель)
* правовая информационная система (сведения о действующем законодательстве, регулирующем и охраняющем деятельность предпринимательских (коммерческих) структур)
* специально оперативная информационная система (сведения о способах, силах и средствах обеспечения безопасности предпринимательской информации от доступа третьих лиц).

# Сущность и значение предпринимательской информации

Предпринимательская деятельность во всех сферах неразрывно связана с получением и использованием различного рода информации. Причем в современных условиях информация представляет собой особого рода товар, имеющий определенную ценность. Для предпринимателя зачастую наиболее ценной является информация, которую он использует для достижения целей фирмы и разглашение которой может лишить его возможностей реализовать эти цели, то есть создает угрозы безопасности предпринимательской деятельности. Конечно, не вся информация может, в случае ее разглашения, создавать эти угрозы, однако существует определенная ее часть, которая нуждается в защите.

До принятия закона в Казахстане предприниматели и фирмы были вынуждены самостоятельно охранять конфиденциальную информацию. Суд или прокуратура, изъяв коммерческие документы, не несли ответственность за разглашение информации или передачу ее третьим лицам. Другими словами, надзорные или судебные органы при проведении проверок финансовой деятельности какой-нибудь компании могли "случайно" передать нужную информацию ее конкурентам и при этом остаться невиновными с точки зрения закона.

Во-первых, законодательство вводит само понятие предпринимательской тайны. Ею признается практически любая информация, представляющая действительную или потенциальную предпринимательскую ценность (научно-техническая, технологическая, производственная, финансово-экономическая и т.п.). Главное - определить в письменной форме, какая именно информация будет "засекречена".

В тексте закона оговаривается, что предпринимательскую тайну не могут составлять сведения о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, качестве пищевых продуктов и других факторах, связанных с обеспечением безопасности населения. Кроме того, не может засекречиваться информация о численности и составе работников организаций, о системе оплаты труда и задолженности работодателей по выплате зарплаты.

Во-вторых, устанавливаются сроки неразглашения предпринимательской тайны и меры ответственности за несоблюдение этого требования и причинение материального ущерба. Теперь работник обязан хранить "секреты фирмы" минимум три года с момента прекращения действия трудового договора (если работодателем не установлен конкретный срок), а в случае невыполнения этого требования он может не просто выплатить штраф, но и лишиться свободы на срок до десяти лет.

Наиболее важным нововведением в законе является то, что теперь пострадавшая от разглашения предпринимательской тайны компания сможет через арбитражный суд потребовать возмещения всего доказанного ущерба у того, кто воспользовался тайной, или у представителей власти, виновных в утечке секретов.

Перед властями, по закону, у предпринимателей предпринимательских тайн быть не должно. Более того, за непредоставление органам государственной власти (суду, прокуратуре и т.п.) и местного самоуправления информации, составляющей предпринимательскую тайну, по специальному требованию могут также привлечь к ответственности.

В связи с этим многие эксперты обеспокоены тем, что закон о предпринимательской тайне легализует вторжение власти в дела бизнеса. Если предпринимательскую тайну хочет узнать орган местного самоуправления, нужно внимательнейшим образом изучить цели такого шага. И если цели подозрительны - доводить дело до суда.

При отнесении той или иной информации к категории предпринимательской тайны следует учитывать два обстоятельства.

Во-первых, на практике возможны случаи, когда под предлогом охраны предпринимательской тайны могут скрывать сведения и документы, свидетельствующие о фактах злоупотреблений, бесхозяйственности и других нарушениях. Для исключения подобных ситуаций необходимо на общегосударственном уровне создать специальную систему регулирования взаимоотношений предприятия и контролирующих его органов.

Во-вторых, в условиях рынка чрезмерно засекречивать информацию становится невыгодно с экономической точки зрения. Информация все чаще выступает как рыночный товар, имеющий определенную цену и спрос. В отдельных промышленно развитых странах около половины валового национального продукта дают производство, распространение и переработка информации в различных видах.

В соответствии с Гражданским кодексом РК информация составляет служебную или предпринимательскую тайну в случае, когда информация имеет действительную или потенциальную предпринимательскую ценность, в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности.

По мнению специалистов, сведения, составляющие предпринимательскую тайну и подлежащие охране, должны удовлетворять следующим пяти критериям:

1. их открытое использование связано с ущербом для предприятия

2. они не являются общеизвестными или общедоступными на законных основаниях

3. предприятие сможет осуществить надлежащие меры по сохранению их конфиденциальности по соображениям экономической и иной выгоды

4. эти сведения нуждаются в защите, так как они не являются государственными секретами и не защищены авторским и патентным правом

5. сокрытие этих сведений не наносит ущерба обществу.

Анализ законодательных актов промышленно развитых стран по вопросам защиты предпринимательской тайны позволяет определить совокупность сведений, сокрытие которых противоречит интересам государства и общества. В наиболее общем виде это информация:

нерациональном природопользовании

сверхнормативном загрязнении окружающей среды

несоблюдении техники безопасности в производстве, представляющем реальную угрозу здоровью и жизни людей

нарушении специального законодательства, регулирующего деятельность предпринимателей (например, законов о качестве продукции и защите прав потребителя)

занятии деятельностью, не предусмотренной уставом данного предприятия или запрещенной законами данной страны

злоупотреблении и недобросовестности руководителей и работников фирмы

фактах проявления недобросовестной конкуренции

возможностях и реальных случаях, уклонения от правильной уплаты налогов

причинах и фактах невыполнения договоров и др.

Гражданским кодексом РК установлено, что "сведения, которые не могут составлять служебную или предпринимательскую тайну, определяются законом и иными правовыми актами". В настоящее время статья "О предпринимательской тайне" определяет перечень сведений, которые не могут составлять предпринимательскую тайну:

1) содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;

2) содержащихся в документах, дающих право на осуществление предпринимательской деятельности;

3) о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;

4) о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;

5) о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;

6) о задолженности работодателей по выплате заработной платы и по иным социальным выплатам;

7) о нарушениях законодательства РК и фактах привлечения к ответственности за совершение этих нарушений;

8) об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;

9) о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности непредпринимательской организации;

10) о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;

11) обязательность раскрытия, которых или недопустимость ограничения доступа, к которым установлена иными федеральными законами.

# Понятие предпринимательской тайны

Предпринимательская тайна, в соответствии с гражданским законодательством РК, это информация, которая имеет действительную или потенциальную предпринимательскую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель принимает меры к охране ее конфиденциальности. Следовательно, предпринимательская тайна не может быть общеизвестной и общедоступной информацией, открытое ее использование несет угрозу экономической безопасности предпринимательской деятельности, в связи с чем, предприниматель осуществляет меры по сохранению ее конфиденциальности и защите от незаконного использования.

Предпринимательская тайна - конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную предпринимательскую выгоду.

Первым вопросом, который необходимо решить при организации охраны предпринимательской тайны, является определение круга сведений, составляющих предпринимательскую тайну, а также возможное распределение их по категориям важности в зависимости от их ценности, 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 предпринимательской тайны должна не только не мешать работе предприятия, но даже способствовать его прибыльной деятельности.

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.

Для подготовки перечня сведений, относящихся к предпринимательской 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:

1. специалиста, владеющего финансовыми вопросами, конъюнктурой рынка и данными в отношении конкурирующих фирм

2. специалиста, полностью представляющего систему организации работы предприятия, ее особенности

3. специалиста, по связям с другими предприятиями, а также по вопросам заключения контрактов, договоров

4. специалиста, обладающего всеми сведениями о выпускаемой продукции, технологическом цикле ее проектирования 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 предпринимательской тайне. Однако это не означает, что следует обязательно знакомить всех привлекаемых экспертов с конкретными сведениями, могущими представлять предпринимательскую 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 предпринимательской тайны.

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

выделить все виды деятельности предприятия, приносящие прибыль на данный момент

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

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 предпринимательской 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, объемы, 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 предпринимательской тайной.

#

# Защита предпринимательской тайны

Лицо, правомерно обладающее технической, организационной или предпринимательской информацией, в том числе секретами производства (ноу-хау), неизвестной третьим лицам (нераскрытая информация), имеет право на защиту этой информации от незаконного использования.

Право на защиту нераскрытой информации от незаконного использования возникает независимо от выполнения в отношении этой информации каких-либо формальностей (ее регистрации, получения свидетельств и т.п.). Правила о защите нераскрытой информации не применяются в отношении сведений, которые в соответствии с законодательными актами не могут составлять служебную или предпринимательскую тайну (сведения о юридических лицах, правах на имущество и сделках с ним; сведения, подлежащие представлению в качестве государственной статистической отчетности и др.).

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 предпринимательская 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 объект 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.

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, шантажом 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, предпринимательскую 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.

Также заключается договор с сотрудником. Как правило, работодатели совмещают трудовой договор и соглашение о неразглашении предпринимательской тайны, указывая одним из пунктов обязательство работника не разглашать сведения, прописанные в отдельном документе - перечне сведений, которые считаются предпринимательской тайной предприятия. Этот перечень может меняться, а внести изменения в трудовой договор гораздо сложнее, чем в перечень. Кстати, в этом же документе можно указать порядок хранения и режим доступа к предпринимательской информации.

Также необходимо прописать и ответственность за нарушение договоренностей. Наказание может быть любым: от выговоров до увольнения, можно предусмотреть материальную ответственность в случае, если разглашение предпринимательской тайны причинит компании убытки. Некоторые работодатели в качестве меры пресечения даже предусматривают уголовную ответственность, однако на практике эта мера практически не реализуется и потому считается, скорее, психологическим моментом.

Типовых форм как соглашения о неразглашении, так и перечня сведений, относящихся к предпринимательской тайне, в законодательстве не предусмотрено. Кроме того, компания может также определить, кто уполномочен утверждать перечень коммерческих сведений: директор или коллегиальный орган. Кстати, разрабатывается перечень чаще всего всем коллективом: комиссия из представителей основных служб и департаментов разрабатывает и рассматривает все варианты сведений, которые могут считаться предпринимательской тайной.

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.

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 предпринимательской 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.

#

# Механизм и способы защиты предпринимательской информации

На каждом предприятии при создании системы защиты информации необходимо правильно организовать:

1. учет и охрану некоторых видов материалов и готовых изделий (особенно опытных образцов)

2. порядок делопроизводства с документами, содержащими предпринимательскую тайну (правила циркуляции, учета, хранения, уничтожения и др.)

3. контроль за средствами копирования и размножения документов

4. защиту предпринимательской информации в средствах связи и вычислительной техники

5. охрану территории предприятия и его основных зданий и сооружений

6. контроль за посещениями данного предприятия посторонними лицами.

Основные элементы защиты предпринимательской тайны предприятия представлены в таблице 1.

Таблица 1.

Механизм защиты предпринимательской тайны

|  |
| --- |
|  МЕХАНИЗМ ЗАЩИТЫ ПРЕДПРИНИМАТЕЛЬСКОЙ ТАЙНЫ |
| 1 | 2 |
| Регламентированный перечень сведений, относимых к предпринимательской тайне предприятия | Система контроля за средствами копирования и размножения документов |
| Система учета и охраны новых материалов и продукции | Порядок защиты предпринимательской информации в средствах связи и вычислительной техники |
| Система охраны территории предприятия, его основных зданий и сооружений | Порядок использования открытых каналов связи при передачи конфиденциальной информации |
| Система контроля за посещением предприятия посторонними лицами | Система мотивации и обучения персонала предприятия способам защиты предпринимательской тайны |
| Порядок делопроизводства с документами, содержащими предпринимательскую тайну | Специализированные службы по защите предпринимательской тайны предприятия |

Принимая во внимание казахстанскую специфику, выделяются следующие основные способы защиты информации, которые могут использоваться предпринимателями:

a) законодательный. Основан на соблюдении тех прав предпринимателя на конфиденциальную информацию, которые содержатся в казахстанском законодательстве, при обнаружении нарушения прав предпринимателя как собственника, владельца или пользователя информации должно быть обращение в соответствующие органы для восстановления нарушенных прав, возмещения убытков и т.п.

b) физическая защита - охрана, пропускной режим, специальные карточки для посторонних, использование закрывающихся помещений, сейфов, шкафов и пр.

c) организационный. Он включает:

1) введение должности или создания службы, ответственной за отнесением определенной информации к категории конфиденциальной, соблюдением правил доступа и пользования этой информацией

2) разделение информации по степени конфиденциальности и организация допуска к конфиденциальной информации только в соответствии с должностью или с разрешения руководства

3) соблюдение правил пользования информацией (не выносить за пределы служебных помещений, не оставлять без присмотра во время обеда, включить сигнализацию при уходе)

4) наличие постоянно действующей системы контроля за соблюдением правил доступа и пользования информацией (контроль может быть визуальный, документальный и др.).

d) технический. Используются такие средства контроля и защиты как сигнализирующие устройства, видеокамеры, микрофоны, средства идентификации, а также программные средства защиты компьютерных систем от несанкционированного доступа.

e) работа с кадрами. Предполагает активную работу кадровых служб фирмы по набору, проверке, обучению, расстановке, продвижению, стимулированию персонала, с обязательным учетом анкетных данных и проверочных результатов тестирования следует регулярно проводить инструктажи персонала о необходимости соблюдения правил пользования конфиденциальной информацией и об ответственности за нарушения.

Основные способы защиты предпринимательской информации представлены на рис.1

Рис.1 Основные способы защиты предпринимательской информации

Часть этих способов предполагает значительные финансовые расходы, в связи, с чем использование всех способов одновременно по средствам только достаточно крупным и платежеспособным фирмам.

# Заключение

Подводя итог можно сказать, что предпринимательская деятельность во всех сферах неразрывно связана с получением и использованием различного рода информации. Причем в современных условиях информация представляет собой особого рода товар, имеющий определенную ценность. Для предпринимателя зачастую наиболее ценной является информация, которую он использует для достижения целей фирмы и разглашение которой может лишить его возможностей реализовать эти цели, то есть создает угрозы безопасности предпринимательской деятельности. Информация, используемая в предпринимательской деятельности весьма разнообразна.

Защита предпринимательской информации как часть деятельности по обеспечению безопасности предпринимательства в целом, предполагает, что возможные противоправные посягательства на предпринимательскую информацию могут идти по различным направлениям. В связи с этим эффективная защита информации должна предусматривать целую систему мер и направлений деятельности, каждому из которых соответствует свой способ защиты.

Для реализации этих мер в каждой компании рекомендуется разработать и утвердить положение "О предпринимательской тайне в компании", с которым должны быть под роспись ознакомлены все сотрудники компании. С сотрудниками, допущенными к работе с конфиденциальными документами, целесообразно заключить Обязательство о неразглашении и защите предпринимательской тайны и служебной информации. Рекомендуется также в целях предотвращения неправомерного использования конфиденциальной информации отслеживать репутацию своих сотрудников, а также случаи приобретения ими материальных ценностей или действий, требующих наличия крупных денежных сумм (покупки квартир, дорогих автомашин, зарубежных поездок и т.п.).

Кроме того, следует учитывать мировой опыт по защите предпринимательской информации. В разных странах существуют различные приоритетные направления защиты предпринимательской информации (предпринимательской тайны). Так, в Германии преобладают законодательные меры, в США и Франции, наряду с ними, предпочтение отдается организации собственных служб безопасности фирм, для Японии характерен корпоративный дух и долгосрочная занятость в фирме, в Великобритании защита обеспечивается договорными обязательствами

Конечно, каждый руководителя сам решает какую информацию защищать, и каким образом, но стоит заметить, что рентабельность и рост фирмы в целом, зависит не только от того, как ведется бизнес, но и от того, как он защищается.

# Список использованной литературы

1. Долгополов Ю.Б., "Предпринимательство и безопасность", Универсум, 2003 стр.65

2. "Гражданский кодекс Республики Казахстан" (общая часть) на электронном носителе от 1 января 2006 года

3. Гражданское право. Том 1. Учебник / Отв. ред. М.К. Сулейменов, Ю.Г. Басин. Алматы. 2000. С.234.

4. Общая экономическая теория (политэкономия): Учебник / Под общ. ред.

акад.В.И. Видяпина, акад. Г.П. Журавлевой. - М., 1995. - С.95.

5. Ярочкин В.И. Системы безопасности фирмы. Концепции. Правовые основы. Организационная структура. - М., 2003 стр.184