#### МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

##### НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

**Контрольная работа по курсу «Основы предпринимательской деятельности»**

**Тема: «Коммерческая тайна в предпринимательской деятельности »**

Выполнил: студент 4 курса

Шифр 400466717

Группа ОТЗ-667

Макаров Сергей Федорович

Г. Горно-Алтайск

20010г.

**Содержание**

**Введение………………………………………………………………….3**

**Сущность и значение коммерческой информации…………………4**

**Порядок отнесения коммерческих сведений к коммерческой тайне предприятия..10**

**Защита коммерческой тайны………………………………………….14**

**Заключение……………………………………………………………….20**

**Список литературы…………………………………………..………….22**

**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.

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 новых 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).

**Сущность и значение коммерческой 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.

Информация, используемая в предпринимательской деятельности весьма разнообразна. Ее можно разделить на два вида: промышленная и коммерческая.

К промышленной относится: информация о технологии и способе производства, технических открытиях и изобретениях, “ноу-хау”, конструкторская документация, программное обеспечение и т.п. Коммерческая информация – о финансово-экономическом положении предприятия (бухгалтерская отчетность), кредитах и банковских операциях, о заключаемых договорах и контрагентах, структуре капиталов и планах инвестиций, стратегических планах маркетинга, анализе конкурентоспособности собственной продукции, клиентах, планах производственного развития, деловой переписке и пр. Вся эта информация представляет различную ценность для самого предпринимателя и, соответственно, ее разглашение может привести (либо не привести) к угрозам экономической безопасности различной степени тяжести.

Поэтому информацию необходимо разделить на три группы: a) информация для открытого пользования любым потребителем в любой форме; b) информация ограниченного доступа – только для органов, имеющих соответствующие законодательно установленные права (милиция, налоговая полиция, прокуратура); c) информация только для работников (либо руководителей) фирмы. Информация относящаяся ко второй и третьей группам является конфиденциальной и имеет ограничения в распространении.

Конфиденциальная информация – это документированная (то есть зафиксированная на материальном носителе и с реквизитами, позволяющими ее идентифицировать) информация, доступ к которой ограничивается в соответствии с законодательством РФ. Часть этой коммерческой информации составляет особый блок и может быть отнесена к коммерческой тайне.

Коммерческая тайна предприятия - это не являющиеся государственными секретами сведения, связанные с производством, технологической информацией, управлением, финансами др., разглашение (передача, утечка) которых может нанести ущерб его интересам. Такова общая характеристика категории «коммерческая тайна» предприятия, определенная законодательно [4].

Обобщение различных точек зрения отечественных и зарубежных авторов позволяет дать расширенную трактовку этой весьма сложной категории. В наиболее общем виде она включает информацию [5]:

. о торговых отношениях фирм

. об организации и размерах оборота средств

. о состоянии рынка сбыта

. о банковских операциях

. о поставщиках и потребителях

. о содержании патентов

. о структуре капиталов

. о планах инвестиций

. о заключенных контрактах

. о формировании цены на товар

. о размере прибыли и объеме производства.

Производственная тайна включает информацию:

. о способах производства и технологии

. об организации труда

. о технических открытиях и изобретениях

. о целях и характере исследовательских работ.

Целесообразно также в общем объеме коммерческой информации выделять два основных блока. Согласно этому подходу, к категории научно-технической и технологической информации относятся сведения о конструкции машин и оборудования, используемых материалах, методах и способах производства, дизайне, программном обеспечении ЭВМ и др. [5].

К категории деловой информации относятся :

. финансы предприятия (финансовая отчетность, состояние расчетов с клиентами, задолженность, кредиты, платежеспособность, прибыль, себестоимость продукции и др.)

. стратегические и тактические планы развития производства, в том числе с использованием новых технологий, изобретений, ноу-хау

. планы и объемы реализации продукции (планы маркетинга, характер и объем торговых операций, уровень цен, складские запасы)

. анализ конкурентоспособности своей продукции, эффективности экспорта и импорта, предполагаемое время выхода на рынок

. планы рекламной деятельности

. списки торговых и других клиентов, конкурентов, сведения о взаимоотношениях с ними, их финансовом положение, условиях контрактов и др.

. методы и организация управления

. собственная оценка характера и репутации персонала и предприятия

. система организации труда.

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

Во-первых, на практике возможны случаи, когда под предлогом охраны коммерческой 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 Российской Федерации [1, ст. 139, п.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.

По мнению специалистов, сведения, составляющие коммерческую тайну и подлежащие охране, должны удовлетворять следующим пяти критериям оценки [4]: a) их открытое использование связано с ущербом для . предприятия b) они не являются общеизвестными или общедоступными на законных основаниях c) предприятие сможет осуществить надлежащие меры по сохранению их конфиденциальности по соображениям экономической и иной выгоды d) эти сведения нуждаются в защите, так как они не являются государственными секретами и не защищены авторским и патентным правом e) сокрытие этих сведений не наносит ущерба обществу.

Анализ законодательных актов промышленно развитых стран по вопросам защиты коммерческой тайны позволяет определить совокупность сведений, сокрытие которых противоречит интересам государства и общества. В наиболее общем виде это информация [6]: a) о нерациональном природопользовании; b) о сверхнормативном загрязнении окружающей среды; c) о несоблюдении техники безопасности в производстве, представляющем реальную угрозу здоровью и жизни людей; d) о нарушении специального законодательства, регулирующего деятельность предпринимателей (например, законов о качестве продукции и защите прав потребителя); e) о занятии деятельностью, не предусмотренной уставом данного предприятия или запрещенной законами данной страны; f) о злоупотреблении и недобросовестности руководителей и работников фирмы; g) о фактах проявления недобросовестной конкуренции; h) о возможностях и реальных случаях, уклонения от правильной уплаты налогов; i) о причинах и фактах невыполнения договоров и др. Гражданским кодексом Российской Федерации [1, ст. 139, п. 1] установлено, что «сведения, которые не могут составлять служебную или коммерческую тайну, определяются законом и иными правовыми актами». В настоящее время в Российской Федерации действует постановление Правительства РСФСР от 5 декабря 1991 года № 35 «О перечне сведений, которые не могут составлять коммерческую тайну».

В нашей стране, по оценкам специалистов, неоправданная секретность приносит народному хозяйству большой ущерб. Современное общество заинтересовано в раскрытии многих «тайн» производства в целях обмена информацией и ускорения научно-технического прогресса. Следует иметь в виду, что при охране государственных секретов во многих случаях невозможно определить количественно стоимость защищаемой информации. Поэтому уровень затрат общества на защиту государственных секретов определяется необходимостью обеспечить максимально высокую степень защиты. Несколько иным должен быть подход к обоснованию размеров затрат предприятия на защиту своей информации. Практика показывает, что при охране коммерческой тайны возможные потери от утечки информации часто имеют конкретную стоимостную оценку. Поэтому и затраты на защиту такой информации должны быть экономически ограничены суммой возможных потерь. При излишнем засекречивании коммерческой информации рост расходов на эти цели неадекватен снижению вероятности утечки наиболее ценных сведений. Целесообразно охранять как коммерческую тайну только ту часть информации предприятия, которая обеспечивает возможность расширять рынок сбыта продукции, существенно улучшать ее качество, заключать особо выгодные сделки с партнерами.

Если государство при размещении госзаказа на промышленном объекте считает необходимым засекретить какую-либо информацию, то оно обязано за это платить предприятию. В подобной ситуации специальным договором определяется перечень сведений, сохраняемых в тайне, оговариваются расходы предприятия на обеспечение защиты и степень участия государства в этих расходах. На практике довольно часто руководители и предприниматели не вполне четко, представляют себе, что входит в понятие «коммерческая тайна», как ее следует охранять и как результаты подобной работы могут влиять на экономическое положение предприятия.

По оценкам экспертов, потеря лишь четверти информации, относимой к категории коммерческой тайны, обеспечивает весомые преимущества конкурентам и в течение нескольких месяцев приводит к банкротству половины фирм, допустивших утечку сведений. Есть все основания полагать, что по мере развития рыночных отношений с присущими им конкуренцией и хозяйственным расчетом подходы к охране коммерческой тайны радикально изменятся [4].

В рыночной экономике информация является товаром и ее получение, хранение, передача и использование должны подчинятся законам товарно- денежных отношений. Каждый собственник имеет право охранять свои интересы и защищать необходимую информацию, получая при этом определенную свободу предпринимательства. Право на тайну означает ограничение государственного вмешательства в экономическую жизнь предприятия и защиту его интересов при взаимодействии с другими субъектами рыночных отношений. В отличие от государственных и военных секретов, коммерческая тайна является собственностью конкретного предприятия. Ее главное назначение - обеспечивать предприятию экономические преимущества в конкурентной борьбе.

В экономике нашей страны государство в лице своих многочисленных органов длительное время занимало монопольное положение в области засекречивания и охраны различной информации. Это объяснялось преобладающей долей государственной собственности на средства производства и продукты труда. Нередко возникали и такие ситуации, когда страна уступала приоритеты в различных областях науки и производства из-за бесхозяйственного отношения к идеям рационализаторов, изобретателей и ученых. Продукты интеллектуальной деятельности уходили за рубеж, а через некоторое время за значительные валютные суммы нам приходилось покупать там продукцию, изготовленную с использованием наших разработок. Утечке за рубеж интеллектуальной продукции (идей, предложений, изобретений, открытий) во многом способствовала устоявшаяся ранее в стране система присвоения ученых степеней ориентированная на число статей, опубликованных в зарубежных научных журналах. Такие «легальные» каналы утечки интеллектуальной информации были чрезвычайно широки. Затрачивая немалые средства на ее получение, мы часто «за так» отдавали, ее западным фирмам, которые имели от ее использования немалые доходы.

В сегодняшних условиях рыночных конкурентных отношений утечка такой информации может негативно отразиться положении предприятия в борьбе за потребителя. Именно поэтому в настоящее время целесообразно юридически точно определить категорию и правовой статус коммерческой тайны, разработать механизм ответственности за ее разглашение. Интересы отдельных предприятий должны быть безусловно подчинены интересам страны. Параллельно с развитием приватизации и становлением предпринимательства в нашей стране необходимо создание системы, обеспечивающей продажу информации предприятия за рубеж без ущерба для государства в целом. В промышленно развитых странах такие системы есть Они предусматривают различные эффективные методы экономического воздействия на частных предпринимателей, позволяющих себе в ущерб национальным интереса страны нарушать запреты государства на экспорт; научно-технической продукции.

В нашей стране в настоящее время отсутствует законодательная защита коммерческой тайны, не практикуется широкое применение мер экономической ответственности при решении этой проблемы, не наработана соответствующая судебная практика. Возможно, именно поэтому в реальной жизни предприятий процветает явное и тайное безвозмездное заимствование интеллектуальной собственности и коммерческой информации конкурентов (кооперативов, малых предприятий и частных лиц).

Экономическая безопасность предприятий нарушается прежде всего, в том случае, когда его сотрудники подрабатывают по совместительству в других местах, используя при этом документацию (методики, чертежи, программы и другую созданную на основном предприятии, но юридически не закрепленную в его собственности. А ведь именно эта интеллектуальная продукция (знания и технология) нередко составляет наиболее ценный капитал предприятия. Любой субъект хозяйственных отношений, использующий данную информацию обязан при этом заключать с предприятием договор и отдавать ему часть прибыли, получаемой от использования достижений. Однако нынешняя экономическая и правовая проработка данного вопроса не позволяет предприятию – собственнику информации заявить и реализовать свои претензии.

Для решения этой проблемы целесообразно законодательно ограничить (а в отдельных случаях - полностью запретить) бесплатный доступ к опыту отдельных предприятий. В то же время необходимо регламентировать порядок купли-продажи приоритетных разработок с учетом их реальной рыночной стоимости. Предприниматели должны подготовиться к переходу внутреннего рынка на патентно-лицензионную систему охраны промышленной собственности. На предприятиях целесообразно укрепить соответствующие подразделения патентно-лицензионных отделов, ввести необходимых специалистов в маркетинговые службы, организовать собственными усилиями эффективную систему защиты информации.

В перспективе на макроуровне необходимо разработать и принять специальный закон о коммерческой тайне. Именно при переходе к рыночным отношениям может стать надежным гарантом защиты интересов отдельных предприятий с страны в целом. Специалисты научно-технических, производственных, экономических и других служб предприятия должны научиться правильно и конкретно (в стоимостной форме) оценивать предполагаемые и реальные потери фирмы вследствие утечки информации, относимой к категории коммерческой тайны.

В наиболее общем виде потери предприятия от несоблюдения условий конфиденциальности сводятся к тому, что [6]: a) снижаются возможности продажи лицензий на собственные научные разработки, теряется приоритет в освоенных областях научно- технического прогресса, растут затраты на переориентации деятельности исследовательских подразделений; b) появляются (или искусственно создаются конкурентами) трудности в закупках сырья, технологии, оборудования и других компонентов нормальной производственной деятельности; c) ограничивается сотрудничество предприятия с деловыми партнерами, снижается вероятность заключения выгодных контрактов, возникают проблемы в выполнении договорных обязательств; d) растут затраты предприятия на создание новой рыночной стратегии, изменение структуры маркетинговых исследований и др.; e) возникает реальная угроза применения экономических санкций к виновным в разглашении коммерческой тайны.

Точный стоимостный расчет совокупной величины всех потерь достаточно сложен, трудоемок, а иногда и невозможен из-за отсутствия достоверных исходных данных. Поэтому в большинстве случаев достаточно укрупненной экспертной оценки потерь предприятия, обусловленных несоблюдением требований защиты информации. Компенсация перечисленных выше потерь предприятия требует нередко значительных дополнительных затрат, что снижает эффективность производства в целом и возможность успеха в конкурентной борьбе. Именно поэтому вопросам защиты коммерческой тайны в настоящее время уделяется все больше внимания.

1.1 Понятие коммерческой информации и коммерческой тайны

Коммерческая тайна, в соответствии с гражданским законодательством РФ [1], это информация которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель принимает меры к охране ее конфиденциальности. Следовательно, коммерческая 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.

Коммерческая тайна - это право на определенную свободу предпринимательства, защиту своих интересов во взаимоотношениях с государством и другими субъектами рыночных отношений. Право на коммерческую тайну это ограничение государственных возможностей командовать в экономике[5].

**Порядок отнесения коммерческих сведений к коммерческой тайне предприятия**

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, утверждаемом руководителем предприятия. При разработке Перечня необходимо учитывать требования постановления Правительства Российской Федерации от 5.12.91 №35 “О передаче сведений, которые не могут составлять коммерческую тайну” [3]. 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 [4]: a) специалиста, владеющего финансовыми вопросами, конъюнктурой рынка и данными в отношении конкурирующих фирм; b) специалиста, полностью представляющего систему организации работы предприятия, ее особенности c) специалиста, по связям с другими предприятиями, а также по вопросам заключения контрактов, договоров d) 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 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:

. 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 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, 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 [5].

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 объектов 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 отечественной 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 объем публикуемых данных не должен быть достаточным для самостоятельного внедрения без дополнительной информации разработчика, которая именно и подлежит защите.

**Защита коммерческой тайны**

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, шантажом представителей других предпринимательских фирм. В принципе здесь идет обоюдная проверка заказчика и клиента перед тем, как заключить договор. Игнорирование этого подхода может привести к серьезным ошибкам.

Специальные меры, которые осуществляются при защите информации, можно подразделить на внешние и внутренние [10].

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 [11].

Как показывает зарубежная практика работы частных фирм, утечка информации зачастую происходит по инициативе их же сотрудников [10]. 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 [5].

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 [10].

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, сре6ди 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...”.

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.

В дополнение к сказанному, на каждом предприятии при создании системы защиты информации необходимо правильно организовать [6]: a) учет и охрану некоторых видов материалов и готовых изделий (особенно опытных образцов); b) порядок делопроизводства с документами, содержащими предпринимательскую тайну (правила циркуляции, учета, хранения, уничтожения и др.); c) контроль за средствами копирования и размножения документов; d) защиту коммерческой информации в средствах связи и вычислительной техники e) охрану территории предприятия и его основных зданий и сооружений; f) контроль за посещениями данного предприятия посторонними лицами.

Основные элементы защиты коммерческой тайны предприятия представлены в таблице 1.

ТАБЛИЦА 1 – Механизм защиты коммерческой тайны предприятия

|МЕХАНИЗМ ЗАЩИТЫ КОММЕРЧЕСКОЙ ТАЙНЫ |

|1 |2 |

|Регламентированный перечень |Система контроля за средствами |

|сведений, относимых к коммерческой |копирования и размножения |

|тайне предприятия |документов |

|Система учета и охраны новых |Порядок защиты коммерческой |

|материалов и продукции |информации в средствах связи и |

| |вычислительной техники |

|Система охраны территории |Порядок использования открытых |

|предприятия, его основных зданий и |каналов связи при передачи |

|сооружений |конфиденциальной информации |

|Система контроля за посещением |Система мотивации и обучения |

|предприятия посторонними лицами |персонала предприятия способам |

| |защиты коммерческой тайны |

|Порядок делопроизводства с |Специализированные службы по защите |

|документами, содержащими |коммерческой тайны предприятия |

| коммерческую тайну | |

**Заключение**

В данном курсовом проекте рассматривались вопросы по коммерческой тайне предприятия и ее защите. Разрабатывались методики по приему на работу будущего персонала, помогающее установить и выявить степень профессиональной пригодности и надежности личности.

Подводя итоги теоретической и расчетной части данного проекта можно сказать. 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. Информация, используемая в предпринимательской деятельности весьма разнообразна. Ее можно разделить на два вида: промышленная и коммерческая. Защита коммерческой информации как часть деятельности по обеспечению безопасности предпринимательства в целом, предполагает, что возможные противоправные посягательства на коммерческую информацию могут идти по различным направлениям. В связи с этим эффективная защита информации должна предусматривать целую систему направлений деятельности, каждому из которых соответствует свой способ защиты.

Кроме того, следует учитывать мировой опыт по защите коммерческой информации. В разных странах существуют различные приоритетные направления защиты коммерческой информации (коммерческой 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. Принимая во внимание российскую 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 российском законодательстве. при обнаружении нарушения прав предпринимателя как собственника, владельца или пользователя информации должно быть обращение в соответствующие органы (МВД, ФСБ, прокуратуру, суд) 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.

Часть этих способов предполагает значительные финансовые расходы, в связи с чем использование всех способов одновременно по средствам только достаточно крупным и платежеспособным фирмам. Разработка данной методики курсового проекта позволяет дать профессионально грамотный анализ в сфере работы подбора кадров и помогает избежать такие проблемы - как утечка конфиденциальной информации и соответственно исключить финансовые потери предприятия.

**Список литературы**

1. «Гражданский кодекс Российской Федерации», “ИНФРА-М”, М, 1995

2. Закона Российской Федерации «О государственной тайне»

3. Постановление Правительства РСФСР "О передаче сведений, которые не могут составлять коммерческую тайну" от 5 декабря 1991 № 35.

4. Долгополов Ю.Б.,“Предпринимательство и безопасность”, “Универсум”, М.,

1991

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

6. Казакевич О.Ю., Конев Н.В., Максименко В.Г. и др. Предприниматель в опасности: способы защиты. Практическое руководство для предпринимателей и бизнесменов. - М.: Юрфак МГУ, 1992

7. Капитонов Э.А. Социология XX века. Ростов-на-Дону, издательство

«Феникс», 1996

8. Коновалов В.Д. Психологические тесты – 1, М., СВЕТОТОН, 1996

9. Лапуста М.Г. «Справочник директора предприятия», М. «ИНФРА-М», 1996

**Задача по курсу «Основы предпринимательской деятельности»**

**Наименование статей**

1. Затраты на сырье и материалы, руб. 350
2. Трудоемкость изготовления изделия рабочим 5 разряда, нормо-часов 43
3. Часовая тарифная ставка рабочего 5 разряда, руб. 38
4. Дополнительная заработная плата (от основной заработной платы), % 13
5. Расходы по содержанию и эксплуатации оборудования (от основной заработной платы), % 105
6. Цеховые расходы (от основной заработной платы), % 80
7. Общепроизводственные расходы (от основной заработной платы), % 80
8. Коммерческие расходы, % 5
9. Прибыль с точки зрения предпринимателя, % 28
10. Выпуск продукции, тыс.шт. 6,5
11. НДС, % 18
12. ЕСН, % 26

С= М+Зо+Зд+Нес+Зэкс+Зоц+Зоз+Зпр+Зк

Где:

М- затраты на основные материалы = 350

Зо- основная з/п производственных рабочих = 1634

Зд- дополнительная з/п вспомагат. рабочих = 212,42

Нес- отчисления на соц. нужды. ЕСН-26% = 424,84

Зэкс- расходы на содержание и эксплуотацию оборудования = 1715,7

Зоц- общецеховые расходы = 1307,2

Зоз- общезаводские расходы = 1307,2

Зпр- прочие расходы. НДС-18% = 294,12

Зк- коммерческие расходы = 81,7

С = 7327,18

Цизд= Спол + 0,4\*Спол

Цизд = 10258,052 руб.

Использованный метод ценообразования- метод полных издержек.

Предприятие близко к монопольному и сбыт продукции практически гарантирован.

Этот метод наиболее эффективен при расчете цен на товары пониженной конкурентоспособности.

**График безубыточности**

70000

Прямая выручка от реализации

60000

50000

Переменные затраты

40000

20000

10000

2621 постоянный затраты

2 4 6 6.5 7