Раздел 1. Общественная роль и экономическая основа бизнеса

Тема: Информационная безопасность предпринимательских структур

Цели занятия:

- обучающая: закрепить теоретические знания по теме, углубить и расширить, систематизировать и проконтролировать знания, сформировать умения и навыки студентов по теме.

- развивающая: развитие творческого подхода к решению самых разнообразных задач; формировать и развивать умение анализировать, выделять главное, вести конспект.

- воспитательная: формирование интереса к профессии у студентов, формирование определенных черт гармонически развитой личности

Формируемые компетенции: осознание социальной значимости будущей профессии; стремление к саморазвитию, повышению своей квалификации и профессионального уровня.

Лекция № 4

(2часа)

План

1. Понятие предпринимательской тайны

2. Защита предпринимательской тайны

3. Шпионаж

1. Понятие предпринимательской тайны

Предпринимательская деятельность во всех сферах экономики неразрывно связана с получением, накоплением, хранением и использованием различных сведений, характеризующих как саму фирму, так и связанных с нею партнеров.

Обеспечение сохранности информации о деятельности фирмы, всех ее факторах развития является условием выживания фирмы в рыночной конкурентной среде.

Конкуренты фирмы могут осуществлять различные формы получения достоверной информации о ее деятельности, чтобы добиться лучших успехов на рынке.

Предпринимательская тайна - включает любые сведения (информацию), разглашение которых (утечка) может нанести экономический и моральный ущерб предпринимательской организации, существенно повлияет на ее деловую репутацию.

Предпринимательская тайна по существу представляет интегрированную совокупность производственной, технической, коммерческой и служебной тайны, сохранение которой обеспечивает фирме возможность добиваться планируемых результатов.

Но не вся информация может быть отнесена к коммерческой тайне. К сведениям, которые не могут составлять коммерческую тайну относятся:

· учредительные документы организации;

· документы, дающие право на занятие определенными видами предпринимательской деятельности;

· документы о платежеспособности организации;

· сведения о результатах финансово-хозяйственной деятельности и иные сведения, необходимые для проверки правильности исчисления и уплаты налогов и других обязательных платежей;

· сведения о численности, составе работающих, их заработной плате и условиях труда, а также о наличии свободных рабочих мест и другие.

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 экономическим издержкам. Правильная организация выделения и защиты предпринимательской тайны должна не только не мешать работе предприятия, но даже способствовать его прибыльной деятельности.

Так, крупнейшие в мире производит ли 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.

2. Защита коммерческой тайны

Недостаточная защита предпринимательской тайны может существенным образом повлиять на конечные результаты деятельности организации, на уровень используемых ресурсов, качество товаров (работ, услуг), ее финансовое положение, ее положение на товарных рынках. Угрозы организации при утечке важных сведений (информации) могут быть потенциально возможными и реальными, по уровню влияния на результаты и условия функционирования они могут различаться от еле ощутимых до катастрофических, когда их воздействие приводит к несостоятельности, банкротству фирмы. По воздействию лиц (организаций) на сбор, утечку и передачу информации угрозы подразделяются на внутренние и внешние. Так, к внутренним угрозам можно отнести следующие факторы:

· излишнюю болтливость сотрудников за пределами организации;

стремление сотрудников зарабатывать любыми средствами, способами и ценой;

· привычку сотрудников делиться друг с другом производственными секретами (информацией, не подлежащей разглашению);

· наличие предпосылок для возникновения среди работников конфликтных ситуаций; случайный подбор кадров;

· слабую работу службы безопасности или ее отсутствие и др.

Для предпринимателя как собственника целесообразно постоянно выявлять реальные угрозы несохранения предпринимательской тайны путем:

· выяснения, кого (физических, юридических лиц) может заинтересовать защищаемая информация, составляющая тайну;

· установления методов, используемых злоумышленниками, для получения информации об условиях и результатах деятельности фирмы;

· правильной оценки возможных источников и объектов предпринимательской тайны;

· определения и оценки вероятных каналов утечки информации.

В зависимости от вида предпринимательской деятельности, размеров фирмы и других критериев ее функционирования состав элементов

механизма защиты предпринимательской тайны может кардинально изменяться. Важную роль играют и финансово-материальные возможности, необходимые для организации защиты экономической безопасности фирмы.

В состав механизма защиты предпринимательской тайны и безопасности организации входят следующие подсистемы:

· правовое обеспечение тайны;

· проведение организационной защиты;

· осуществление инженерно-технической защиты;

· мотивация в первую очередь тех сотрудников, от поведения которых зависит утечка сведений, составляющих предпринимательскую тайну;

· усиление различных форм ответственности за разглашение сведений, наносящих экономический ущерб фирме, и др.

Особое значение имеет организация инженерно-технической защиты, которая представляет собой совокупность специальных инженерно-технических средств, применение которых обеспечивает безопасность организации, сохранность ее имущества, ресурсов, а также сведений о ее деятельности.

Меры, принимаемые для предотвращения утечки сведений, составляющих предпринимательскую тайну. Основным фактором, способствующим защите информации, пока остаются режимные, т.е. специальные меры, направленные на предотвращение утечки конкретных сведений. Принятие специальных мер зависит, прежде всего, от владельца (владельцев) информации, конкурентной обстановки, ценности, которую представляет производственная или коммерческая информация, и других факторов.

Хранение секретной информации для владельца, если она больше никому не известна, не представляет большой сложности и не вызывает затрат на охрану. Владелец сам должен не допускать к ней третьих лиц. При этом он не должен быть болтливым, доверчивым. Носитель информации (документ, дискета, предмет) должен иметь соответствующее место для хранения (сейф или другое недоступное для других лиц место). Несколько усложняется охрана этих сведений, когда об их наличии становится известно заинтересованным лицам, поэтому необходимо ограничивать доступ посторонних лиц к месту хранения секретных материалов.

Организация, где имеется не один владелец информации, а несколько, к тому же работают сотрудники, не допущенные к производственным (коммерческим) секретам, представляет собой более сложный объект защиты.

Возникает вопрос о необходимости обеспечения внешней и внутренней безопасности структурных подразделений организации. Для его решения можно использовать частные предпринимательские фирмы, частные службы безопасности (т.е. те, которые функционируют самостоятельно, принимая заказы от клиентов), собственные службы безопасности. При этом целесообразно получить достоверную информацию о деятельности частной службы безопасности перед тем, как обратиться к ней за помощью. Почему? Имеются данные, что некоторые частные детективные организации, вместо того, чтобы действовать в соответствии со своим уставом, занимаются вымогательством, шантажом представителей других предпринимательских организаций. В принципе стоит вопрос об обоюдной проверке заказчика и клиента перед тем, как заключить договор. Игнорирование этого подхода может привести к серьезным ошибкам.

Принимаемые меры по защите сведений, составляющих предпринимательскую тайну, следует подразделять на внешние и внутренние.

К внешним мероприятиям относятся изучение партнеров, клиентов, с которыми приходится вести хозяйственную, коммерческую деятельность, сбор информации об их надежности, платежеспособности и другие данные. При необходимости изучаются связи сотрудников фирмы, выясняются лица, проявляющие интерес к фирме, ее деятельности, сотрудникам, их принадлежность к конкурирующей фирме или 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 предпринимательской фирме. По возможности следует установить, в чем суть этого интереса и кому понадобилась та или иная информация, не возникнет ли этот интерес в будущем, т.е. что можно ожидать от конкурента (не исключено и преступных элементов).

В ходе осуществления внутренних мероприятий по обеспечению безопасности организации следует решать такие вопросы как подбор, проверка лиц, желающих поступить на работу; изучение их анкетных данных, поведения по месту жительства и прежней работы, личностные и деловые качества, положительные и отрицательные стороны изучаемого лица, межличностные отношения; находилось ли это лицо в конфликте с законом (судимость, административные задержания, связь с преступным миром).

Как показывает зарубежная и отечественная 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.

Компьютеризация предпринимательских организаций, накопление с ее помощью различной информации привлекают как конкурентов, так и преступников. Часто 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 действий в интересах конкурента, могут совершиться и действия, преследуемые по закону: мошенничество, саботаж, повреждение ЭВМ.

Организации, располагающие ценной информацией, должны хранить ее в специальных несгораемых шкафах или сейфах, не допускать утери ключей от них или передачи их 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, вместе с комплексом защитных (физических и технических) мер здания, где расположен сейф, иное хранилище.

В экономической литературе, исследующей развитие предпринимательской деятельности, обращается внимание на поддержание этики честной коммерческой деятельности

3. Шпионаж

Одним из наиболее опасных для нормального осуществления предпринимательства видов незаконной деятельности является коммерческий шпионаж.

Коммерческий шпионаж – это действия лиц, направленные на незаконное получение коммерческой информации, находящейся под защитой. Коммерческий шпионаж включает в себя промышленный шпионаж, производственный, научно-технический, коммерческий, экономический и т.п. Объектом коммерческого шпионажа является информация, составляющая коммерческую тайну. Как уже отмечалось, к ней относится информация: деловая, научно-техническая, производственная, организационно-управленческая, маркетинговая, финансовая, о персонале фирмы, программное обеспечение. Утечка этой информации может привести к реальным потерям для фирмы, либо к упущенной выгоде или к обоим последствиям сразу.

Чаще всего коммерческий шпионаж осуществляется:

- конкурентами,

- криминальными структурами,

- лицами, стремящимися получить доход от перепродажи полученных незаконным путем сведений.

Конкуренты, получив информацию о секретах производства (“ноу-хау”), новейших научных разработках, планах других фирм, могут использовать ее для получения преимуществ в конкурентной борьбе, выпуска аналогичной продукции, либо для непосредственного воздействия на успех деятельности своих “противников” (срыв сделок, недопущение объединения конкурентов и пр.). Криминальные структуры чаще всего используют информацию для шантажа в целях получения незаконных доходов.

В условиях острой конкурентной борьбы каждая фирма, действующая на рынке, неизбежно сталкивается с необходимостью решения двух проблем.

Первая связана с получением информации о деятельности конкурентов, причем как можно более полной, точной и своевременной. Без наличия такой информации невозможно строить производственную, научно-техническую, финансовую, рыночную стратегии и тактику поведения фирмы. Особенно важна информация, составляющая коммерческую тайну. Зачастую получение такой информации позволяет фирме экономить огромные суммы на научно-исследовательских работах и опытно-конструкторских разработках. Если способы получения информации выходят за разрешенные законом рамки (например, с помощью подкупа сотрудников, незаконного доступа к компьютерной системе), то эта деятельность может считаться коммерческим шпионажем.

Вторая проблема – защита конфиденциальной информации. Как сама фирма стремится узнать секреты других, так и ее конкуренты делают то же самое. Следовательно, каждая фирма может являться одновременно как объектом, так и субъектом коммерческого шпионажа, или, если использовать более “мягкий” термин – экономической разведки.

Субъектом коммерческого шпионажа в развитых странах все чаще становятся не сами фирмы-конкуренты, а специализированные коммерческие организации, основной целью деятельности которых как раз и является изъятие или защита конфиденциальной информации. В этих странах даже государственные спецслужбы вынуждены обеспечивать защиту наиболее важной коммерческой информации частных фирм от международного экономического шпионажа, поскольку потери от утраты информации такого рода достигают сотен миллиардов долларов.

Объектом преступных посягательств являются люди (персонал фирмы), документы, технические средства. Непосредственным носителем информации могут быть бумажные документы, планы, отчеты, финансовые документы, чертежи, техническая документация, дискеты, кассеты.

Наряду с названными выше используются технические средства коммерческого шпионажа. К ним относятся: направленные микрофоны, минирадиозакладки (“жучки”), звукозаписывающая аппаратура, специальные системы наблюдения, фотоаппаратура, приборы для съема информации с телефонных аппаратов, приборы для съема информации через стекло здания.

Борьба с угрозами данного вида может быть эффективной, как правило, на основе:

во-первых, соблюдения общих требований режима безопасности,

во-вторых, создания собственной службы безопасности,

в-третьих, обращения предпринимателей в соответствующие специализированные фирмы, агентства, оказывающие услуги по охране информации,

в-четвертых, своевременного информирования правоохранительных органов.

Вывод: в ходе лекции студенты ознакомились с понятием предпринимательской тайны и средствами ее защиты.

Основная литература:

1. Рубин Ю.Б., Потапова О.Н. Основы бизнеса. Часть 1. Основы предпринимательской профессии: учеб. пособие Ю.Б.– М.: Московская финансово промышленная академия 2018. – 108 с. – (Серия «Непрерывное образование»).

2. https://studopedia.ru/10_215919_kommercheskiy-shpionazh.html