УПРАВЛЕНИЕ РИСКАМИ ОРГАНИЗАЦИЙ

(учебное пособие)

О.А. Фирсова
(кандидат экономических наук, доцент кафедры «Предпринимательство и маркетинг» ФГБОУ ВПО «Госуниверситет – УНПК»)

СОДЕРЖАНИЕ

Введение

Существование рисков как неотъемлемой части предпринимательской деятельности привело к необходимости разработки конкретных методов и приемов их выявления при принятии и реализации управленческих решений. Предприятия работают в различных условиях конкурентной среды, имея разную внутреннюю среду, уровень производственного потенциала, кадровый состав и т.д. В связи с этим у каждого предприятия возникают риски, непосредственно присущие только данной компании и связанные со спецификой производственной, технологической, коммерческой, финансовой и других видов деятельности. Важно своевременно их выявить и определить вероятность наступления, время наступления, а также возможный ущерб.

Методы управления рисками, получившие широкое применение в банковской деятельности, рассматриваются как инструмент управления предприятиями. Многие из этих методов могут применяться для снижения рисков в деятельности компаний различных отраслей и видов бизнеса.

Сегодня одним из наиболее прогрессивных способов повышения эффективности бизнеса по праву считается бюджетирование. Вопросам организации бюджетного процесса в предприятиях посвящено множество научных исследований и специализированной литературы. Польза бюджетирования очевидна. Поэтому многие предприятия уже внедрили или планируют внедрение соответствующих методов корпоративного управления. Именно это обстоятельство — ключевой момент в решении вопроса об организации риск-ориентированного управления предприятием. Управление рисками требует определенного уровня развития корпоративной культуры и органов корпоративного управления, во многом схожего с тем, которое необходимо для успешной организации бюджетного процесса. Это вполне логично, так как само по себе бюджетирование можно рассматривать как метод управления одним из основных рисков деятельности предприятий — стратегическим риском. Внедрение бюджетного процесса, как и организация системы управления рисками, нередко требует пересмотра организационной структуры предприятия, процедур принятия управленческих решений, а также определенной работы по повышению квалификации персонала (в том числе руководителей среднего и высшего звена) и даже набора новых сотрудников — специалистов в данной области. Более того, постановка бюджетирования может рассматриваться как первый шаг к внедрению риск-ориентированного управления предприятием, предоставляя удачную базу для дальнейшего развития, так как предполагает выполнение ряда аналогичных условий.

Целью предпринимательства является получение максимальных доходов при минимальных затратах капитала в условиях конкурентной борьбы. Реализация указанной цели требует соизмерения размеров вложенного (авансированного) в производственно-торговую деятельность капитала с финансовыми результатами этой деятельности. Вместе с тем, при осуществлении любого вида хозяйственной деятельности объективно существует опасность (риск) потерь, объем которых обусловлен спецификой конкретного бизнеса. Цель данного учебного пособия раскрыть политику управления финансовыми рисками. Для этого необходимо реализовать следующие основные задачи:

1. дать понятие риска, рассмотреть его основные виды;
2. раскрыть сущность и содержание риск-менеджмента;
3. проследить тенденции риск-менеджмента в различных отраслях;
4. рассмотреть методы управления финансовым риском.

ГЛАВА 1. ПОНЯТИЕ РИСКА, ВИДЫ РИСКОВ

1.1. История развития исследования теории риска

В 1855 г. представитель немецкой классической школы Г. фон Мангольдт опубликовал работу "Действительное назначение предпринимателя и истинная природа предпринимательской прибыли". В центр своих теоретических исследований предпринимательства он поставил несение риска как важнейшую ролевую функцию предпринимателя.

Относительно теории риска Мангольдт разделил понятия "производства на заказ" и "производство на рынок". В производстве на заказ гарантирован доход, поскольку заранее ясен заказчик и определена цена, следовательно, риск минимален или вообще отсутствует.

В подобных ситуациях фактически устраняется неопределенность, сопутствующая процессу между началом производства и продажей конечного продукта. В производстве на рынок такая неопределенность присутствует, так как продукт предназначен для продажи при неопределенном спросе и неизвестной цене.

Относя деятельность предпринимателя к "производству для рынка", Мангольдт первым ставит вопрос об оценке степени риска, который несет предприниматель. Для его оценки он вводит в свое исследование фактор времени. Чем больше отрезок времени, отделяющий начало производства товара от его продажи, тем больше неопределенность успеха, больше риск возможных потерь для предпринимателя и, соответственно, больше ожидаемое вознаграждение.

Наиболее полное развитие фактор риска как важнейшая составляющая предпринимательской функции получила у американского экономиста Фрэнка Найта. Он связывал появление предпринимательского дохода не с любым видом риска. Риск, измеренный вероятностным распределением, следует относить к категории страхуемых заранее. Такой риск может учитываться в первоначальных инвестиционных решениях и превращается, по словам Ф. Найта, в "постоянный элемент издержек" в виде страховки. Поэтому такой риск не является фактором неопределенности для предпринимателя и, соответственно, служит причиной его прибыли или потерь.

Риск, по Ф. Найту, представляет собой объективную вероятность того или иного события и может быть выражен количественно, в частности в виде математически вероятностного распределения доходов. Чем больше вероятность стандартного отклонения от ожидаемой величины при таком распределении, тем меньше риск, и наоборот. В то же время существует неопределенность, означающая, что ожидаемый доход в принципе может быть получен, однако вероятность такого события нельзя измерить или просчитать. К таким ситуациям Ф. Найт относил, например, невозможность предсказать поведение или направленность потребительского спроса.

Для понимания природы предпринимательского риска фундаментальное значение имеет связь риска и прибыли. Адам Смит в "Исследованиях о природе и причинах богатства народов" писал, что достижение даже обычной нормы прибыли всегда связано с большим или меньшим риском. Известно, что получение прибыли предпринимателю не гарантировано, вознаграждением за затраченные им время, усилия и способности могут оказаться как прибыль, так и убытки.

Предприниматель проявляет готовность идти на риск в условиях неопределенности, поскольку наряду с риском потерь существует возможность дополнительных доходов. И. Шуймпетер в книге "Теория экономического развития" пишет о том, что, если риски не учитываются в хозяйственном плане, тогда они становятся, с одной стороны, источником убытков, а с другой - прибылей. Можно выбрать решения, содержащие меньше риска, но при этом меньше будет и получаемая прибыль.

Поскольку основной целью любого коммерческого предприятия является получение прибыли, то в ситуации с созданием или функционированием любого финансового субъекта возникает проблема его доходности.

Доходность - это относительная величина, характеризующая эффективность предпринимательской деятельности, представляющая собой отношение дохода к затратам, измеряется в процентах.

Если доходность предприятия, бизнеса ниже средней банковской процентной ставки или отсутствует совсем, то его существование бессмысленно с точки зрения получения прибыли.

Стремление предпринимателя получить наибольшую прибыль ограничивается возможностью понести убытки. Риск предпринимательской деятельности означает вероятность того, что фактическая прибыль предпринимателя окажется меньше запланированной, ожидаемой. Чем выше ожидаемая прибыль, тем выше риск.

В рамках дилеммы "доходность - риск" предприниматель вынужден ограничивать норму прибыли, страхуя себя от излишнего риска. Связь между доходностью предпринимателя и его риском в очень упрощенном варианте может быть выражена прямолинейной зависимостью.

Таким образом, можно сделать вывод, что прибыли и потери предпринимателя есть следствия риска и неопределенности, сопровождающих его решения. Сама прибыль или доход зависят от разницы между вполне определенной закупочной ценой факторов производства или товаров и той неопределенной ценой, по которой их или результирующий продукт можно будет продать.

Необходимо отметить, что неопределенность и риск в предпринимательской деятельности играют очень важную роль, заключая в себе противоречие между планируемым и действительным.

Риск объективно составляет неизбежный элемент принятия любого хозяйственного решения в силу того, что неопределенность - неизбежная характеристика условий хозяйствования. В момент принятия решения не всегда возможно получить полные и точные знания об отдаленной во времени среде реализации решения, обо всех действующих или потенциально могущих проявиться внутренних и внешних факторах.

Объективно существует и неустранимая неопределенность, имеющая место при принятии решений, приводящая к тому, что риск никогда не бывает нулевым. Следствием этого является неуверенность в достижимости поставленной цели, и в результате реализации выбранного решения намеченная цель в большей или меньшей степени не достигается.

Неопределенность ситуации предопределяется тем, что она зависит от множества переменных, контрагентов и лиц, поведение которых не всегда можно предсказать с приемлемой точностью. Сказывается также и отсутствие четкости в определении целей, критериев и показателей их оценки (сдвиги в общественных потребностях и потреби-

тельском спросе, появление технических и технологических новшеств, изменение конъюнктуры рынка, непредсказуемые природные явления).

1.2. Система рисков

Понятие риска имеет различные трактовки в литературе, что усложняет изучение данного явления. Риск определяют как действие, событие, ситуацию, неопределенность, вероятность. Попробуем разобраться, что же представляет собой риск и почему его трактовки столь многогранны.

По сущности рисков вообще не сложилось до сих пор однозначного толкования. Это объясняется сложностью данного явления и его недостаточным теоретическим изучением.

В словаре Ожегова дается следующее определение риска.

Риск - возможная опасность; и риск - действие наудачу в надежде на счастливый исход. Сразу встречаем две трактовки понятия риск - как возможность и как действие.

Продолжим наше исследование: "Риск - действие, направленное па привлекательную цель, достижение которой сопряжено с элементом опасности, угрозой потери или неуспеха. Ситуация риска предполагает возможность выбора из двух альтернативных вариантов поведения; рискованного, связанного с риском, и надежного, т.е. гарантирующего сохранность достигнутого. Различают объективную и субъективную оценку проявления риска. Действия, воспринимаемые наблюдателем как осторожные, могут ощущаться самим субъектом как рискованные, и наоборот.

Таким образом, в данном определении риск понимается как действие субъекта, либо ведущее к потере, либо гарантирующее сохранность достигнутого, но не предусматривающее возможность успеха, получения прибыли и т.п., что несколько сужает понятие риска (об этом речь пойдет ниже).

В другом определении риска используется как раз более широкая трактовка риска. Риск - это деятельность субъектов хозяйственной жизни, связанная с преодолением неопределенности в ситуации неизбежного выбора, в процессе которой имеется возможность оценить вероятность достижения желаемого результата, неудачи, отклонения от цели, содержащиеся в выбираемых альтернативах.

Но правомерно ли определять риск как деятельность? Деятельность - специфически человеческая форма активного отношения к окружающему миру, содержание которой составляет его целесообразное изменение и преобразование. Таким образом, не все проявления риска на практике можно определить через форму активного отношения человека к окружающему миру. Объективно существуют такие виды риска, как риск стихийных бедствий, систематический риск и т.п. Конечно, можно их связать с проявлениями человеческой деятельности, но цепь причинно-следственных связей будет очень длинна.

Таким образом, определение риска как деятельности субъектов хозяйственной жизни не вполне корректно. Проанализируем следующее определение: риск - ситуативная характеристика деятельности любого субъекта рыночных отношений, отображающая неопределенность ее исхода и возможные неблагоприятные (или, напротив, благоприятные) последствия в случае неуспеха (или успеха).

Сущность риска состоит в возможности отклонения полученного результата от запланированного. Однако полученный результат может отклоняться от запланированного

и в положительную сторону. Следовательно, можно говорить не только о риске потерь, но и о риске выгоды.

Таким образом, можно выделить две позиции относительно сущности риска. Первая состоит в том, что риск рассматривается в виде возможного ущерба от реализации того или иного решения, в виде финансовых, материальных и иных потерь. Вторая позиция выражается в том, что риск рассматривается с точки зрения возможной удачи, получения доходов или прибыли в результате реализации решения.

Риск в данном определении рассматривается как ситуация. Чем же ситуация отличается от деятельности? Ситуация - совокупность обстоятельств, положение, обстановка. Ситуация включает как совокупность событий, приведших к данному исходу в результате деятельности человека, так и объективно действующие факторы. На данном этапе нашего исследования определим риск как ситуацию. Рассмотрим, какие признаки присущи ситуации риска.

Функционированию и развитию многих экономических процессов присущи элементы неопределенности. Это обуславливает появление ситуаций, не имеющих однозначного исхода. Понятие "ситуация риска" можно определить как сочетание, совокупность различных обстоятельств и условий, создающих определенную обстановку для того или иного вида деятельности.

Если существует вероятность количественно и качественно определять степень вероятности того или иного варианта, то это и будет ситуация риска.

Ситуации риска сопутствуют три условия:

- наличие неопределенности;
- необходимость выбора альтернативы (в т.ч. отказ от выбора);
- возможность оценить вероятность осуществления выбираемых альтернатив.

Ситуацию риска следует отличать от ситуации неопределенности. Последняя характеризуется тем, что вероятность наступления результатов решений или событий в принципе неустанавливаема.

Ситуацию же риска можно охарактеризовать как разновидность неопределенности, когда наступление событий вероятно и может быть определено, т.е. объективно существует возможность оценить вероятность событий, предположительно возникающих в результате осуществления хозяйственной деятельности.

Стремясь снять рискованную ситуацию, субъект делает выбор и стремится реализовать его. Тем самым риск предстает моделью снятия субъектом неопределенности, способом практического разрешения противоречия при неясном (альтернативном) развитии противоположных тенденций в конкретных обстоятельствах.

Понимание того, что субъект столкнулся с "ситуацией риска" и ему предстоит выбор из нескольких альтернативных вариантов поведения, называется "осознанием риска".

Кроме того, при рассмотрении сущности риска надо учитывать, что это понятие включает в себя не только наличие рисковой ситуации и ее осознание, но и принятие решения, сделанного на основе количественного и качественного анализа риска.

Таким образом, риск как ситуация, связанная с наличием выбора из предполагаемых альтернатив, имеет важное свойство - вероятность. Вероятность - математический признак, означающий возможность рассчитать частоту наступления события при наличии достаточного количества статистических данных. Вот почему риск нельзя опреде-

лять через вероятность (вероятность - признак риска) и тем более неопределенность (отсутствующую возможность определить вероятность исхода события).

Помимо этого необходимо отметить основную особенность риска - риск имеет свойство уменьшаться с увеличением предсказуемости рискосодержащего события. Под рискосодержащим событием понимается то событие, от совершения или несовершения которого зависит соответственно успех или неудача предполагаемого предприятия. И так как риск в таком случае выражается процентной (или количественной) возможностью несовершения благоприятного события, то чем больше существует возможностей предвидеть, совершится или не совершится это событие, тем меньше значение риска.

Таким образом, риск нельзя определить и как событие. Событие в данном случае - условие возникновения рисковой ситуации. Исходя из вышесказанного, дадим следующее определение.

Риск - ситуация, связанная с наличием выбора из предполагаемых альтернатив путем оценки вероятности наступления рискосодержащего события, влекущего как положительные, так и отрицательные последствия.

В современной экономической литературе категория риск представляет собой событие, которое может произойти или не произойти. В случае совершения такого события возможны три экономических результата: отрицательный (проигрыш, ущерб, убыток), нулевой, положительный (выигрыш, выгода, прибыль).

Другими словами, риск можно охарактеризовать как опасность потенциально возможной, вероятной потери ресурсов или недополучения доходов по сравнению с вариантом, рассчитанным на рациональное использование ресурсов в данном виде деятельности. Сказанное характеризует категорию "риск" с качественной стороны и создает основу для перевода понятия "риск" в количественное.

Действительно, если риск - это опасность потери ресурсов или дохода, то существует его количественная мера, определяемая абсолютным или относительным уровнем потерь.

В абсолютном выражении риск может определяться величиной возможных потерь в материально-вещественном (физическом) или стоимостном (денежном) выражении, если только ущерб поддается такому измерению.

В относительном выражении риск определяется как величина возможных потерь, отнесенная к некоторой базе, в виде которой наиболее удобно принимать либо имущественное состояние, либо общие затраты ресурсов на данный вид деятельности, либо ожидаемый доход (прибыль) от операции.

Выбор той или иной базы не имеет принципиального значения, но следует предпочесть показатель, определяемый с высокой степенью достоверности.

Как правило, в абсолютном выражении риск исчисляется, когда речь идет об одной конкретной сделке. Если же необходимо определить допустимый уровень риска при совершении различных коммерческих операций, то применяются относительные показатели.

1.3. Классификация рисков

Эффективность организации управления рисками во многом определяется их классификацией, которая создает возможности для эффективного применения соответствующих методов и приемов управления риском.

К *природным рискам* относятся риски стихийных бедствий, такие как землетрясения, наводнения, ураганы, тайфуны, удары молнии, извержения вулканов и т.д.

Техногенные риски связаны с хозяйственной деятельностью человека.

Смешанными рисками являются события природного характера, ставшие результатом хозяйственной деятельности человека.

*Чистые (простые) риск*и, или статические, практически всегда наносят предприятию ущерб, то есть связаны только с потерями для предпринимательской деятельности. Это риск потерь реальных активов вследствие нанесения ущерба собственности или неудовлетворительной организации.

Спекулятивные риски, или динамические, — это риски непредвиденных изменений стоимостных оценок управленческих решений фирмы, а также изменения рыночных отношений или политических обстоятельств. Они характеризуются тем, что могут быть связаны как с потерями, так и с получением дополнительной прибыли по отношению к ожидаемым результатам. Основные причины возникновения внешних и внутренних рисков представлены в таблице 1.

Производственные риски — это риски, характерные для производственной деятельности и связанные с убытками от остановки производства по различным причинам, а также с неадекватным использованием техники и технологии, основных и оборотных фондов, производственных ресурсов и рабочего времени.

Финансовые риски — это риски, связанные с вероятностью потерь финансовых ресурсов (денежных средств). Финансовые риски подразделяются на два вида: риски, связанные с покупательной способностью денег, и риски, связанные с вложением капитала (инвестиционные риски, кредитные риски, риски прямых финансовых потерь).

По типу потерь финансовые риски разделяют на прямые имущественные риски и риски, связанные с обязательствами, т.е. риск убытков по вине конкурентов, сотрудников или партнеров в связи с изменениями условий выполнения обязательств.

Имущественные риски — это риски, связанные с возможностью потерь имущества по различным причинам: кражи, диверсии, халатность, перенапряжения технической и технологической систем, порчи и т.п.

Под коммерческим риском понимается риск, связанный с предпринимательской деятельностью, ориентированной на получение максимальной прибыли и возникающий в процессе реализации товаров и услуг, произведенных или закупленных предприятием.

Социальные риски непосредственно связаны с жизнью, здоровьем и трудоспособностью работников предприятия, а также их личностными характеристиками и условиями труда.

Предпринимательский риск связан со случайными потерями предпринимательской прибыли. Потери в предпринимательской деятельности разделяют на материальные, трудовые, финансовые, потери времени и специальные виды потерь.

Материальные потери проявляются в дополнительных затратах или прямых потерях оборудования, имущества, продукции, сырья, энергии и т.д. Материальные потери измеряются в тех же единицах, в которых измеряется количество данного вида материальных ресурсов, т.е. в физических единицах веса, объема, площади и др., а также в стоимостном выражении, в денежных единицах. Для этого потери в физическом измерении переводятся в стоимостные путем умножения его на цену единицы соответствующего материального ресурса. Для достаточного количества материальных ресурсов, стоимость которых заранее известна, потери можно сразу оценивать в денежном выражении.

Таблица 1. Основные причины возникновения внешних и внутренних рисков

Риски	Основные причины возникновения	Объект направления
	Внешние риски	
Стразовый	нестабильность государственной власти, особенности государственного законодательства, национализация и т.п.	имущество, имущественный
Валютные	изменение валютных курсов, валютного регулирования	имущественный интерес
Налоговый	изменение налоговой политики, налоговых ставок	имущественный интерес
Форс-мажорные	природные катастрофы, войны, революции, путчи	имущество, имущественный интерес, человек
	Внутренние риски	
Организационный	низкий уровень организации, ошибки планирования, прогнозирования, слабое регулирование, плохая организация труда сотрудников и т.д.	имущество, имущественный интерес, человек
Ресурсный	нехватка производственных запасов, срывы поставок, недостаточная квалификация рабочей силы, отсутствие запаса прочности по ресурсам	имущество, имущественный интерес, человек
Инвестиционный	риски реального инвестирования: перебои в поставках стройматериалов, ошибки в разработке инвестиционного проекта строительства или реконструкции, неудачный выбор месторасположения строительства. портфельные риски: изменение условий контракта, ошибки в выборе объектов инвестирования, неправильный подбор финансовых инструментов	имущество, имущественный интерес, человек
Кредитный	Невозврат долга и процентов по нему, невыполнение условий кредитного договора, невольное банкротство заемщика, изменение платежеспособности заемщика	Имущественный интерес
Инновационный	Неправильный выбор нововведений, неверные расчеты, применение научно-технических новшеств	Имущественный интерес
Правовые	Используемые лицензии, патентные права, невыполнение контрактов, судебные процессы с внешними партнерами, внутренние судебные процессы	Имущество, имущественный интерес, человек

Трудовые потери представляют собой потери рабочего времен, вызванные случайными, непредвиденными обстоятельствами. В непосредственном измерении трудовые потери выражаются в человеко-часах, человеко-днях или просто часах рабочего време-

ни. Перевод трудовых потерь в стоимостное, денежное выражение осуществляется путем умножения трудочасов на стоимость одного часа. Финансовые потери — это прямой денежный ущерб, связанный с непредусмотренными платежами, выплатой штрафов, уплатой дополнительных налогов, потерей денежных средств и ценных бумаг, невозвратом долгов, неоплатой покупателем поставленной ему продукции. Временные финансовые потери могут быть обусловлены замораживанием счетов, несвоевременной выдачей средств, отсрочкой выплаты долгов, изменением валютного курса рубля, инфляцией и др. Потери времени существуют тогда, когда процесс предпринимательской деятельности идет медленнее, чем было намечено. Прямая оценка таких потерь осуществляется в часах, днях, неделях, месяцах запаздывания в получении намеченного результата. Чтобы перевести оценку потерь времени в стоимостное измерение, необходимо установить, к каким потерям дохода и прибыли приводят случайные потери рабочего времени. Специальные виды потерь проявляются в виде нанесения ущерба здоровью и жизни людей, окружающей среде, престижу предприятия, а также в виде других неблагоприятных социальных и морально-психологических последствий, чаще всего их крайне трудно определить в количественном и тем более в стоимостном выражении.

Предпринимательский риск связан с конечным финансово-хозяйственным результатом деятельности предприятия, в котором объединяются многочисленные частные риски (рис. 1).

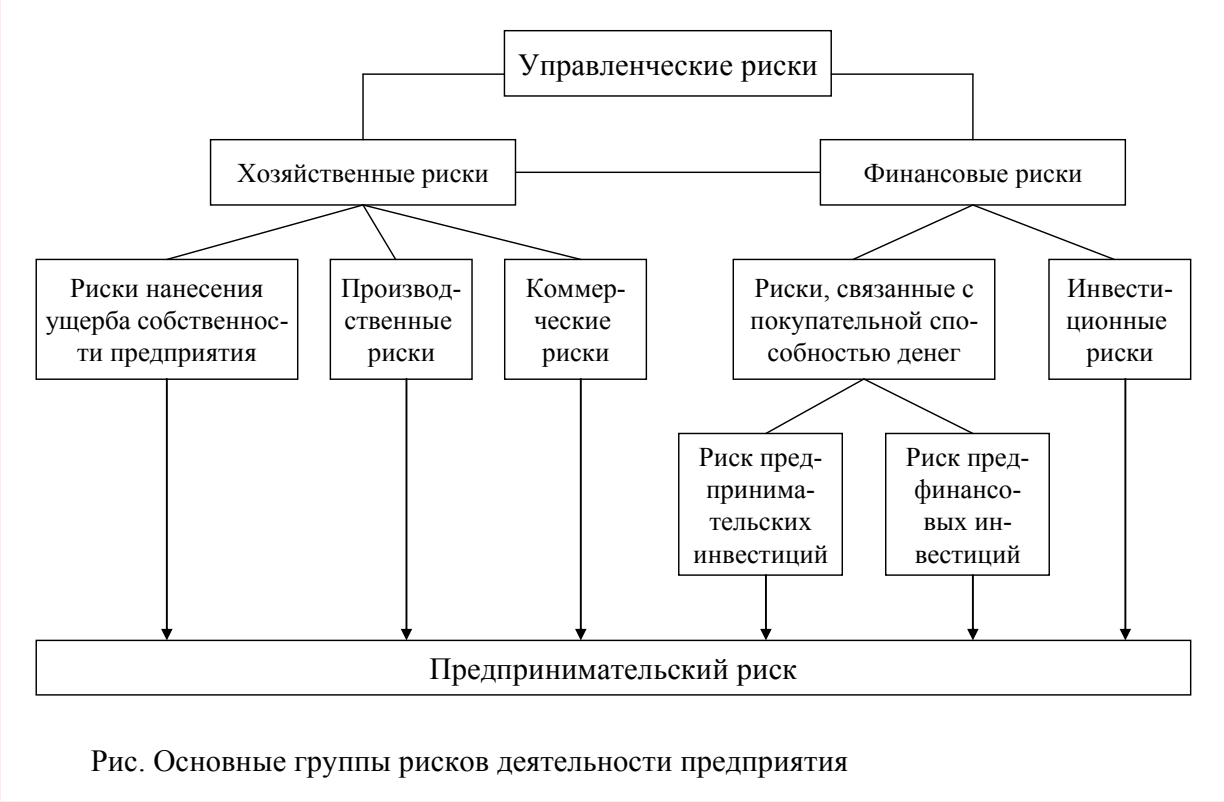


Рис. Основные группы рисков деятельности предприятия

Финансовый риск представляет собой функцию времени. Как правило, степень риска для данного финансового актива или варианта вложения капитала увеличивается во времени. Например, убытки импортера сегодня зависят от времени от момента заключения контракта до срока платежа по сделке, так как курсы иностранной валюты по отношению к российскому рублю продолжают расти.

В зарубежной практике в качестве метода количественного определения риска

вложения капитала предлагается использовать древо вероятностей.

Этот метод позволяет точно определить вероятные будущие денежные потоки инвестиционного проекта в их связи с результатами предыдущих периодов времени. Если проект вложения капитала приемлем в первом периоде времени, то он может быть также приемлем и в последующих периодах времени.

Если же предполагается, что денежные потоки в разных периодах времени являются независимыми друг от друга, тогда необходимо определить вероятное распределение результатов денежных потоков для каждого периода времени.

В случае, когда связь между денежными потоками в разных периодах времени существует, необходимо принять данную зависимость и на ее основе представить будущие события так, как они могут произойти.

В качестве примера произведем древо вероятностей для трех периодов времени (рис. 1).

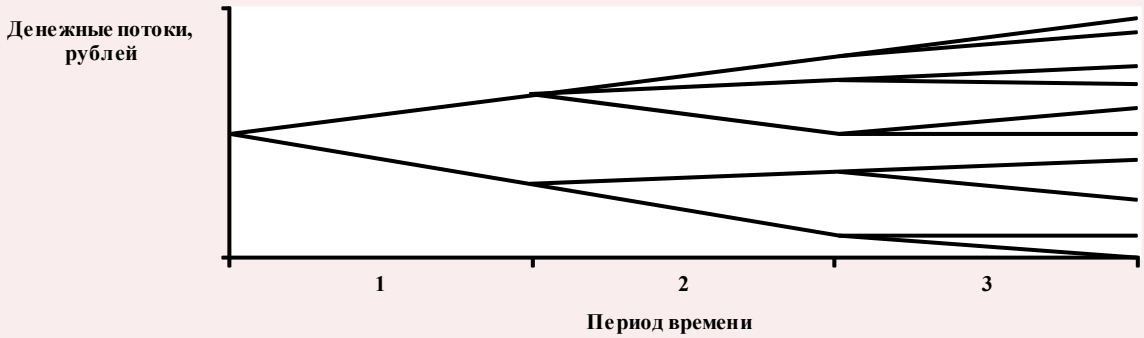


Рис. 1. Древо вероятностей

Древо вероятностей показывает, что если в периоде 1 результатом будет верхняя ветвь, то она приведет в периоде 2 к другому множеству возможных результатов, чем это было бы, если бы результат в периоде 1 выражался нижней ветвью. Аналогичная картина наблюдается и при переходе от периода времени 2 к периоду 3. Поэтому в момент временного периода 0 древо вероятностей представляет наилучшую оценку того результата, который, вероятно, будет иметь место в будущем, в зависимости от того, что происходило прежде. Для каждой из ветвей денежные потоки привязаны к вероятности.

В периоде 1 результат денежного потока не зависит от того, что было прежде. Поэтому вероятности, связанные с двумя ветвями, называются исходными вероятностями. Для всех последующих периодов (т.е. периодов 2, 3 и т.д.) результаты денежных потоков зависят от предыдущих результатов. Поэтому вероятности этих периодов называются условными. Кроме того, существует совместная вероятность, которая представляет собой вероятность появления определенной последовательности денежных потоков. Совместная вероятность равна произведению исходной и условной вероятностей.

Профессиональные риски связаны с выполнением должностными лицами своих профессиональных обязанностей.

Инвестиционные риски возникают при вложении инвесторами средств в инвестиционные объекты с целью получения прибыли. Различают систематический и несистематический риски; риски реального и финансового инвестирования.

Транспортные риски представляют собой риски, связанные с убытком по причине транспортировки товара; различают морские, воздушные и наземные.

Банковские риски представляют собой опасность потерь в банковских операциях, они могут иметь внешние причины возникновения (страновый и валютный) и внутренние, такие как риски пассивных и активных операций, риски, связанные со спецификой клиента.

Страховой риск связан с неэффективной страховой деятельностью как на этапе, предшествующем заключению договора страхования, так и на последующих этапах перестрахования, формирования страховых резервов и т.п.

1.4. Прогнозирование рисковой ситуации

Рассматривая риск как экономическую категорию, необходимо глубоко понимать и применять на практике системы прогнозирования, оценки, анализа и управления предпринимательскими рисками. Рассмотрим поэтапно весь алгоритм действий предпринимателя, направленный на оптимизацию рисковой ситуации в своей деятельности.

Изначально рисковая ситуация подвергается прогнозированию, причем важное место здесь занимает предупреждение неопределенности возможного риска. На данном этапе решается целый комплекс задач, основными из которых являются:

- определение источников информации, которые позволяют выявить причины риска и возможные его виды;
- выяснение источников риска;
- прогнозирование основных видов риска для конкретного предприятия;
- определение объектов, на которые воздействует тот или иной вид риска.

Определение источников информации. Для того чтобы определить источники риска и возможные их виды, необходимо иметь надежное информационное обеспечение. Все источники такой информации могут быть классифицированы:

- внутренние и внешние;
- учтенные и неучтенные;
- разовые и постоянные;
- полученные легальным и нелегальным путем;
- полученные с магнитных носителей, с документов, от партнеров, приобретенные за плату, от осведомителей, агентов и т.д.;
- достоверные и сомнительные;
- другие.

Их может быть великое множество, и каждое предприятие выбирает для себя наиболее важные. Назовем некоторые из наиболее значимых и доступных: каталог факторов риска и рисковых ситуаций; личный опыт руководитеней предприятия и специалистов группы оценки и управления риском; прогнозная информация; материалы ревизий, аудита, проверок налоговой службы, лабораторного и врачебно-санитарного контроля, печати, объяснительных и докладных записок, совещаний, переписки, получаемые в результате личных контактов; бухгалтерский учет и отчетность; статистические данные; сведения о конкурентах, партнерах, поставщиках и потребителях; материалы маркетинговых исследований о состоянии рынка; сведения правоохранительных органов о криминальной обстановке; экономическая, политическая, демографическая и т.д. ситуации в стране и регионе; платежеспособность покупателей и т.п.

Информация, необходимая для определения уровня риска, может быть оценена с количественной, смысловой и ценностной точек зрения.

Количество информации должно быть достаточным для оценки риска. Ее смысловое выражение должно быть доступным и применимым для управления рисками, а ценностность состоит в том, что она должна способствовать достижению поставленной цели.

Выяснение источников риска. Информация является питательной средой для определения источников хозяйственного риска. В каждом конкретном случае они могут быть различны для каждого предприятия. Поэтому руководители и специалисты предприятия могут их заблаговременно определить, сгруппировать и отранжировать в зависимости от опасности для хозяйственной деятельности предприятия.

О некоторых из этих источников речь уже шла ранее, поэтому для примера выделим лишь самые главные. К ним можно отнести:

- недобросовестное поведение конкурентов, партнеров, поставщиков, потребителей;
- промышленный шпионаж;
- непредсказуемость колебаний спроса и предложения;
- рэкет;
- внезапные изменения налогового, таможенного, валютного законодательства;
- колебания цен, валютных и биржевых курсов, инфляция;
- ошибки в планировании, организации и управлении производством;
- разглашение конфиденциальной информации и противоправные действия сотрудников фирмы;
- форс-мажорные обстоятельства;
- другие.

Прогнозирование основных видов риска. Как уже отмечалось, каждое предприятие работает в разных условиях конкурентной среды, имеет свои кадровый и производственный потенциалы, свои производственные связи, деловых партнеров и т.д. Исходя из этого у различных предприятий могут возникать свои виды рисков и их разновидности.

Например, производственный, коммерческий, финансовый, технологический, страховой и т.д. На данном этапе важно своевременно выявить их и по возможности определить наиболее опасные как по вероятному ущербу, так и по времени наступления. Это послужит основой для принятия своевременных и правильных мер по предотвращению риска.

Определение объектов, на которые воздействует тот или иной вид риска. Для оптимального выбора наиболее предпочтительного варианта действий по управлению риском важно иметь четкую информацию и о том, какой объект подвергается риску. Это может быть и информация, и какой-то объект, и персонал, и руководители фирмы, и прибыльность производства, и т.д.

Владея этой информацией и зная реальную степень защищенности объекта, можно рассчитать потребность в объеме необходимых сил и средств для предотвращения риска, выработать правильные меры по защите объекта

1.5. Способы оценки степени риска

Оценка риска - это совокупность аналитических мероприятий, позволяющих

спрогнозировать возможность получения дополнительного предпринимательского дохода или определенной величины ущерба от возникшей рисковой ситуации и несвоевременного принятия мер по предотвращению риска.

В данном разделе особое значение имеет своевременный подсчет величины возможного ущерба. Оценка предпринимательских рисков может осуществляться как с позиции качественных характеристик, так и количественно.

Качественная оценка рисков. Человек от природы стремиться избегать риска. Если мы не можем контролировать риск, то обычно предпочитаем избежать его. Вынужденные признать наличие риска в нашей жизни, мы желаем свести его к минимуму.

Также мы хотим иметь возможность выбора наименее рискованной из двух и более альтернатив. Или мы хотим соотнести риск какого-либо события или рискованности предприятия с возможными выгодами, т.е. мы хотим выбрать оптимальное соотношение риска и выгоды какого-либо предприятия.

Для того чтобы выбрать наименее рискованную или предлагающую наиболее привлекательное соотношение риска и выгод альтернативу, мы должны оценить риск, что позволит сравнить величину риска различных вариантов решения и выбрать из них тот, который больше всего отвечает выбранной предприятием стратегии риска.

Основная часть оценки риска сегодня основана на теории вероятности - систематическом статистическом методе определения вероятности того, что какое-то будущее событие произойдет. Однако надо заметить, что вероятность не каждого будущего события можно измерить.

Несмотря на разработанность критериев риска, которые позволяют ранжировать альтернативные события в зависимости от степени риска, зачастую, чтобы применить эти критерии, нам необходимо сделать ряд допущений по этому вопросу.

С другой стороны, существует множество ситуаций, в которых мы имеем в своем распоряжении обширные массивы информации о наблюдавшихся в прошлом событиях, которые позволяют нам делать полновесные выводы о вероятности осуществления будущего события.Многие финансовые операции (венчурное инвестирование, покупка акций, селинговые операции, кредитные операции и др.) связаны с довольно существенным риском. Они требуют оценить степень риска и определить его величину.

Степень риска - это вероятность наступления случая потерь, а также размер возможного ущерба от него.

Риск может быть:

- допустимым - имеется угроза полной потери прибыли от реализации планируемого проекта;
- критическим - возможны непоступление не только прибыли, но и выручки и покрытие убытков за счет средств предпринимателя;
- катастрофическим - возможны потеря капитала, имущества и банкротство предпринимателя.

(Смотрите рис.)

Область, в которой потери не ожидаются называется безрисковой зоной. Ей соответствуют нулевые потери или даже отрицательные (превышение прибыли над ожидаемой).

Под зоной допустимого риска понимается область, в пределах которой данный вид предпринимательской деятельности сохраняет свою экономическую целесообразность, т.е. потери имеют место, но они меньше ожидаемой прибыли. Граница зоны допустимо-

го риска соответствует уровню потерь, равному расчетной прибыли от предпринимательской деятельности.

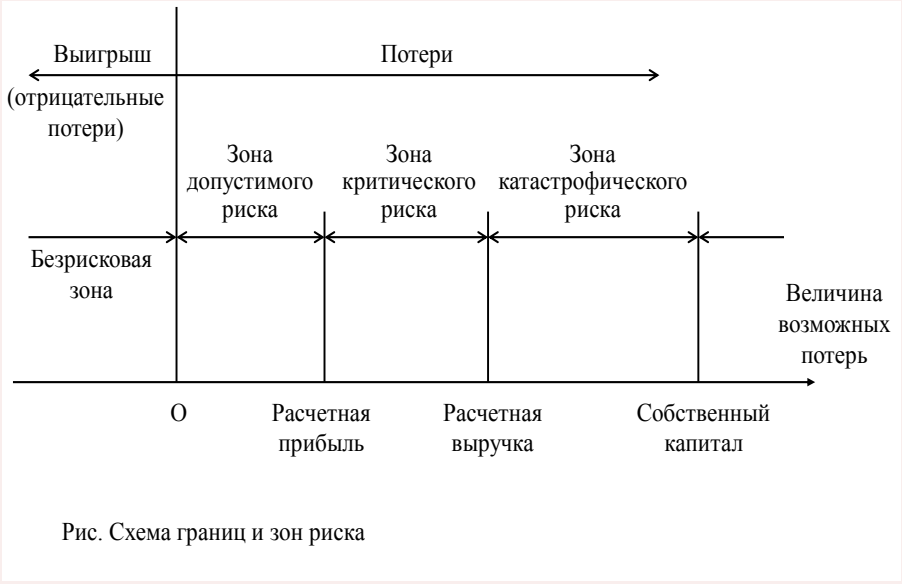


Рис. Схема границ и зон риска

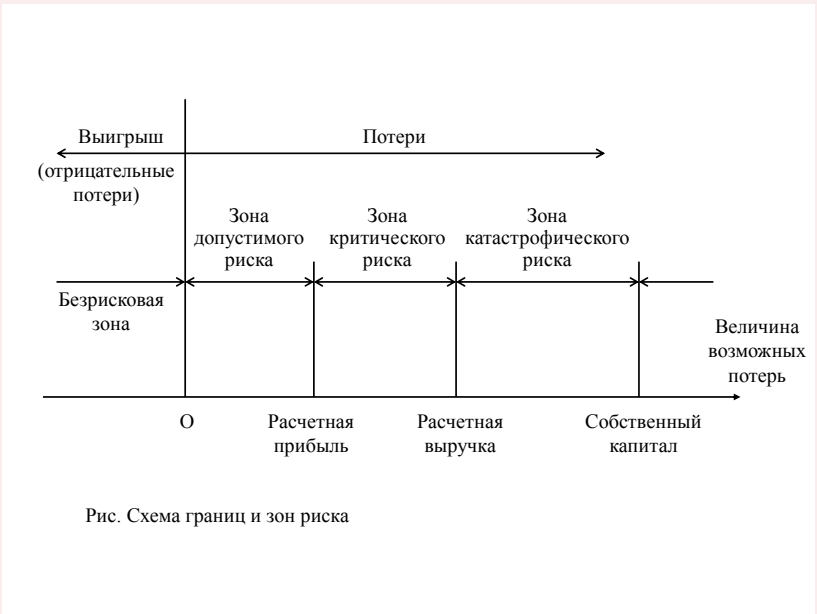


Рис. Схема границ и зон риска

Более опасная область – зона критического риска. Это область, характеризуемая возможностью потерь, превышающих величину ожидаемой прибыли и достигающих в пределе величины денежного объема операции, исчисляемого полной расчетной выручкой от предпринимательской сделки, т.е. суммой затрат и прибыли. Иначе говоря, зона критического риска характеризуется опасностью потерь, которые заведомо превышают ожидаемую прибыль и в пределе, максимуме могут привести к невозместимой потере всех средств, вложенных предпринимателем в проект. В последнем случае предприниматель не только не получает от сделки никакого дохода, но и несет убытки в сумме всех своих бесплодных затрат.

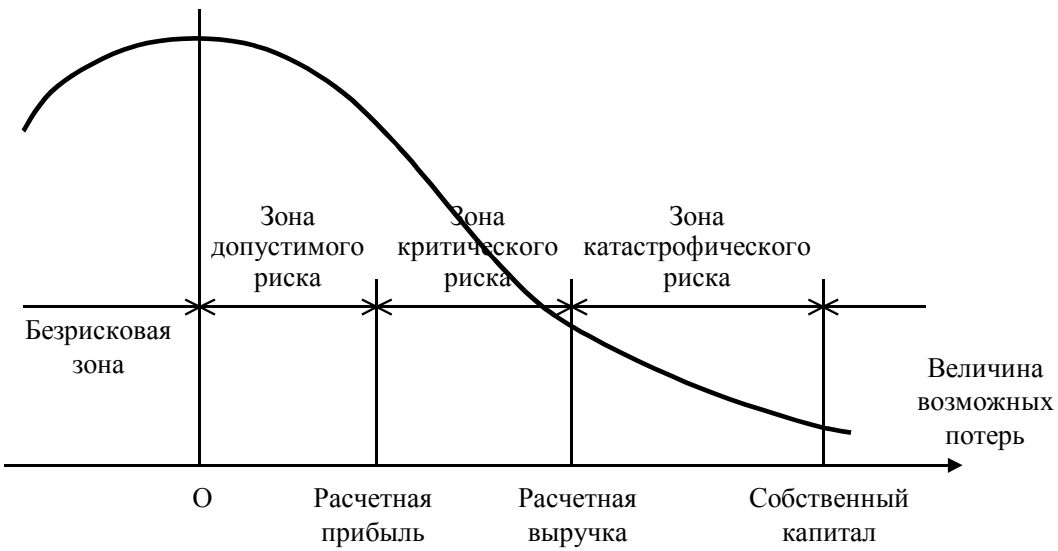


Рис. Кривая риска

Зона катастрофического риска представляет область потерь, которые по своей величине превосходят критический уровень, ожидаемую выручку и в максимуме могут достигать величины, равной всему собственному капиталу, имущественному состоянию фирмы или превосходить его.

Количественный анализ - это определение конкретного размера денежного ущерба отдельных подвидов финансового риска и финансового риска в совокупности.

Иногда качественный и количественный анализ производится на основе оценки влияния внутренних и внешних факторов: осуществляются поэлементная оценка удельного веса их влияния на работу данного предприятия и ее денежное выражение. Такой метод анализа является достаточно трудоемким с точки зрения количественного анализа, но приносит свои несомненные плоды при качественном анализе. В связи с этим следует уделить большее внимание описанию методов количественного анализа финансового риска, поскольку их немало и для их грамотного применения необходим некоторый навык.

В абсолютном выражении риск может определяться величиной возможных потерь в материально-вещественном (физическом) или стоимостном (денежном) выражении.

В относительном выражении риск определяется как величина возможных потерь, отнесенная к некоторой базе, в виде которой наиболее удобно принимать либо имущественное состояние предприятия, либо общие затраты ресурсов на данный вид предпринимательской деятельности, либо ожидаемый доход (прибыль). Тогда потерями будем считать случайное отклонение прибыли, дохода, выручки в сторону снижения. в сравнении с ожидаемыми величинами. Предпринимательские потери - это в первую очередь случайное снижение предпринимательского дохода. Именно величина таких потерь и характеризует степень риска. Отсюда анализ риска прежде всего связан с изучением потерь.

В зависимости от величины вероятных потерь целесообразно разделить их на три группы:

- потери, величина которых не превышает расчетной прибыли, можно назвать допустимыми;
- потери, величина которых больше расчетной прибыли относятся к разряду критических - такие потери придется возмещать из кармана предпринимателя;
- еще более опасен катастрофический риск, при котором предприниматель рискует понести потери, превышающие все его имущество.

Если удается тем или иным способом спрогнозировать, оценить возможные потери по данной операции, то значит получена количественная оценка риска, на который идет предприниматель. Разделив абсолютную величину возможных потерь на расчетный показатель затрат или прибыли, получим количественную оценку риска в относительном выражении, в процентах.

Говоря о том, что риск измеряется величиной возможных. вероятных потерь, следует учитывать случайный характер таких потерь. Вероятность наступления события может быть определена объективным методом и субъективным.

Объективным методом пользуются для определения вероятности наступления события на основе исчисления частоты, с которой происходит данное событие.

Субъективный метод базируется на использовании субъективных критериев, которые основываются на различных предположениях. К таким предположениям могут относиться суждение оценивающего, его личный опыт, оценка эксперта по рейтингу, мнение аудитора-консультанта и т.п.

Таким образом, в основе оценки финансовых рисков лежит нахождение зависимости между определенными размерами потерь предприятия и вероятностью их возникновения. Эта зависимость находит выражение в строящейся *кривой вероятностей возникновения определенного уровня потерь.*

Построение кривой - чрезвычайно сложная задача, требующая от служащих, занимающихся вопросами финансового риска, достаточного опытами знаний. Для построения кривой вероятностей возникновения определенного уровня потерь (кривой риска) применяются различные способы: статистический; анализ целесообразности затрат; метод экспертных оценок; аналитический способ; метод аналогий. Среди них следует особо выделить три: статистический способ, метод экспертных оценок, аналитический способ.

Суть *статистического способа* заключается в том, что изучается статистика потерь и прибылей, имевших место на данном или аналогичном производстве, устанавливаются величина и частотность получения той или иной экономической отдачи, составляется наиболее вероятный прогноз на будущее.

Несомненно, риск - это вероятностная категория, ив этом смысле наиболее обоснованно с научных позиций характеризовать и измерять его как вероятность возникновения определенного уровня потерь. Вероятность означает возможность получения определенного результата.

Финансовый риск, как и любой другой, имеет математически выраженную вероятность наступления потери, которая опирается на статистические данные и может быть рассчитана с достаточно высокой точностью.

Чтобы количественно определить величину финансового риска, необходимо знать

все возможные последствия какого-либо отдельного действия и вероятность самих последствий.

Применительно к экономическим задачам методы теории вероятности сводятся к определению значений вероятности наступления событий и к выбору из возможных событий самого предпочтительного исходя из наибольшей величины математического ожидания, которое равно абсолютной величине этого события, умноженной на вероятность его наступления.

Главные инструменты статистического метода расчета финансового риска: вариация, дисперсия и стандартное (среднеквадратическое) отклонение.

Вариация - изменение количественных показателей при переходе от одного варианта результата к другому.

Дисперсия - мера отклонения фактического знания от его среднего значения.

Степень риска измеряется двумя показателями: средним ожидаемым значением и колеблемостью (изменчивостью) возможного результата.

Среднее ожидаемое значение связано с неопределенностью ситуации, оно выражается в виде средневзвешенной величины всех возможных результатов E(x), где вероятность каждого результата (A) используется в качестве частоты или веса соответствующего значения (x). В общем виде это можно записать так:

$$E(x)=A1X1 +A2X2+\cdots+AnXn.$$

Пример: при вложении денежных средств в мероприятие А из 150 случаев прибыль в сумме 20,0 тыс. руб. была получена в 75 случаях (вероятность - 75: 150 = 0,5), прибыль 25,0 тыс. руб. - в 60 случаях (вероятность - 60 : 150 = 0,4) и прибыль 30,0 тыс. руб. - в 15 случаях (вероятность - 15 : 150 = 0,1).

Среднее ожидаемое значение прибыли составит:

$$20,0 \times 0,5 + 25,0 \times 0,4 + 30.0 \times 0,1 = 23.$$

Осуществление мероприятия Б из 150 случаев давало прибыль 19,0 тыс. руб. в 60 случаях (вероятность - 60 : 150 = = 0,4), прибыль 24,0 тыс. руб. - в 45 случаях (вероятность 45 : 150 = 0,3), 31,0 тыс. руб. - в 45 случаях (вероятность 45: 150=0,3).

При проведении мероприятия Б средняя ожидаемая прибыль составит:

$19,0 \times 0,4+24,0 \times 0,3+1,0 \times 0,3=24,1.$

Сравнивая величины ожидаемой прибыли при вложении денежных средств в мероприятия А к Б, можно сделать вывод, что вепичина получаемой прибыли при мероприятии А колеблется от 20,0 до 30,0 тыс. руб., средняя величина составляет 23 тыс. руб.; в мероприятии Б величина получаемой прибыли колеблется от 19,0 до 31,0 тыс. руб. и средняя величина равна 24,1 тыс. руб.

Средняя величина представляет собой обобщенную количественную характеристику и не позволяет принять решение в пользу какого-либо варианта вложения капитала.

Для окончательного решения необходимо измерить колеблемость (размах или изменчивость) показателей, т.е. определить меру колеблемости возможного результата.

Колеблемость возможного результата представляет собой степень отклонения

ожидаемого значения от средней величины. Для ее определения обычно вычисляют дисперсию или среднеквадратическое отклонение:

$$\sigma = \sqrt{\frac{\sum_{i=1}^{N} (X_{cp} - X_i)^2}{N}},$$

Коэффициент вариации - это отношение среднего квадратичного отклонения к средней арифметической.

Он показывает степень отклонения полученных значений.

$$V = \sigma / X_{cp} \times 100\%,$$

где V — коэффициент вариации, %.

Коэффициент вариации позволяет сравнивать колеблемость признаков, имеющих разные единицы измерения.

Чем выше коэффициент вариации, тем сильнее колеблемость признака.

Установлена следующая оценка коэффициентов вариации:

до 10% - слабая колеблемость;

10-25% - умеренная колеблемость;

свыше 25% - высокая колеблемость.

В нашем примере среднее6 квадратическое отклонение составляет:

в мероприятии А - 6,68;

в мероприятии Б - 4,95.

Коэффициент вариации:

для мероприятия А: V А = 29%;

для мероприятия Б: VБ = 20%.

Коэффициент вариации при вложении денежных средств в мероприятие А больше, чем при мероприятии Б. Следовательно, мероприятие Б сопряжено с меньшим риском, а значит, предпочтительнее.

Дисперсионный метод успешно применяется и при наличии более чем двух альтернативных признаков.

Таким образом, величина риска, или степень риска, может быть измерена двумя критериями: среднее ожидаемое значение, колеблемость (изменчивость) возможного результата.

Среднее ожидаемое значение - это то значение величины события, которое связано с неопределенной ситуацией. Оно является средневзвешенной всех возможных результатов, где вероятность каждого результата используется в качестве частоты, или веса, соответствующего значения. Таким образом вычисляется тот результат, который предположительно ожидается.

Анализ целесообразности затрат ориентирован на идентификацию потенциальных зон риска с учетом показателей финансовой устойчивости фирмы. В данном случае можно просто обойтись стандартными приемами финансового анализа результатов деятельности основного предприятия и деятельности его контрагентов (банка, инвестиционного фонда, предприятия-клиента, предприятия-эмитента, инвестора, покупателя,

продавца и т.п.)

Метод экспертных оценок обычно реализуется путем обработки мнений опытных предпринимателей и специалистов. Он отличается от статистического лишь методом сбора информации для построения кривой риска.

Метод экспертных оценок основан на обобщении мнения специалистов-экспертов о вероятностях риска. Интуитивные характеристики, основанные на знаниях и опыте эксперта, дают в ряде случаев достаточно точные оценки. Экспертные методы позволяют быстро и без больших временных и трудовых затрат получить информацию, необходимую для выработки управленческого решения.

Метод экспертных оценок применяется в случаях, когда:

1) длина исходных динамических рядов недостаточна для оценивания с использованием экономико-статистических методов;

2) связь между исследуемыми явлениями носит качественный характер и не может быть выражена с помощью традиционных количественных измерителей;

3) входная информация неполная и невозможно предсказать влияние всех факторов;

4) возникли экстремальные ситуации, когда требуется принятие быстрых решений. Суть экспертных методов заключается в организованном сборе суждений и предположений экспертов с последующей обработкой полученных ответов и формированием результатов.

Выделяют следующие стадии экспертного опроса:

1) формулировка цели экспертного опроса;

2) подбор основного состава рабочей группы;

3) разработка и утверждение технического задания на проведение экспертного опроса;

4) разработка подробного сценария проведения сбора и анализа экспертных мнений (оценок), включая как конкретный вид экспертной информации (слова, условные градации, числа, ранжирование, разбиения или иные виды объектов нечисловой природы), так и конкретные методы анализа этой информации;

5) подбор экспертов в соответствии с их компетентностью;

6) формирование экспертной комиссии;

7) проведение сбора экспертной информации;

8) анализ экспертной информации;

9) интерпретация полученных результатов и подготовка заключения;

10) принятие решения - выбор альтернативы.Данный способ предполагает сбор и изучение оценок, сделанных различными специалистами (данного предприятия или внешними экспертами) вероятностей возникновения различных уровней потерь. Эти оценки базируются на учете всех факторов финансового риска, а также статистических данных. Реализация способа экспертных оценок значительно осложняется, если количество показателей оценки невелико.

Существует масса методов получения экспертных оценок. В одних с каждым экспертом работают отдельно, он даже не знает, кто еще является экспертом, а потому высказывает свое мнение независимо от авторитетов.

В других - экспертов собирают вместе, при этом эксперты обсуждают проблему друг с другом, учатся друг у друга, и неверные мнения отбрасываются. В одних методах число экспертов фиксировано, в других - число экспертов растет в процессе проведения

экспертизы.

Среди наиболее распространенных методов получения экспертных оценок можно выделить:

1) метод "Дельфы"
2) метод "снежного кома";
3) метод "дерева целей";
4) метод "комиссий круглого стола";
5) метод эвристического прогнозирования;
6) матричный метод

Рассмотрим пример количественной оценки экспертами возможного приращения платежеспособного спроса на пищевую продукцию (по методу Дельфы).

К участию в эксперименте привлечено 8 человек, после оценки уровня компетентности - 5 человек.

На первом этапе ответы на вопросы даются в произвольной форме (числовые характеристики, словесные описания).

На второй стадии называются конкретные значения возможного приращения платежеспособного спроса с аргументацией данных значений. Далее проводится статистическая обработка результатов экспертизы. Для этого находят медиану и квартили.

Медиана - серединное или центральное значение признака, делит числовой ряд пополам.

Квартиль - значения переменной, делящей ряд распределения на четыре равные части.

Считается, что медиана характеризует обобщенное мнение группы экспертов, а значения нижнего и верхнего квартилей ограничивают доверительную зону прогноза.

Предположим, что в данном примере экспертиза дала следующие результаты, представленные в таблице 3.

Таблица 3. Результаты экспертизы по определению возможного приращения платежеспособного спроса на пищевую продукцию

№ п/п	Коэффициент компетентности	Величина приращения платежеспособного спроса, %
1.	0,5	4
2.	0,6	5
3.	0,6	6
4.	0,5	8
5.	0,5	9
6.	0,7	10
7.	0,6	11

Результаты доводятся до сведения экспертов. Экспертам, чьи прогнозы не попали в доверительный интервал, предлагается аргументировать свою точку зрения или пере-

смотреть ее и присоединиться к мнению большинства.

Последующие этапы корректировки данных позволят усилить согласованность результатов.

Аналитический способ построения кривой риска наиболее сложен, поскольку лежащие в основе его элементы теории игр доступны только очень узким специалистам. Чаще используется подвид аналитического метода - анализ чувствительности модели.

Анализ чувствительности модели состоит из следующих шагов: выбор ключевого показателя, относительно которого и производится оценка чувствительности (внутренняя норма доходности, чистый приведенный доход и т.п.); выбор факторов (уровень инфляции, степень состояния экономики и др.); расчет значений ключевого показателя на различных этапах осуществления проекта (закупка сырья, производство, реализация, транспортировка, капстроительство и т.п.). Сформированные таким путем последовательности затрат и поступлений финансовых ресурсов дают возможность определить потоки фондов денежных средств для каждого момента (или отрезка времени), т.е. определить показатели эффективности. Строятся диаграммы, отражающие зависимость выбранных результирующих показателей от величины исходных параметров. Сопоставляя между собой полученные диаграммы, можно определить так называемые ключевые показатели, в наибольшей степени влияющие на оценку доходности проекта.

Анализ чувствительности имеет и серьезные недостатки: он не является всеобъемлющим и не уточняет вероятность осуществления альтернативных проектов.

Метод аналогий при анализе риска нового проекта весьма полезен, так как в данном случае исследуются данные о последствиях воздействия неблагоприятных факторов финансового риска на другие аналогичные проекты других конкурирующих предприятий.

Индексация представляет собой способ сохранения реальной величины денежных ресурсов (капитала) и доходности в условиях инфляции. В основе ее лежит использование различных индексов.

Например, при анализе и прогнозе финансовых ресурсов необходимо учитывать изменение цен, для чего используются индексы цен. Индекс цен - показатель, характеризующий изменение цен за определенный период времени.

Метод целесообразности затрат. Этот метод позволяет определить критический объем производства или продаж, т.е. нижний предельный размер выпуска продукции, при котором прибыль равна нулю.

Производство продукции в объемах меньше критического приносит только убытки. Критический объем производства необходимо оценивать при освоении новой продукции и при сокращении ее выпуска, вызванного падением спроса, сокращением поставок материалов и комплектующих изделий, заменой продукции на новую, ужесточением экологических требований и другими причинами.

Для проведения соответствующих расчетов все затраты на производство и реализацию продукции подразделяют на переменные и постоянные.

Под переменными понимают издержки, общая величина которых находится в непосредственной зависимости от объемов производства и реализации, а также от их структуры при производстве и реализации нескольких видов продукции. Это затраты на сырье и материалы, топливо, энергию, транспортные услуги, большую часть трудовых ресурсов и т.д.

К постоянным издержкам производства относят затраты, величина которых не ме-

няется с изменением объемов производства.

Они должны быть оплачены, даже если предприятие не производит продукцию (отчисления на амортизацию, аренда зданий и оборудования, страховые взносы, оплата высшего управленческого персонала и т.д.).

Критический объем производства (Vкр) можно представить в следующем виде:

Vкр = Зпост/ (Ц - Зпер),

где Ц - цена издения (единицы продукции), руб.;

Зпост - постоянные затраты, руб.;

Зпер - переменные затраты, руб.

Некоторые зарубежные авторы называют критический объем производства порогом рентабельности и используют этот показатель дпя оценки финансовой устойчивости предприятия.

Чем больше разность между фактическим объемом производства и критическим, тем выше финансовая устойчивость.

Любое изменение объема производства (продаж) оказывает существенное влияние на прибыль. Данная зависимость называется эффектом производственного (или операционного) левериджа.

Производственный леверидж показывает степень влияния постоянных затрат на прибыль (убытки) при изменениях объема производства.

Чем больше удельный вес постоянных затрат в общей сумме издержек при некотором объеме производства, тем выше производственный леверидж, следовательно, тем выше предпринимательский риск.

Работать с высоким производственным левериджем могут только те предприятия, которые в состоянии обеспечить большие объемы производства и сбыта; имеют устойчивый спрос на свою продукцию.

Метод аналогий обычно используется при анализе рисков нового проекта.

Проект рассматривастся как "живой" организм, имеющий определенные стадии развития.

Жизненный цикл проекта состоит из:

этапа разработки,

этапа выведения на рынок,

этап роста,

этапа зрелости и

этапа упадка.

Изучая жизненный цикл проекта, можно получить информацию о каждом этапе проекта, выделить причины нежелательных последствий, оценить степень риска. Однако на практике бывает довольно трудно собрать соответствующую информацию.

Нельзя забывать, что последствия неверных оценок рисков или отсутствия возможности противопоставить действенные меры могут быть самыми неприятными.

1.6. Специфика сбора информации для оценки рисков на различных предприятиях

Каждое предприятие имеет свою информационную среду для определения источников хозяйственного риска, и одна из функций риск-менеджера как раз и заключаются в своевременном выявлении, группировке и ранжировании опасностей.

Важной составной частью организации работ по сбору информации и выявлению

рисков является разработка специальной программы по контролю и выявлению новых рисков, которая имеет собственный бюджет и экономическое обоснование.

Итак, к основным методам получения исходной информации и выявления опасностей относятся:

1. Опросные листы. Существует два типа — стандартизированные и специализированные. Стандартизированные, или универсальные, листы разрабатываются и используются международными ассоциациями консультантов или страховщиков для унификации статистических данных и применимы для большинства предприятий. Опросный лист включает несколько разделов, каждый из которых содержит перечень вопросов, позволяющих составить полное представление о структуре и количественных показателях описываемого объекта. Специализированные опросные листы разрабатываются для конкретных видов деятельности и стимулируют респондентов выявлять характерные для них особенности рисков.

2. Структурные диаграммы, позволяющие выявлять, прежде всего, внутренние риски, связаные с качеством менеджмента, маркетинга, организацией работы и т.д. Структурные диаграммы описывают особенности структуры предприятия и зависят от сложившегося типа управления и принципов разделения функций. В основном структурные диаграммы предоставляют возможность выявления внутренних рисков, таких как дублирование функций одного отдела другими, зависимость и концентрация, а также позволяют определить отсутствие или недостаточность хорошо налаженных связей между подразделениями.

3. Карты потоков или потоковые диаграммы выявляют основные опасности производственного процесса и позволяют примерно оценить надежность и устойчивость узловых элементов производства. В то же время, без привлечения дополнительных источников информации потоковые диаграммы не дают возможности определить степень вероятности наступления риска. Виды карт потоков делятся на три группы: описывающие отдельный технологический процесс внутри предприятия; совокупность производственных процессов и элементов управления; технологическую цепочку, в которой предприятие является отдельным звеном.

4. Инспектирование дает возможность получения дополнительной информации и проверки ее достоверности и полноты на местах. Существует практика неожиданных инспекций объектов и заблаговременного извещения. В любом случае при планировании посещения объекта прежде всего необходимо четко определить перечень задач и вопросов, которые могут быть решены либо уточнены в процессе прямой инспекции. После предварительной оценки задач и учета различных особых факторов составляется программа посещения объекта, содержащая логическую схему выявления рисков, которая позволяет не упустить что-либо существенное. Все результаты инспекции оформляются в виде отчета, в котором указывается цель обследования, дата и место проведения, краткое содержание, результаты, заключение. Эффективность инспекции зависит от умения риск-менеджера отмечать важные нюансы, которые могут быть упущены респондентами опросных листов или специалистами, осуществляющими определенные технологические операции.

5.Анализ отчетности важен для выявления финансовых, коммерческих, предпринимательских рисков. В финансовой и управленческой документации фиксируются все события, имеющие отношение к увеличению или уменьшению риска. Риск-менеджер, анализируя финансовые и управленческие документы, систематически использует всю

доступную информацию для идентификации опасностей, связанных с условиями заключения договоров, эффективностью использования финансовых ресурсов предприятия и выполнением обязательств. Наличие у менеджера надежной деловой информации позволяет ему быстро принимать оптимальное финансовое или коммерческое решение, влияет на правильность таких решений и ведет к снижению потерь и увеличению прибыли. Надлежащее использование информации при заключении сделок сводит к минимуму вероятность финансовых потерь.

В целом риск-менеджмент весьма динамичен. Эффективность его функционирования во многом зависит от скорости реакции на изменение условий рынка, экономической ситуации, финансового состояния объекта управления. Поэтому риск-менеджмент должен базироваться на знании стандартного набора приемов управления риском, на умении быстро и адекватно оценивать конкретную экономическую ситуацию, на способности быстро найти оптимальное, если не единственное, решение

Таким образом, существующие способы построения кривой вероятностей возникновения определенного уровня потерь не совеем равноценны, но так или иначе позволяют произвести приблизительную оценку общего объема финансового риска.

ГЛАВА 2. СИСТЕМА УПРАВЛЕНИЯ РИСКАМИ В ПРЕДПРИНИМАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ

2.1. Система управления рисками

Система управления представляет собой сложный механизм воздействия управляющей системы на управляемую с целью получения желаемого результата. Таким образом, управление риском как система состоит из двух подсистем:

Управляемой подсистемы (объекта управления) и управляющей подсистемы (субъекта управления).

В системе управления риском объектом управления являются риск, рисковые вложения капитала, экономические отношения между хозяйствующими подразделениями в процессе реализации риска.

Субъектом управления в системе управления риском является специальная группа людей (руководитель, финансовый менеджер, менеджер по риску и другие), которая посредством различных приемов и способов управления осуществляет целенаправленное воздействие на объект управления.

Существует интересное мнение по поводу использования термина "система управления риском". Специалисты считают, что с точки зрения исследования операций словосочетание управление риском лишено смысла, поскольку неопределенностью управлять нельзя.

Таким образом, когда говорят о системе управления риском, речь идет о системе поддержки принятия решения того или иного субъекта, главная задача которой в максимальной степени снизить неопределенность, имеющую место при принятии решений

субъектом. На наш взгляд, такая трактовка системы управления риском несколько сужает ее предназначение.

Система управления РИСКОМ, несомненно, включает процесс принятия решений, однако на этом ее функции не ограничиваются. Система управления риском включает также дальнейший мониторинг рисковых позиций, их хеджирование, порядок взаимодействия подразделений в процессе контроля за принятыми рисками и т.п.

При анализе системы управления рисками целесообразно использовать в качестве основного методологического инструмента системный подход.

Системный подход представляет собой всесторонний подход, фокусирующий внимание не только на организации, но и на окружающей ее среде. Центральным понятием системного подхода является понятие "система", которое отражает понятие о том, что различные элементы, соединяясь, приобретают новое качество, которое отсутствует у каждого из них в отдельности.

Новое качество возникает благодаря наличию связей в системе, которые осуществляют перенос свойств каждого элемента системы ко всем остальным элементам системы. Такие связи называются интегральными или системными.

Эффективность функционирования системы управления риском, исходя из основных положений системного подхода, определяется эффективным взаимодействием между частями системы, нежели результативной работой ее отдельных частей.

Таким образом, система управления рисками представляет собой совокупность взаимосвязанных и взаимозависимых элементов, конечной целью существования которых является минимизация рисков.

Систему управления риском можно охарактеризовать как совокупность методов, приемов и мероприятий, позволяющих в определенной степени прогнозировать наступление рисковых событий и принимать меры к исключению или снижению отрицательных последствий наступления таких событий. На систему управления риском оказывают влияние как внутренние, так и внешние факторы.

Системный подход предписывает искать истоки проблем, возникающих в работе, в первую очередь во внешней среде.

2.2. Принципы риск-менеджмента

Для организации корпоративной системы управления рисками необходимо соблюдение четырех основополагающих принципов.

Первый принцип. Коллегиальный орган управления. Многолетний опыт, накопленный банкирами-лидерами в решении задач корпоративного риск-менеджмента, свидетельствует о том, что для эффективного управления рисками нужна децентрализация функций по принятию управленческих решений. Решения, связанные с риском, не должны приниматься одним человеком, или, если это необходимо, полномочия такого лица должны быть ограничены в разумных пределах. Как говорится, одна голова — хорошо, а две или десять — лучше. Это объясняется потребностью в устранении конфликта интересов (злоупотреблений в целях получения личной выгоды) и однобоких суждений (ясно, что ни один человек не обладает сверхспособностями). Как правило, такой коллегиальный орган управления формируется из наиболее разносторонних и опытных руководителей высшего и среднего руководящего звена. Здесь можно провести параллель с организацией бюджетного процесса, когда из общего числа руководителей предприятия

разного уровня выделяется ряд лиц, ответственных за его создание и подготовку стратегических планов развития предприятия, которые рассматривают проекты бюджетов до их утверждения на высшем уровне и периодически собираются на оперативные совещания (планерки). Именно эти люди могут рассматриваться в качестве членов коллегиального органа управления предприятием, на который будут возложены функции по управлению рисками.

Второй принцип. Независимое аналитическое подразделение. Для поддержки процесса принятия управленческих решений требуется формирование специализированного и самостоятельного аналитического подразделения, сотрудники которого, являясь высококвалифицированными экономистами, должны обладать также знаниями во всех специфических областях деятельности предприятия. Нельзя сказать, что подобного подразделения и сотрудников у предприятий никогда не было. Речь идет о планово-экономическом отделе, который может послужить в качестве базы для создания подразделения, отвечающего за независимую оценку рисков и информационно-аналитическую поддержку решений, принимаемых упомянутым коллегиальным органом управления.

Третий принцип. Система внутреннего контроля. Как в любой сфере деятельности, для обеспечения эффективности принимаемых управленческих решений в сфере управления рисками необходима система контроля над их выполнением, как подразделениями предприятия, так и отдельно взятыми должностными лицами. Это, кстати, тоже нельзя назвать новшеством, так как действующий бюджетный процесс предполагает контроль исполнения утвержденных бюджетов. Если на предприятии внедрено бюджетирование, создание системы внутреннего контроля будет в значительной степени облегчено. Кроме того, в штате крупных предприятий нередко встречаются внутренние аудиторы, на которых могут и должны быть возложены соответствующие функции.

Четвертый принцип. Мотивация персонала. Как уже неоднократно отмечалось, важным (если не ключевым) условием внедрения предприятием риск-ориентированного менеджмента является развитие культуры корпоративного управления — культуры управления рисками. Практика показывает, что ни одна инициатива со стороны высшего руководства предприятия (кроме индексации зарплаты) не будет восприниматься рядовыми сотрудниками и менеджерами среднего звена должным образом без соответствующей мотивации, будь то административные, в том числе материальные поощрения либо взыскания или же какие-нибудь иные способы.

Как видно из сказанного выше, управление рисками нельзя назвать чем-то принципиально новым для менеджмента предприятия — многие его составляющие в том или ином виде уже знакомы руководящему составу и даже присутствуют в повседневной работе предприятия. Поэтому интерес к внедрению риск-ориентированного менеджмента можно охарактеризовать как очередной эволюционный этап развития предприятия, который является закономерной реакцией на постоянный рост технологичности бизнеса и объективное ужесточение конкуренции как на внутреннем рынке, так и на международной арене. Это становится особенно актуальным, если учесть, что Россия находится на пороге вхождения во Всемирную торговую организацию (ВТО).

Еще одним аргументом в пользу сделанных выводов может послужить бурный рост интереса к такой, казалось бы, не связанной с обсуждаемой темой, но очень популярной в последнее время проблеме, как контроль качества. Можно даже говорить о настоящем буме вокруг получения предприятиями сертификатов соответствия международным стандартам контроля качества серии ISO 9000. Это связано с тем, что сертификат ISO

давно уже является знаком качества продукции или услуг для конечного потребителя, а значит, дополнительной гарантией надежности и профессиональной компетентности предприятия, его руководителей и персонала. Наличие таких сертификатов в значительной степени распространено среди иностранных предприятий, которые из сегодняшних партнеров завтра смогут превратиться в прямых конкурентов.

2.3. Функции риск-менеджмента

Риск-менеджмент выполняет определенные функции. Различают два типа функций риск-менеджмента:

1) функции объекта управления;
2) функции субъекта управления.

К функциям объекта управления в риск-менеджменте относится организация:

- разрешения риска;
- рисковых вложений капитала;
- работы по снижению величины риска;
- процесса страхования рисков;
- экономических отношений и связей между субъектами хозяйственного процесса.

К функциям субъекта управления в риск-менеджменте относятся:

- прогнозирование;
- организация;
- регулирование;
- координация;
- стимулирование;
- контроль.

Прогнозирование в риск-менеджменте представляет собой разработку на перспективу изменений финансового состояния объекта в целом и его различных частей. Прогнозирование - это предвидение определенного события. Оно не ставит задачу непосредственно осуществить на практике разработанные прогнозы. Особенностью прогнозирования является также альтернативность в построении финансовых показателей и параметров, определяющая разные варианты развития финансового состояния объекта управления на основе наметившихся тенденций. В динамике риска прогнозирование может осуществляться как на основе экстраполяции прошлого в будущее с учетом экспертной оценки тенденции изменения, так и на основе прямого предвидения изменений. Эти изменения могут возникнуть неожиданно. Управление на основе предвидения этих изменений требует выработки у менеджера определенного чутья рыночного механизма и интуиции, а также применения гибких экстренных решений.

Организация в риск-менеджменте представляет собой объединение людей, совместно реализующих программу рискового вложения капитала на основе определенных правил и процедур. К этим правилам и процедурам относятся: создание органов управления, построение структуры аппарата управления, установление взаимосвязи между управленческими подразделениями, разработка норм, нормативов, методик и т.п.

Регулирование в риск-менеджменте представляет собой воздействие на объект управления, посредством которого достигается состояние устойчивости этого объекта в

случае возникновения отклонения от заданных параметров. Регулирование охватывает главным образом текущие мероприятия по устранению возникших отклонений.

Координация в риск-менеджменте представляет собой согласованность работы всех звеньев системы управления риском, аппарата управления и специалистов.

Координация обеспечивает единство отношений объекта управления, субъекта управления, аппарата управления и отдельного работника.

Стимулирование в риск-менеджменте представляет собой побуждение финансовых менеджеров и других специалистов к заинтересованности в результате своего труда.

Контроль в риск-менеджменте представляет собой проверку организации работы по снижению степени риска. Посредством контроля собирается информация о степени выполнения намеченной программы действия, доходности рисковых вложений капитала, соотношении прибыли и риска, на основании которой вносятся изменения в финансовые программы, организацию финансовой работы, организацию риск-менеджмента. Контроль предполагает анализ результатов мероприятий по снижению степени риска.

2.4. Организация системы риск-менеджмента на предприятии

Одни и те же риски могут встречаться в различных областях производственно-хозяйственной деятельности. Поэтому при управлении рисками главное — идентифицировать возможные области риска применительно к исследуемому предприятию. Риск количественно характеризуется субъективной оценкой ожидаемой величины максимального и минимального доходов (убытков) от конкретного вложения капитала. При этом чем больше диапазон между возможным максимальным и минимальным доходами (убытками) при равной вероятности их получения, тем выше степень риска. Степень риска — это вероятность наступления рискового события; чем больше неопределенность хозяйственной ситуации при принятии решения, тем больше и степень риска. Факторы, влияющие на величину степени риска, можно разделить на объективные и субъективные. К объективным факторам относятся причины, возникающие во внешней среде предприятия, то есть не зависящие непосредственно от деятельности фирмы. Например, политические, экономические и экологические кризисы, таможенная, налоговая, бюджетная политика государства. Субъективные факторы связаны непосредственно с внутренней средой фирмы и характеризуют ее деятельность: уровень производительности труда, уровень технического и технологического оснащения, производственный потенциал, система управления, организация труда, маркетинговая, ценовая, инвестиционная политика предприятия.

Риск-менеджмент характеризуется совокупностью методов, приемов и мероприятий, позволяющих в определенной степени прогнозировать наступление рисков и принимать решения по воздействию на них. Стратегия управления риском строится в зависимости от направлений деятельности предприятия. Для эффективного управления риском на предприятиях может создаваться специальное подразделение — отдел управления рисками. Во главе его стоит риск-менеджер, который занимается исключительно проблемами управления риском и координирует деятельность всех подразделений в плане регулирования риска и обеспечения компенсации возможных потерь и убытков. Риск-менеджер формирует организационную структуру управления риском на предприятии и разрабатывает основные положения и инструкции, связанные с этой деятельностью.

2.5. Задачи и процесс управления рисками

Важнейшим этапом, следующим за прогнозированием оценкой и анализом риска в предпринимательской деятельности, является управление риском.

Управление риском имеет целью решение следующих задач:

1. Выживание. Удержание издержек и других параметров (моральных, экологических, юридических и др.) организации в границах, которые позволяют сохранить фирму как работающую и прибыльную.

2. Приемлемый уровень беспокойства. Иногда эту задачу называют "обеспечением покоя и нормального сна". Следует добавить, что эта задача ставится, как правило, с точки зрения руководства или владельца фирмы, но вопрос стоит более широко.

Все, кто так или иначе заинтересован судьбой фирмы, должен спать по возможности спокойно. Чувство безопасности, вера в устойчивость достигнутого благосостояния и в возможность улучшения благосостояния - это базовые потребности человека.

Человек спокойный обычно лучше работает. Однако человек слишком спокойный и уверенный в том, что ему гарантирована хорошая жизнь, начинает расслабляться.

Следовательно, уровень беспокойства должен быть по заданным критериям оптимальным. Критерии могут быть разными.

3. Стабильность доходов. Эту задачу следует трактовать как стабильность благосостояния всех сторон, заинтересованных в фирме.

4. Приемлемая непрерывность работы. В любой организации возможны сбои в работе. Задача - не допустить сбоев и остановок, чреватых гибелью фирмы.

5. Целесообразный темп устойчивого роста фирмы. Требуется подготовленность к риску срыва роста и ситуационное обеспечение возможных потерь, которые могут замедлить рост или сделать его неустойчивым.

6. Социальная ответственность. Прямого отношения к бизнесу данной фирмы это может и не иметь, но любой индивидуальный и групповой член общества должен вносить свою лепту в благосостояние общества.

7. Удовлетворение ограничений внешнего характера: юридических, регуляторных, традиционных и т.п.

8. Экономичность, удержание себестоимости управления предпринимательским риском на уровне, минимально достаточном для нормальной работы фирмы.

Все эти задачи имеют разную окраску и должны по-разному планироваться до потерь, во время кризиса и после потерь.

Например, решение задачи выживания до потерь может планироваться как прогнозирование сокрушительных потерь, проведение профилактических мероприятий.

Во время кризиса возникает необходимость оперативного планирования управления кризисом, снижение фактических потерь и недопущение сокрушительных потерь.

После потерь: оценка потенциально сокрушительных потерь:

- защита страховых интересов фирмы по сокрушительным потерям;
- преследование виновных и судебная защита фирмы.

Четкое определение задач очень важно при организаации службы управления рисками, а также при согласованной деятельности ее различных компонент.

Процесс управления рисками фирмы - это прежде все принятие стратегии отношения фирмы к рискам вообще и каждому конкретному риску в отдельности.

Для обеспечения рисковой стратегии создается программа интегрированного управления рисками фирмы. После принятия программы к исполнению и внедрению на этой основе ведется мониторинг рисковой обстановки. При необходимости производится корректировка рисковой стратегии, и, соответственно, программы управления рисками.

Говоря о процессах управления риском, не следует иметь в виду только продукт, производимый фирмой. Сама фирма является "живым", целостным организмом, проходящим различные циклы своей деятельности. На этапах этих циклов возникают риски, источники которых могут быть как внутри, так и вне самой фирмы.

На первых этапах жизни фирма расходует деньги, разрабатывает продукт, подготавливая производство и обустраивая рыночную нишу, а доходов не зарабатывает.

На этапе быстрого роста возникает необходимость постоянного внешнего финансирования, которое относительно легко доступно, но опасна эйфория роста и избыточное заимствование.

На этапе зрелости темп роста замедляется, а фирма производит больше денег, чем может эффективно реинвестировать в свой бизнес.

На последней стадии фирма может быть умеренно прибыльной при снижающихся продажах, но неспособна реинвестировать в свою деятельность.

Этапы жизненного цикла организации могут быть представлены самым различным образом. Целесообразно анализировать прежде всего ее внутреннюю и внешнюю динамику.

1 . Внутренняя динамика

1 .1. Создание коммерческой организации:

разработка миссии и стратегических целей бизнеса;

определение рыночной ниши;

определение продуктового ряда;

выбор источника финансирования проекта создания фирмы;

проведение PR-компании;

запуск проекта.

1.2. Управление текущей деятельностью коммерческой организации:

трансакции;

максимизация прибыли;

сокращение издержек;

технологические переходы;

решение социальных задач;

решение экологических задач;

страхование;

фондовые операции.

1.3. Стратегическое управление коммерческой организацией:

реструктуризация в рамках сложившейся структуры;

рост фирмы;

замедление;

стабилизация;

рецессия;

упадок или новый цикл.

2. Внешняя динамика

2.1. Интеграционные процессы:
слияние;
разделение;
приобретение;
альянсы;
партнерство;
вертикальная интеграция.
2.2. Освоение новых рынков:
горизонтальная интеграция;
диверсификация;
развитие экспортного потенциала.

Внутренняя и внешняя динамика коммерческой организации формирует одно измерение задач управления рисками, которые могут иметь место на каждом этапе жизненного цикла коммерческой организации.

Другое - виды финансовых ресурсов, используемых для реализации внутренней и внешней динамики фирмы (внутреннее финансирование, привлечение средств акционеров - пассивные инвесторы, заемное финансирование).

Можно построить матрицу, дающую самое общее представление о видах рисков, "разнесенных" по источникам финансирования и источникам жизненного цикла. На пересечении осей матрицы будет сформировано пять (в соответствии с приведенными ранее жизненными циклами) основных классов задач управления рисками.

Тот факт, что организационные системы - деловые организации, фирмы, корпорации и т.д. - многомерные не нов. Через всю последнюю треть прошедшего века красной нитью проходит идея системности. Это произошло в результате эволюции теории управления и бурного развития компьютеров, компьютерных сетей и программ обработки знаний.

В приложении к формирующейся ныне теории рисков фирмы многомерный подход к управлению может опираться на следующие идеи:

- необходимо выявление логично строгих информационных иерархий, через которые фирма получает данные;
- процесс детализации структур информации создает основу для дальнейшего манипулирования информацией на разных должностных позициях в фирме с разной степенью обобщения информации без нарушения целостности подхода;
- база данных строится на многомерном пересечении этих иерархий, образующих многомерный параллелепипед. Каждая рисковая экспозиция имеет по крайней мере три измерения:

1) тип ценности, находящийся под угрозой;
2) источник, вызывающий риск;
3) величина возможных и фактических финансовых и других последствий.

Кроме того, классификация экспозиций фирмы должна учитывать еще одно измерение, а именно - внутрифирменные, внефирменные, отечественные, зарубежные риски.

Важно отметить особую значимость информационного обеспечения управления риском, состоящего из разного рода и вида информации: статистической, экономиче-

ской, коммерческой, финансовой и т.д., а также методов ее обработки, хранения и обновления.

2.6. Этапы организации риск-менеджмента

Риск-менеджмент по экономическому содержанию представляет собой систему управления риском и финансовыми отношениями, возникающими в процессе этого управления.

Как система управления, риск-менеджмент включает в себя процесс выработки цели риска и рисковых вложений капитала, определение вероятности наступления события, выявление степени и величины риска, анализ окружающей обстановки, выбор стратегии управления риском, выбор необходимых для данной стратегии приемов управления риском и способов его снижения (т.е. приемов риск-менеджмента), осуществление целенаправленного воздействия на риск. Указанные процессы в совокупности составляют этапы организации риск-менеджмента.

Организация риск-менеджмента представляет собой систему мер, направленных на рациональное сочетание всех его элементов в единой технологии процесса управления риском (рис. 5).

Первым этапом организации риск-менеджмента является определение цели риска и цели рисковых вложений капитала. **Цель** риска - это результат, который необходимо получить. Им может быть выигрыш, прибыль, доход и т.п. Цель рисковых вложений капитала - получение максимальной прибыли.

Любое действие, связанное с риском, всегда целенаправленно, так как отсутствие цели делает решение, связанное с риском, бессмысленным. Цели риска и рисковых вложений калитка должны быть четкими, конкретизированными и сопоставимыми с риском и капиталом.

Следующим важным моментом в организации риск-менеджмента является получение информации об окружающей обстановке, которая необходима для принятия решения в пользу того или иного действия. На основе анализа такой информации и с учетом целей риска можно правильно определить вероятность наступления события, в том числе страхового события, выявить степень риска и оценить его стоимость. Управление риском означает правильное понимание степени риска, который постоянно угрожает людям, имуществу, финансовым результатам хозяйственной деятельности.

Для предпринимателя важно знать действительную стоимость риска, которому подвергается его деятельность.

Под стоимостью риска следует понимать фактические убытки предпринимателя, затраты на снижение величины этих убытков или затраты по возмещению таких убытков и их последствий. Правильная оценка финансовым менеджером действительной стоимости риска позволяет ему объективно представлять объем возможных убытков и наметить пути к их предотвращению или уменьшению, а в случае невозможности предотвращения убытков обеспечить их возмещение.

На основе имеющейся информации об окружающей среде, вероятности, степени и величине риска разрабатываются различные варианты рискового вложения капитала и проводится оценка их оптимальности путем сопоставления ожидаемой прибыли и величины риска.

Это позволяет правильно выбрать стратегию и приемы управления риском, а так-

же способы снижения степени риска.

На этом этапе организации риск-менеджмента главная роль принадлежит финансовому менеджеру, его психологическим качествам. Об этом подробнее будет рассказано в следующей главе.

При разработке программы действия по снижению риска необходимо учитывать психологическое восприятие рисковых решений. Принятие решений в условиях риска является психологическим процессом. Поэтому наряду с математической обоснованностью решений следует иметь в виду проявляющиеся при принятии и реализации рисковых решений психологические особенности человека: агрессивность, нерешительность, сомнения, самостоятельность, экстраверсию, интроверсию и др.

Одна и та же рисковая ситуация воспринимается разными людьми по-разному. Поэтому оценка риска и выбор финансового решения во многом зависит от человека, принимающего решения. От риска обычно уходят руководители консервативного типа, не склонные к инновациям, не уверенные в своей интуиции и в своем профессионализме, не уверенные в квалификации и профессионализме исполнителей, т.е. своих работников.

Экстраверсия - есть свойство личности, проявляющееся в ее направленности на окружающих людей, события. Она выражается в высоком уровне общительности, живом эмоциональном отклике на внешние явления.

Интроверсия - это направленность личности на внутренний мир собственных ощущений, переживаний, чувств и мыслей. Для интровертивной личности характерны некоторые устойчивые особенности поведения и взаимоотношений с окружающими, опора на внутренние нормы, самоуглубленность. Суждения, оценки интравертов отличаются значительной независимостью от внешних факторов, рассудительностью. Обычно человек совмещает в определенной пропорции черты экстраверсии и интроверсии.

Неотъемлемым этапом организации риск-менеджмента является организация мероприятий по выполнению намеченной программы действия, т.е. определение отдельных видов мероприятий, объемов и источников финансирования этих работ, конкретных исполнителей, сроков выполнения и т.п.

Важным этапом организации риск-менеджмента являются контроль за выполнением намеченной программы, анализ и оценка результатов выполнения выбранного варианта рискового решения.

Организация риск-менеджмента предполагает определение органа управления риском на данном хозяйственном субъекте. Органом управления риском может быть финансовый менеджер, менеджер по риску или соответствующий аппарат управления: сектор страховых операций, сектор венчурных инвестиций, отдел рисковых вложений капитала и т.п. Эти секторы или отделы являются структурными подразделениями финансовой службы хозяйствующего субъекта.

Отдел рисковых вложений капитала в соответствии с уставом хозяйствующего субъекта может осуществлять следующие функции:

- проведение венчурных и портфельных инвестиций, т.е. рисковых вложений капитанов в соответствии с действующим законодательством и уставом хозяйствующего субъекта;
- разработка программы рисковой инвестиционной деятельности;
- сбор, обработка, анализ и хранение информации об окружающей обстановке;
- определение степени и стоимости рисков, стратегии и приемов управления

риском;

- разработка программы рисковых решений и организация ее выполнения, включая контроль и анализ результатов;
- осуществление страховой деятельности, заключение договоров страхования и перестрахования, проведение страховых и перестраховых операций, расчетов по страхованию;
- разработка условий страхования и перестрахования, установление размеров тарифных ставок по страховым операциям;
- выполнение функции аварийного комиссара, выдача гарантии по поручительству российских и иностранных страховых компаний, возмещение убытков за их счет, поручение другим лицам исполнение аналогичных функций за рубежом;
- ведение соответствующей бухгалтерской, статистической и оперативной отчетности по рисковым вложениям капитала.

2.7. Внешние и внутренние факторы системы управления рисками

Внешними факторами системы управления риском являются:

· нормативная база в сфере регулирования риска (нормативы, методики, рекомендации, стандарты бухгалтерского учета и т.п.);

· макроэкономические факторы;

· зарубежный опыт управления риском.

Наиболее характерными чертами внешней среды является динамичность многообразие и интегрированность.

Динамичность предполагает быструю изменчивость внешней среды. Задача - создавать адаптивные системы управления риском, которые не сопротивляются изменениям внешней среды, а меняются вместе с ней.

Следующая характерная черта внешней среды - многообразие. Современная организация взаимодействует с огромным числом различных объектов - акционерами, клиентами, партнерами, Центральным банком, органами власти, конкурентами и т.д. Все это многообразие усугубляется еще и тем, что все объекты связаны между собой множеством нитей - экономических, информационных, политических, административных, постоянно влияют друг на друга, то есть внешняя среда интегрирована.

Следовательно, изменение взаимодействия организации с любым из этих объектов влечет за собой изменение отношений и с остальными.

Внутренние факторы системы управления риском включают:

1. специфику деятельности организации, его политику, стратегию и тактику,
2. организационную структуру,
3. квалификацию персонала.

Основными чертами внутренней среды являются:

· стремление к выживанию,

· постоянное изменение, развитие, направленное на приспособление к внешней среде,

· совершенствование,

· наличие целостности, единого предназначения для всех элементов.

Как система управления, управление риском предполагает осуществление ряда процессов и действий, которые представляют собой элементы системы управления

риском. К ним можно отнести:

- идентификацию и локализацию риска;
- анализ и оценку риска;
- способы минимизации и предотвращения риска;
- мониторинг рисковых позиций.

Процесс управления риском можно упрощенно представить в виде блок-схемы (рис. 4).

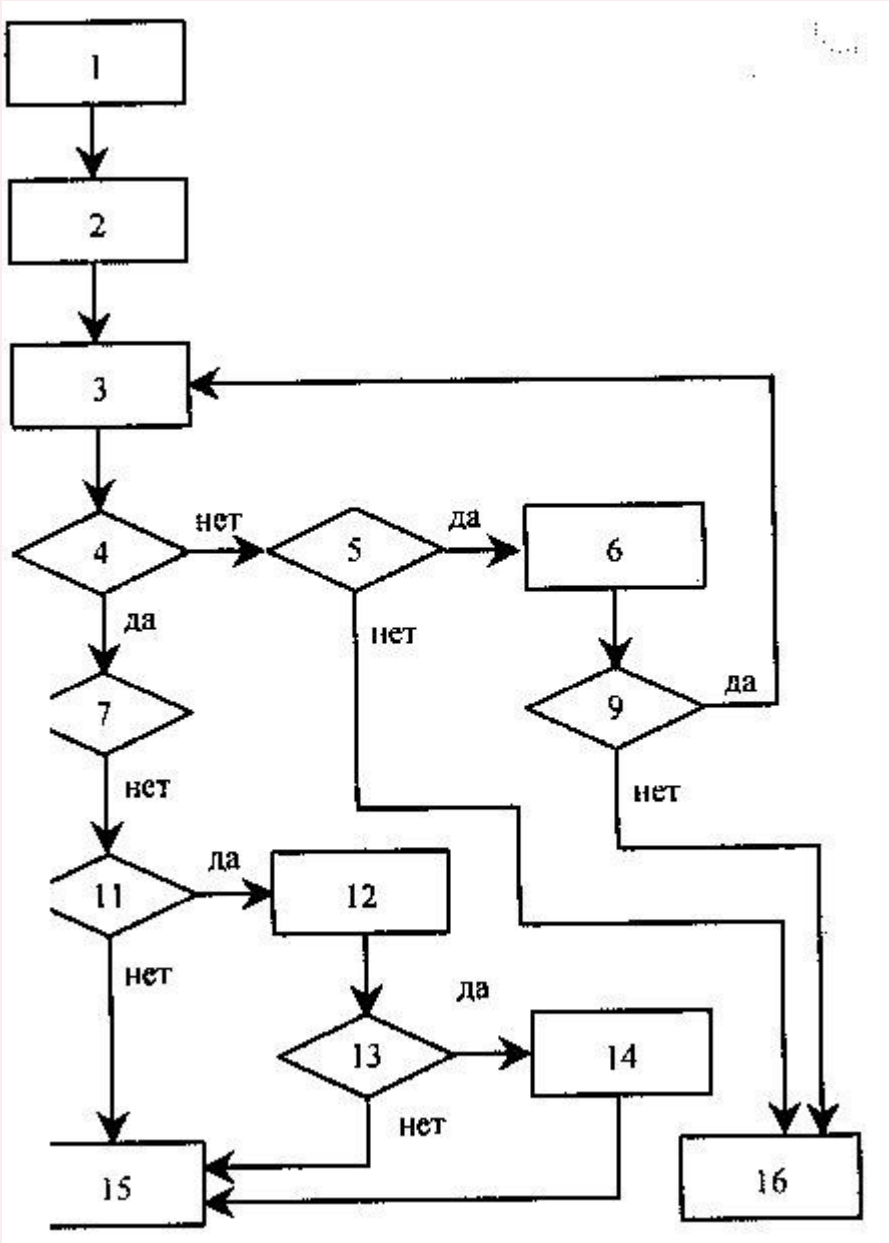


Рис. 4. Блок-схема процесса управления риском:

1 - сбор и обработка данных; 2 - качественный анализ риска;

3 - количественная оценка риска; 4 - оценка приемлемости риска;

5, 11 - оценка возможности снижения риска; 6,12 - выбор методов и формирование вариантов снижения риска,

7 - оценка возможности увеличения риска; 8- формирование и выбор вариантов увеличения риска;

9,13 - оценка целесообразности снижения риска;

10 -оценка целесообразности увеличения риска;

14 - выбор варианта снижения риска;
15 - реализация проекта (принятие риска);
16 - отказ от реализации проекта (избежание риска)

Следует отметить, что сбор и обработка информации является важным этапом процесса управления независимо от его конкретного содержания. В процессе управления риском к полноте и качеству информации предъявляются особые требования, так как отсутствие полной информации является одним из существенных факторов риска, и принятие решения в условиях неполной информации служит источником дополнительных финансовых потерь.

На схеме для упрощения блок-схемы сбор и обработка информации по аспектам риска представлены в качестве первого этапа. В действительности эта работа осуществляется на протяжении всего процесса принятия решения

По мере перехода от одного этапа к другому при необходимости может уточняться потребность в дополнительной информации, осуществляться ее сбор и обработка.

Особую роль играет информация в процессе качественного и количественного анализа риска.

Качественный анализ предполагает: выявление источников и причин риска, этапов и работ, при выполнении которых возникает риск, т.е. установление потенциальных зон риска, идентификацию всех возможных рисков, выявление практических выгод и возможных негативных последствий, которые могут наступить при реализации содержащего риск решения.

Результаты качественного анализа служат важной исходной информацией для осуществления количественного анализа.

Количественный анализ предполагает численное определение отдельных рисков и общего риска. На этом этапе определяется вероятность наступления рисковых событий и их последствий, осуществляется количественная оценка степени риска, определяется также допустимый уровень риска.

В результате проведения анализа риска получается картина возможных рисковых событий, вероятность их наступления и последствий. После сравнения полученных значений рисков с предельно допустимыми вырабатывается стратегия управления риском, и на этой основе - меры предотвращения и уменьшения риска.

Меры по устранению и минимизации риска включают следующие этапы:

1. оценку приемлемости полученного уровня риска;
2. оценку возможности снижения риска или его увеличения (в случае, когда полученные значения риска значительно ниже допустимого, а увеличение степени риска обеспечит повышение ожидаемой отдачи);
3. выбор методов снижения (увеличения) рисков;
4. оценку целесообразности и выбор вариантов снижения (увеличения) рисков.

После выбора определенного набора мер по устранению и минимизации риска следует принять решение о степени достаточности выбранных мер. Если мер недостаточно целесообразно отказаться от реализации проекта (избежать риска).

Следует отметить, что нами рассмотрена лишь общая схема процесса управления риском. Характер и содержание перечисленных этапов и работ, используемые методы их выполнения в значительной степени зависят от специфики предпринимательской деятельности и характера возможных рисков.

2.8. Особенности выбора стратегии и методов решения управленческих задач

На этом этапе организации риск-менеджмента главная роль принадлежит финансовому менеджеру, его психологическим качествам. Финансовый менеджер, занимающийся вопросами риска (менеджер по риску), должен иметь два права: право выбора и право ответственности за него.

Право выбора означает право принятия решения, необходимого для реализации намеченной цели рискового вложения капитала. Решение должно приниматься менеджером единолично. В риск-менеджменте из-за его специфики, которая обусловлена прежде всего особой ответственностью за принятие риска, нецелесообразно, а в отдельных случаях и вовсе недопустимо коллективное (групповое) принятие решения, за которое никто не несет никакой ответственности. Коллектив, принявший решение, никогда не отвечает за его выполнение. При этом следует иметь в виду, что коллективное решение в силу психологических особенностей отдельных индивидов (их антагонизма, эгоизма, политической, экономической или идеологической платформы и т.п.) является более субъективным, чем решение, принимаемое одним специалистом.

Для управления риском могут создаваться специализированные группы людей, например сектор страховых операций, сектор венчурных инвестиций, отдел рисковых вложений капитала (т.е. венчурных и портфельных инвестиций) и др.

Данные группы людей могут подготовить предварительное коллективное решение и принять его простым или квалифицированным (т.е. две трети, три четверти, единогласно) большинством голосов.

Однако окончательно выбрать вариант принятия риска и рискового вложения капитала должен один человек, так как он одновременно принимает на себя и ответственность за данное решение.

Ответственность указывает на заинтересованность принимающего рисковое решение в достижении поставленной им цели.

При выборе стратегии и приемов управления риском часто используется какой-то определенный стереотип, который складывается из опыта и знаний финансового менеджера в процессе его работы и служит основой автоматических навыков в работе. Наличие стереотипных действий дает менеджеру возможность в определенных типовых ситуациях действовать оперативно и наиболее оптимальным образом. При отсутствии типовых ситуаций финансовый менеджер должен переходить от стереотипных решений к поискам оптимальных, приемлемых для себя рисковых решений.

Подходы к решению управленческих задач могут быть самыми разнообразными, потому риск-менеджмент обладает многовариантностью.

Многовариантность риск-менеджмента означает сочетание стандарта и неординарности финансовых комбинаций, гибкость и неповторимость тех или иных способов действия в конкретной хозяйственной ситуации. Главное в риск-менеджменте - правильная постановка цели, отвечающая экономическим интересам объекта управления.

Риск-менеджмент весьма динамичен. Эффективность его функционирования во многом зависит от быстроты реакции на изменения условий рынка, экономической ситуации, финансового состояния объекта управления. Поэтому риск-менеджмент должен базироваться на знании стандартных приемов управления риском, на умении быстро и правильно оценивать конкретную экономическую ситуацию, на способности быстро найти хороший, если не единственный выход из этой ситуации.

В риск-менеджменте готовых рецептов нет и быть не может. Он учит тому, как, зная методы, приемы, способы решения тех или иных хозяйственных задач, добиться ощутимого успеха в конкретной ситуации, сделав ее для себя более или менее определенной.

Особую роль в решении рисковых задач играют интуиция менеджера и инсайт.

Интуиция представляет собой способность непосредственно, как бы внезапно, без логического продумывания находить правильное решение проблемы. Интуитивное решение возникает как внутреннее озарение, просветление мысли, раскрывающее суть изучаемого вопроса. Интуиция является непременным компонентом творческого процесса. Психология рассматривает интуицию во взаимосвязи с чувственным и логическим познанием и практической деятельностью как непосредственное знание в его единстве со знанием опосредованным, ранее приобретенным.

Инсайт - это осознание решения некоторой проблемы. Субъективно инсайт переживают как неожиданное озарение, постижение. В момент самого инсайта решение осознается очень ясно, однако эта ясность часто носит кратковременный характер и нуждается в сознательной фиксации решения.

2.9. Правила риск-менеджмента

В случаях, когда рассчитать риск невозможно, принятие рисковых решений происходит с помощью эвристики.

Эвристика представляет собой совокупность логических приемов и методических правил теоретического исследования и отыскания истины. Иными словами, это правила и приемы решения особо сложных задач.

Конечно, эвристика менее надежна и менее определенна, чем математические расчеты. Однако она дает возможность получить вполне определенное решение.

Риск-менеджмент имеет свою систему эвристических правил и приемов для принятия решений в условиях риска.

Основные правила риск-менеджмента:

1. Нельзя рисковать больше, чем это может позволить собственный капитал.
2. Надо думать о последствиях риска.
3. Нельзя рисковать многим ради малого.
4. Положительное решение принимается лишь при отсутствии сомнения.
5. При наличии сомнений принимаются отрицательные решения.
6. Нельзя думать, что всегда существует только одно решение. Возможно, есть и другие.

Реализация первого правила означает, что прежде, чем принять решение о рисковом вложении капитала, финансовый менеджер должен:

1) определить максимально возможный объем убытка по данному риску;
2) сопоставить его с объемом вкалываемого капитала:
3) сопоставить его со всеми собственными финансовыми ресурсами и определить, не приведет ли потеря этого капитала к банкротству данного инвестора.

Объем убытка от вложения капитала может быть равен объему данного капитала, чуть меньше или больше его.

При прямых инвестициях объем убытка, как правило, равен объему венчурного капитала.

Инвестор вложил 1 млн. руб. в рисковое дело. Дело прогорело. Инвестор потерял 1 млн. руб.

Однако с учетом снижения покупательной способности денег в условиях инфляции объем потерь может быть больше, чем сумма вкладываемых денег. В этом случае объем возможного убытка следует определять с учетом индекса инфляции. Инвестор вложил 1 млн. руб. в рисковое дело в надежде получить через год 5 млн. руб. Дело прогорело. Если через год деньги не вернули, то объем убытка следует считать с учетом индекса инфляции (например, 220%), т.е. 2,2 млн. руб. (2,2 х 1). При прямом убытке, нанесенном пожаром, наводнением, кражей и т.п., размер убытка больше прямых потерь имущества, так как оно включает еще дополнительные денежные затраты на ликвидацию последствий убытка и приобретение нового имущества.

При портфельных инвестициях, т.е. при покупке ценных бумаг, которые можно продать на вторичном рынке, объем убытка обычно меньше суммы затраченного капитала.

Соотношение максимально возможного объема убытка и объема собственных финансовых ресурсов инвестора представляет собой степень риска, ведущую к банкротству. Она измеряется с помощью коэффициента риска: К=У/С,

где К - коэффициент риска;

У - максимально возможная сумма убытка, руб.;

С - объем собственных финансовых ресурсов с учетом точно известных поступлений средств, руб.

Исследования рисковых мероприятий, проведенные автором, позволяют сделать вывод, что оптимальный коэффициент риска составляет 0,3, а коэффициент риска, ведущий к банкротству инвестора, - 0,7 и более.

Реализация второго правила требует, чтобы финансовый менеджер, зная максимально возможную величину убытка, определил бы, к чему она может привести, какова вероятность риска, и принял решение об отказе от риска (т.е. от мероприятия), принятии риска на свою ответственность или передаче риска на ответственность другому лицу.

Действие третьего правила особенно ярко проявляется при передаче риска, т.е. при страховании. В этом случае он означает, что финансовый менеджер должен определить и выбрать приемлемое для него соотношение между страховым взносом и страховой суммой. Страховой взнос - это плата страхователя страховщику за страховой риск. Страховая сумма - это денежная сумма, на которую застрахованы материальные ценности, ответственность, жизнь и здоровье страхователя. Риск не должен быть удержан, т.е. инвестор не должен принимать на себя риск, если размер убытка относительно велик по сравнению с экономией на страховом взносе.

Реализация остальных правил означает, что в ситуации, для которой имеется только одно решение (положительное или отрицательное), надо сначала попытаться найти другие решения. Возможно, они действительно существуют. Если же анализ показывает, что других решений нет, то действуют по правилу «в расчете на худшее», т.е. если сомневаешься, то принимай отрицательное решение.

ГЛАВА 3. ПРОФИЛЬНЫЕ РИСКИ

3.1. Риск-профиль финансовых организаций

Как уже отмечалось, компании реального сектора экономики и финансовые организации — это как бы два разных, но в то же время очень похожих друг на друга мира. Значит, и риски в их деятельности должны быть сопоставимы. Поэтому обратимся к уже накопленному финансовыми организациями опыту.

В относительно устоявшейся в настоящее время практике управления рисками принято выделять следующие основные виды рисков:

- кредитные риски — риски возникновения потерь вследствие несвоевременных платежей или неплатежей со стороны контрагентов;
- рыночные риски (в том числе фондовые, процентные и валютные) — риски возникновения убытков вследствие неблагоприятного изменения рыночных цен (например, котировок ценных бумаг, уровня процентных ставок по кредитам, обменных курсов валют и т. д.);
- риски ликвидности— риски возникновения неблагоприятных последствий (в том числе убытков) в результате неспособности организации своевременно и в полном объеме исполнить обязательства перед кредиторами;
- операционные риски (в том числе правовые) — риски возникновения непредвиденных убытков следующего характера:
- внутреннего — из-за неадекватности бизнес-процессов, квалификации персонала и надежности применяемых технических средств масштабам деятельности организации;
- внешнего — в результате негативного воздействия неконтролируемых организацией факторов (например, катастрофы, стихийные бедствия, преступность и коррупция);
- стратегические риски — риски возникновения убытков вследствие принятия высшим руководством организации компетентных управленческих решений, однако основанных на оказавшихся ошибочными предположениях о развитии внешней экономической среды; другими словами, непредска зуемые риски деловых неудач;
- репутационные риски — риски сужения масштабов деятельности организации (вплоть до ликвидации) вследствие утраты доверия к ней со стороны клиентов и деловых партнеров.

Все указанные виды рисков называют типичными банковскими рисками. По крайней мере, потому, что так делают центральные банки (регуляторы) подавляющего большинства развитых стран. Однако считать, что сфера влияния этих рисков ограничивается лишь банковским сектором экономики, по меньшей мере, некорректно.

Чтобы проиллюстрировать ход мысли регуляторов банковского сектора экономики, приведем простой пример: если завтра назвать закупку карандашей типичным видом банковской деятельности, то любой банк будет вынужден под страхом отзыва лицензии приобретать карандаши в строгом соответствии с предъявляемыми требованиями. Другими словами, чтобы заставить банки задумываться о чем-то важном, но непривлекательном с финансовой точки зрения, регуляторам проще всего назвать это типичным для банковской деятельности, а затем устанавливать соответствующие требования. Поэтому, учитывая широту затрагиваемых проблем, приведенный список типичных банковских

рисков с некоторыми допущениями можно признать если не исчерпывающим, то хотя бы достаточным для организации абсолютно любой отраслевой принадлежности. Так, например, кредитные риски для предприятий часто проявляются в виде недоставок и неплатежей со стороны клиентов и поставщиков. Однако предприятия также принимают кредитные риски в классическом понимании этого слова на обслуживающие банки, не говоря уже о предоставлении займов (по сути, тех же кредитов) другим организациям.

Пожалуй, единственное серьезное отличие списка типичных рисков для предприятий от соответствующего списка для финансовых организаций — наличие в деятельности первых существенных концентрационных рисков. Сущность этих рисков заключается в объективно меньшей способности предприятий диверсифицировать свой бизнес как географически, так и по отраслям экономики, чем это могут позволить себе финансовые организации, перемещая свои капиталы с помощью фондового рынка буквально за считанные дни.

3.2. Основные направления нейтрализации предпринимательских рисков

Предпринимательская организация в процессе осуществления производственно-хозяйственной деятельности может отказаться от совершения отдельных операций или видов деятельности, связанных с высоким уровнем риска, т.е. уклониться от риска. Данное направление нейтрализации рисков является наиболее простым и радикальным. Оно позволяет полностью избежать потенциальных потерь, связанных с предпринимательскими рисками, но, с другой стороны, не позволяет и получить прибыли, связанные с рискованной деятельностью. Кроме того, в отдельных случаях уклонение от риска может быть просто невозможным, а также избежание одного вида риска может привести к возникновению других. Поэтому, как правило, данный способ применим лишь в отношении очень серьезных и крупных рисков.

Решение об отказе от определенных предпринимательских рисков может быть принято как на предварительной стадии принятия решения, так и позднее, путем отказа от дальнейшего осуществления деятельности, в том случае, если риск оказался выше предполагаемого. Однако большинство решений об избегании риска принимается на предварительной стадии принятия решения, так как отказ от продолжения деятельности часто влечет значительные финансовые и иные потери для предприятия, а иногда затруднителен в связи с контрактными обязательствами предпринимательской организации.

Применение такого способа нейтрализации предпринимательских рисков, как уклонение от риска, эффективно при выполнении определенных условий.

Отказ от одного вида предпринимательского риска не влечет за собой возникновения других видов рисков более высокого или однозначного уровня.

Уровень риска намного выше уровня возможной доходности предпринимательской сделки или деятельности в целом.

Финансовые потери по данному виду риска предпринимательская фирма не имеет возможности возместить за счет собственных финансовых средств, так как эти потери слишком высоки.

Естественно, что не от всех видов предпринимательских рисков предприятие может уклониться, большую часть из них оно "принимает на себя", т.е. сознательно идет на риск и занимается бизнесом до тех пор, пока убытки от последствий наступивших рис-

ков не приведут к невосполнимым потерям. Некоторые риски принимаются, так как несут в себе потенциал возможной прибыли, другие принимаются в силу своей неизбежности.

При "принятии риска на себя" основной задачей является изыскание источников необходимых ресурсов для покрытия возможных потерь. В данном случае потери покрываются из любых ресурсов, оставшихся после наступления предпринимательского риска, и, как следствие, наступления потерь. Если оставшихся ресурсов у предприятия недостаточно, то это может привести к сокращению объемов бизнеса.

Ресурсы, имеющиеся в распоряжении предпринимательской организации для покрытия потерь, можно разделить на две группы:

1. ресурсы внутри самого бизнеса;
2. кредитные ресурсы.

Ресурсы внутри самого бизнеса. При возникновении потерь крайне редко бывают повреждены все виды собственности одновременно, поэтому к внутренним ресурсам относятся:

- наличность в кассе, которая не страдает при физическом повреждении зданий и сооружений, принадлежащих предприятию;
- остаточная стоимость поврежденной собственности;
- доход от частичного продолжения как финансовой, так и производственной деятельности;
- дивиденды и процентный доход от ценных бумаг и доходных инвестиций;
- дополнительные средства, вносимые владельцами бизнеса с целью его поддержания и пр.;
- нераспределенный остаток прибыли, полученной в отчетном периоде, до его распределения он может рассматриваться как резерв финансовых ресурсов, направляемых в необходимом случае на ликвидацию негативных последствий отдельных финансовых рисков.

Резервный фонд образуется за счет отчислений от прибыли в размере, определенном уставом, но не менее 15% его уставного капитала. Ежегодно в резервный фонд должно отчисляться не менее 5% чистой прибыли до тех пор, пока резервный капитал не достигнет установленного уставом размера. Резервный капитал в узком смысле предназначен для покрытия его убытков, а в акционерных обществах также для погашения облигаций общества и выкупа их акций в случае отсутствия иных средств. Если резервный фонд используется на указанные цели, то отчисления в него производятся из прибыли до налогообложения, т.е. отчисления в резервный фонд не облагаются налогом на прибыль.

Кредитные ресурсы. В том случае, если предпринимательская организация не в состоянии покрыть все потери, возникающие в результате воздействия предпринимательских рисков, из внутренних ресурсов, часть из них можно покрыть с использованием кредитных ресурсов. Однако в данном случае доступность кредитных ресурсов имеет существенные ограничения. И главным из них является перспектива будущей прибыльности предприятия. Доступность кредитных ресурсов во многом зависит от остаточной стоимости бизнеса после возникновения потерь. Другим ограничением в привлечении кредитных ресурсов после возникновения рисков может быть их цена. Использование кредитных ресурсов может ослабить финансовое положение предпринимательской организации.

Следующий возможный метод нейтрализации рисков, возникающих в процессе осуществления предпринимательской деятельности предприятия, - это передача или трансферт риска партнерам по отдельным сделкам или хозяйственным операциям путем заключения контрактов. При этом хозяйственным партнерам передается та часть предпринимательских рисков предприятия, по которой оно имеет больше возможностей нейтрализации их негативных последствий и, как правило, располагает более эффективными способами внутренней страховой защиты. В современной практике управления рисками получили распространение следующие основные направления передачи рисков.

Передача рисков путем заключения договора факторинга. Предметом передачи в данном случае является кредитный риск предприятия, который в преимущественной его доле передается коммерческому банку или специализированной факторинговой компании, что позволяет предприятию в существенной степени нейтрализовать негативные финансовые последствия кредитного риска.

Передача риска путем заключения договора поручительства. Российское законодательство предусматривает возможность заключения договора поручительства. В силу договора поручитель обязывается перед кредитором третьего лица отвечать за исполнение последним его обязательства полностью или частично. При неисполнении или ненадлежащем исполнении должником обеспеченного поручительством обязательства поручитель и должник отвечают перед кредитором солидарно. Предприятие использует поручительства для привлечения заемного капитала и при этом несет ответственность перед поручителем за четкое исполнение договора поручительства. Таким образом, предприятие-кредитор передает риск невозврата кредита и связанные с этим потери поручителю.

Существует еще один вид гаранта – это банковская гарантия, - письменное обязательство кредитной организации, выданное по просьбе другого лица - принципала, уплатить кредитору принципала – бенефициару в соответствии с условиями даваемого гарантом обязательства денежную сумму по представлении бенефициаром письменного требования о ее уплате. За выдачу банковской гарантии принципал уплачивает гаранту вознаграждение. Банковская гарантия позволяет предпринимательской организации избежать риски при заключении сделок с оплатой в будущем или по факту предоставления услуг, выполнения работ, отгрузки товаров.

Передача рисков поставщикам сырья и материалов. Предметом передачи в данном случае являются прежде всего риски, связанные с порчей или потерей имущества в процессе транспортировки и осуществления погрузочно-разгрузочных работ. Однако потери, связанные с падением рыночной цены продукции, несет предприятие, даже если подобное падение вызвано задержкой в доставке груза.

Передача рисков путем заключения биржевых сделок. Этот метод передачи риска осуществляется путем хеджирования.

Биржевые сделки снижают риск снабжения в условиях инфляционных ожиданий и отсутствия надежных оперативных каналов закупок. Минимизация рисков снабжения в данном случае также осуществляется за счет передачи риска путем:

приобретения опционов на закупку товаров и услуг, цена на которые в будущем увеличится;

заключения фьючерсных контрактов на закупку растущих в цене товаров.

5. Контракты продажи, обслуживания, снабжения. Договоры, связанные с распространением товаров и услуг, также предоставляют предприятию широкие возможности по снижению риска путем их передачи. Производитель или дистрибьютор обычно предлагает потребителю гарантию устранения дефектов либо замены недоброкачественного товара или недоброкачественно выполненной услуги. При этом потребитель, покупая товар или услугу, передает риски, связанные с его эксплуатацией, производителю или дистрибьютору на период гарантии.

Возможно также соглашение между оптовым торговцем и производителем или между розничным и оптовым торговцами о возврате части непроданных товаров. В данном случае речь идет о передаче рыночного риска.

К этой же группе контрактов сносятся:

- соглашение о снабжении товаром на условиях поддержания неснижаемого остатка на складе;
- аренда оборудования с гарантией его технического обслуживания и текущего ремонта;
- гарантия поддержания производительности (определенных технических характеристик) используемого оборудования;
- договоры на сервисное обслуживание техники.

В целом же передача риска происходит, если в заключенном сторонами контракте существует специфическое положение относительно передачи конкретных (или всех) предпринимательских рисков контрагенту. Сторона, принявшая на себя риск, обычно вторично передает его, заключив договор страхования ответственности.

Еще одним способом минимизации или нейтрализации рисков является распределение риска путем объединения (с разной степенью интеграции) с другими участниками, заинтересованными в успехе общего дела. Предприятие имеет возможность уменьшить уровень собственного риска, привлекая к решению общих проблем в качестве партнеров другие предприятия и даже физических лиц. Для этого могут создаваться акционерные общества, финансово-промышленные группы; предприятия могут приобретать или обмениваться акциями друг друга, вступать в различные консорциумы, ассоциации, концерны.

Таким образом, под объединением предпринимательского риска понимается метод снижения риска, при котором риск делится между несколькими субъектами экономики. Объединяя усилия в решении проблемы, несколько предпринимательских организаций могут разделить между собой как возможную прибыль, так и убытки от ее реализации. Как правило, поиски партнеров проводятся среди тех предприятий, которые располагают дополнительными финансовыми ресурсами, а также информацией о состоянии и особенностях рынка.

Одним из эффективных способов нейтрализации рисков является диверсификация. В качестве основных форм диверсификации предпринимательских рисков предприятием могут быть использованы следующие основные виды диверсификации.

Диверсификация предпринимательской деятельности предприятия, которая предусматривает использование альтернативных возможностей получения дохода от различных видов деятельности, не посредственно не связанных друг с другом. В таком случае, если в результате непредвиденных событий один вид деятельности окажется убыточным, другие будут приносить прибыль.

Диверсификация портфеля ценных бумаг. Данный вид диверсификации позволяет снижать инвестиционные риски, не уменьшая при этом уровень доходности инвестиционного портфеля.

Диверсификация программы реального инвестирования. В области формирования реального инвестиционного портфеля фирме рекомендуется отдавать предпочтение программам реализации нескольких проектов, относительно небольшой капиталоемкости перед программами, состоящими из единственного крупного инвестиционного проекта.

Диверсификация кредитного портфеля, которая направлена на снижение кредитного риска предприятия и предусматривает разнообразие покупателей продукции или услуг предпринимательской организации.

Диверсификация поставщиков сырья, материалов и комплектующих. В случае сбоя в поставках предпринимательской фирме не придется искать альтернативных поставщиков, а можно будет увеличить объемы закупок у других поставщиков.

Диверсификация покупателей продукции.

Диверсификация валютной корзины предприятия. Данный вид диверсификации предусматривает выбор нескольких различных видов валют в процессе осуществления предприятием внешнеэкономических операций. В результате использования этого вида диверсификации предпринимательская организация имеет возможность минимизировать валютные риски.

Существуют еще так называемые упреждающие методы нейтрализации предпринимательских рисков. Эти методы, как правило, более трудоемки, требуют обширной предварительной аналитической работы, от полноты и тщательности которой зависит эффективность их применения. К методам компенсации относятся:

- стратегическое планирование деятельности предпринимательской организации;
- обеспечение компенсации возможных финансовых потерь за счет включаемой в контракты системы штрафных санкций;
- сокращение перечня форс-мажорных обстоятельств в контрактах с партнерами;
- совершенствование управления оборотными средствами предприятия;
- сбор и анализ дополнительной информации о финансовом рынке;
- прогнозирование тенденций изменения внешней предпринимательской среды и конъюнктуры рынка.

В данном разделе были рассмотрены лишь основные пути нейтрализации предпринимательских рисков. Применение отдельных из них в деятельности конкретной предпринимательской организации зависит от опыта и возможностей, которыми она обладает.д.ля получения более эффективного результата, как правило, используется не один, а совокупность способов. Перечисленные способы могут быть существенно дополнены с учетом специфики деятельности отдельных предприятий и конкретного состава портфеля их предпринимательских рисков.

Следующий метод минимизации риска – это страхование. Страхование хозяйственных рисков представляет собой отношения по защите имущественных интересов физических и юридических лиц при наступлении определенных событий (страховых случаев) за счет денежных фондов, формируемых из уплачиваемых ими страховых взносов (страховых премий). Следует отметить, что данный метод минимизации) риска имеет ряд ограничений:

- в первую очередь – это слишком высокая цена (иногда премия), запрашиваемая страховщиком за принятие на себя риска. Нередко она превышает ту цену, которую принципиальный страхователь полагает разумной за передачу данного риска;
- во вторую – ограниченная доступность страхования – некоторые риски не принимаются к страхованию. Так, если вероятность наступления рискового события очень велика, страховые организации либо не берутся страховать данный вид риска, либо назначают непомерно высокие платежи.

Цена и доступность страхования прямо связаны между собой, так как страхователь принимает на себя тот риск, потери от которого он может оценить.

Страхуемый вид риска характерен для таких чрезвычайных ситуаций, когда существует статистическая закономерность их возникновения, т.е. определена вероятность убытка. Отметим, что с помощью страхования можно минимизировать практически все имущественные, а также многие кредитные, коммерческие и производственные риски. Вместе с тем страхованию, как правило, не подлежат риски, связанные с недобросовестностью партнеров, - задержка платежей, неоплата продукции и т.п.

3.3. Управления рисками организаций инвестиционно-строительного комплекса

Сегодня одним из важнейших условий успешного функционирования предприятий инвестиционно-строительной сферы, обеспечивающих увеличение стоимости их активов, стабильное получение прибыли и реализацию социальных программ, является управление рисками. Вопросы риск-менеджмента в строительстве приобретают все большую актуальность. Управление рисками предприятия становится одним из ключевых конкурентных преимуществ независимо от формы собственности, и организационно-правовой формы предприятия инвестиционно-строительного комплекса.

Процесс управления и оценки рисков при принятии инвестиционных решений имеет большое значение, поскольку позволяет оценить возможные потери, запланировать процедуры для возможного их снижения, а также определить экономический эффект от управления рисками.Целью управления риском является снижение вероятности, частоты событий совпадения проявления рисков по различным причинам и, как следствие, снижение суммарных потерь (ущерба) по проекту.

При разработке и реализации инвестиционного проекта в строительстве преследуются две основные цели:

создать объект, удовлетворяющий требованиям, предъявляемым заказчиком, инвестором или покупателем и соответствующий действующим нормам и правилам;

создать механизм для покрытия понесенных заказчиком затрат и дальнейшего получения прибыли.

Непосредственным решением этих задач и занимается система риск-менеджмента в инвестиционном строительстве.

Управление риском в инвестиционном строительстве является сложной проблемой, на сегодняшний день мало изученной как в России, так и за рубежом. Основная причина такого положения — отсутствие аналитического описания воздействия возмущающих факторов, оказывающих влияние на систему управления и её составляющие.

Неизбежность возникновения рисковых ситуаций при строительстве требует разработки и применения соответствующих методов предупреждения, идентификации и ре-

агирования на них с целью исключения или максимально влзможного снижения убытков.

Эффективное управление рисками в строительстве должно базироваться на принципах управления, являющихся одной из составляющих управленческой методологии, к которым следует отнести:

- осознанность принятия рисков;
- управляемость принимаемых рисков;
- независимость управления рисками;
- сопоставимость уровня управления принимаемых рисков с доходностью;
- сопоставимость уровня управления принимаемых рисков с финансовыми возможностями предприятия;
- экономичность управления рисками;
- учет временного фактора;
- учет финансовой стратегии предприятия;
- возможность передачи рисков.

Современный этап эволюции теории управления характеризуется появлением новой парадигмы – управление рисками, где в качестве интегрированного объекта управления выступает интегрированный риск предприятия. В соответствии с данной парадигмой риск-менеджмент должен быть:

- системным и интегрированным, т. е. управление рисками должно осуществляться в рамках всего предприятия, охватывая все уровни наблюдений: исполнителей, подразделения, стратегические бизнес-единицы, бизнес-процессы;

– непрерывным, т. е. управление рисками не должно зависеть от желаний менеджеров и должно охватывать все уровни управления: стратегический, тактический, оперативный;

– расширенным и комплексным, т. е. объектом управления должны быть все риски: внешние и внутренние, страхуемые и не страхуемые, частные и интегрированные. Предприятия должны на основе предлагаемого рискового спектра разрабатывать свой рисковый профиль;

– структурированным и последовательным, т. е. при управлении рисками должны реализовываться все функции управления: анализ и синтез, прогнозирование и планирование, организация и координация, учет и контроль, мотивация;

– целевым и стоимостноориентированным, т. е. управление рисками должно быть направлено на увеличение стоимости предприятия за счет выявления факторов неопределенности, рискообразующих факторов и управления ими, а также за счет непосредственного воздействия на риски методами страхования и самострахования.

Укрупненная схема управления рисками предприятия должна быть представлена в определенной логической последовательности.

1. Выявление и анализ рисков предприятия.
2. Описание угроз и классификация рисков.
3. Выявление и идентификация рисков.
4. Оценка рисков.
5. Выбор методов управления (воздействия) рисками при сравнении их эффективности.
6. Принятие решений о воздействии на риски.
7. Непосредственное управление (воздействие) рисками.

8. Мотивация менеджеров и сотрудников к максимальному выявлению и эффективному управлению рисками.

9. Контроль и корректировка результатов управления рисками.

При управлении рисками предприятия целесообразно использовать стоимостный подход, при этом необходимо разработать и внедрить систему управления рисками, включающую стратегию, структурные решения, совокупность методов воздействия на риски, кадровое и информационное обеспечение.

Система риск-менеджмента на предприятиях инвестиционно-строительного комплекса имеет свои особенности, которые во многом объясняются сложностью, многоэтапностью и длительными сроками процесса строительства. Процесс возведения объектов строительства осуществляется в общем случае в сферах инвестиций, изысканий, проектирования, управления и контроля качества строительства.

В процессе строительства стоимость возведенного объекта изменяется от нуля – в начале работ, до полной стоимости в соответствии с исполненным проектом – при сдаче объекта заказчику. Соответственно, изменяется и тяжесть возможного ущерба. Однако нельзя не отметить тот факт, что по мере строительства уменьшается количество монтажных нагрузок и воздействий, а следовательно, и риск возникновения ущерба от превышения их расчетных значений. По мере завершения строительства увеличивается риск возникновения ущерба от превышения эксплуатационных нагрузок и воздействий. Указанные характерные особенности строительства как процесса создания недвижимого имущества, безусловно, важны при оценке рисков возникновения ущербов, однако, как показывает опыт аварий строительных объектов в России, значительные материальные ущербы возникают в основном не из-за воздействий на объекты строительства опасностей, размеры которых превышают учтенные при расчетах в проектах, а по другим причинам. Анализ информации о крупных авариях зданий и сооружений показывает, что в половине случаев причинами являются низкое качество строительства и монтажа, материалов и конструкций.

Международная практика страхования строительных рисков предусматривает страховое покрытие не отдельных рисков, оговоренных в договоре страхования, а от всех рисков, которые могут произойти на строительной площадке. Именно такой полис, заключенный на условиях CAR (Contractors All Risks) может обеспечить по-настоящему эффективную защиту сооружаемого объекта от строительных рисков.

Однако время идет вперед, и сегодня строительным организациям необходимо уже не просто страхование, а комплексная система управления рисками – риск-менеджмент, поэтому некоторые страховые компании начали предлагать подрядчикам профессиональные услуги по управлению рисками. Сущность риск-менеджмента в на предприятиях инвестиционно-строительного комплекса заключается в исследовании возможных рисков, которым подвержен конкретный проект, оценке по специальным методикам их вероятности и разрушительности, в выявлении альтернативы, где величина риска остается приемлемой, и в выборе методов управления риском, способствующих устранению или минимизации возможных отрицательных последствий.

Для построения эффективной системы управления рисками предприятия необходимо применять различные методы воздействия па них. К методам воздействия на риски предприятий инвестиционно-строительной сферы, существующим в настоящее время и реально используемым в практической деятельности, можно отнести: страхование рисков; уклонение от рисков (избежание), передача рисков; распределение (разделение) и

диверсификация рисков; объединение рисков; лимитирование рисков; резервирование средств (создание фондов), локализация и предупреждение рисков; компенсация рисков.

Страхование рассматривается в этой системе как один из инструментов управления рисками, но инструмент наиболее эффективный, позволяющий решать вопросы комплексной защиты не только строительного процесса, а всего строительно-инвестиционного проекта.

Страхование риска является одним из наиболее распространенных способов снижения его степени. Страхование – это особые экономические отношения. Для них обязательно наличие двух сторон: страховщика и страхователя. Страховщик создает за счет платежей различных страхователей единый денежный фонд (страховой или резервный фонд). Сущность страхования выражается в том, что стратег готов отказаться от части доходов для того, чтобы минимизировать риск, т. е. он готов заплатить определенную сумму (очевидно меньшую ожидаемого дохода) за снижение степени риска до нуля.

ГЛАВА 4. СПОСОБЫ СНИЖЕНИЯ ФИНАНСОВОГО РИСКА

Высокая степень финансового риска проекта приводит к необходимости поиска путей ее искусственного снижения.

Снижение степени риска - это сокращение вероятности и объема потерь.

Для снижения степени риска применяются различные приемы. Наиболее распространенными являются:

- диверсификация;
- приобретение дополнительной информации о выборе и результатах;
- лимитирование;
- самострахование;
- страхование;
- страхование от валютных рисков;
- хеджирование;
- приобретение контроля над деятельностью в связанных областях;
- учет и оценка доли использования специфических фондов компании в ее общих фондах и др.

Диверсификация представляет собой процесс распределения капитала между различными объектами вложения, которые непосредственно не связаны между собой.

Диверсификация позволяет избежать части риска при распределении капитала между разнообразными видами деятельности. Например, приобретение инвестором акций пяти разных акционерных обществ вместо акций одного общества увеличивает вероятность получения им среднего дохода в пять раз и соответственно в пять раз снижает степень риска.

Диверсификация является наиболее обоснованным и относительно менее издержкоемким способом снижения степени финансового риска.

Диверсификация - это рассеивание инвестиционного риска. Однако она не может свести инвестиционный риск до нуля. Это связано с тем, что на предпринимательство и инвестиционную деятельность хозяйствующего субъекта оказывают влияние внешние факторы, которые не связаны с выбором конкретных объектов вложения капитала, и,

следовательно, на них не влияет диверсификация.

Внешние факторы затрагивают весь финансовый рынок, т.е. они влияют на финансовую деятельность всех инвестиционных институтов, банков, финансовых компаний, а не на отдельные хозяйствующие субъекты.

К внешним факторам относятся процессы, происходящие в экономике страны в целом, военные действия, гражданские волнения, инфляция и дефляция, изменение учетной ставки Банка России, изменение процентных ставок по депозитам, кредитам в коммерческих банках, и т.д. Риск, обусловленный этими процессами, нельзя уменьшить с помощью диверсификации.

Таким образом, риск состоит из двух частей: диверсифицируемого и недиверсифицируемого риска (рис. 6).

Диверсифицируемый риск, называемый еще несистематическим, может быть устранен путем его рассеивания, т.е. диверсификацией.

Недиверсифицируемый риск, называемый еще систематическим, не может быть уменьшен диверсификацией.

Причем исследования показывают, что расширение объектов вложения капитала, т.е. рассеивания риска, позволяет легко и значительно уменьшить объем риска. Поэтому основное внимание следует уделить уменьшению степени недиверсифицируемого риска.

С этой целью зарубежная экономика разработала так называемую «портфельную теорию». Частью этой теории является модель увязки систематического риска и доходности ценных бумаг (Capital Asset Pricing Model – CAPM)

Информация играет важную роль в риск-менеджменте. Финансовому менеджеру часто приходится принимать рисковые решения, когда результаты вложения капитала не определены и основаны на ограниченной информации. Если бы у него была более полная информация, то он мог бы сделать более точный прогноз и снизить риск. Это делает информацию товаром, причем очень ценным. Инвестор готов заплатить за полную информацию.

Стоимость полной информации рассчитывается как разница между ожидаемой стоимостью какого-либо приобретения или вложения капитала, когда имеется полная информация, и ожидаемой стоимостью, когда информация неполная.

Лимитирование - это установление лимита, т.е. предельных сумм расходов, продажи, кредита и т.п. Лимитирование является важным приемом снижения степени риска и применяется банками при выдаче ссуд, при заключении договора на овердрафт и т.п. Хозяйствующими субъектами он применяется при продаже товаров в кредит, предоставлении займов, определении сумм вложения капитала и т.п.

Самострахование означает, что предприниматель предпочитает подстраховаться сам, чем покупать страховку в страховой компании. Тем самым он экономит на затратах капитала по страхованию. Самострахование представляет собой децентрализованную форму создания натуральных и страховых (резервных) фондов непосредственно в хозяйствующем субъекте, особенно в тех, чья деятельность подвержена риску.

Создание предпринимателем обособленного фонда возмещения возможных убытков в производственно-торговом процессе выражает сущность самострахования. Основная задача самострахования заключается в оперативном преодолении временных затруднений финансово-коммерческой деятельности. В процессе самострахования создаются различные резервные и страховые фонды. Эти фонды в зависимости от цели назна-

чения могут создаваться в натуральной или денежной форме.

Так, фермеры и другие субъекты сельского хозяйства создают прежде всего натуральные страховые фонды: семенной, фуражный и др. Их создание вызвано вероятностью наступления неблагоприятных климатических и природных условий.

Резервные денежные фонды создаются прежде всего на случай покрытия непредвиденных расходов, кредиторской задолженности, расходов по ликвидации хозяйствующего субъекта. Создание их является обязательным для акционерных обществ.

Акционерные общества и предприятия с участием иностранного капитала обязаны в законодательном порядке создавать резервный фонд в размере не менее 15% и не более 25% от уставного капитала.

Акционерное общество зачисляет в резервный фонд также эмиссионный доход, т.е. сумму разницы между продажной и номинальной стоимостью акций, вырученной при их реализации по цене, превышающей номинальную стоимость. Эта сумма не подлежит какому-либо использованию или распределению, кроме случаев реализации акций по цене ниже номинальной стоимости.

Резервный фонд акционерного общества используется для финансирования непредвиденных расходов, в том числе также на выплату процентов по облигациям и дивидендов по привилегированным акциям в случае недостаточности прибыли для этих целей.

Хозяйствующие субъекты и граждане для страховой защиты своих имущественных интересов могут создавать общества взаимного страхования.

Наиболее важным и самым распространенным приемом снижения степени риска является страхование риска.

Сущность страхования выражается в том, что инвестор готов отказаться от части своих доходов, чтобы избежать риска, т.е. он готов заплатить за снижение степени риска до нуля.

Хеджирование (англ. *heaging* - ограждать) используется в банковской, биржевой и коммерческой практике для обозначения различных методов страхования валютных рисков. Так, в книге Долан Э. Дж. и др. «Деньги, банковское дело и денежно-кредитная политика» этому термину дается следующее определение: «Хеджирование - система заключения срочных контрактов и сделок, учитывающая вероятностные в будущем изменения обменных валютных курсов и преследующая цель избежать неблагоприятных последствий этих изменений». В отечественной литературе термин «хеджирование» стал применяться в более широком смысле как страхование рисков от неблагоприятных изменений цен на любые товарно-материальные ценности по контрактам и коммерческим операциям, предусматривающим поставки (продажи) товаров в будущих периодах.

Контракт, который служит для страховки от рисков изменения курсов (цен), носит название «хедж» (англ. *hedge* - изгородь, ограда). Хозяйствующий субъект, осуществляющий хеджирование, называется «хеджер». Существуют две операции хеджирования: хеджирование на повышение; хеджирование на понижение.

Хеджирование на повышение, или хеджирование покупкой, представляет собой биржевую операцию по покупке срочных контрактов или опционов. Хедж на повышение применяется в тех случаях, когда необходимо застраховаться от возможного повышения цен (курсов) в будущем. Он позволяет установить покупную цену намного раньше, чем был приобретен реальный товар. Предположим, что цена товара (курс валюты или ценных бумаг) через три месяца возрастет, а товар нужен будет именно через три

месяца. Для компенсации потерь от предполагаемого роста цен необходимо купить сейчас по сегодняшней цене срочный контракт, связанный с этим товаром, и продать его через три месяца в тот момент, когда будет приобретаться товар. Поскольку цена на товар и на связанный с ним срочный контракт изменяется пропорционально в одном направлении, то купленный ранее контракт можно продать дороже почти на столько же, на сколько возрастет к этому времени цена товара. Таким образом, хеджер, осуществляющий хеджирование на повышение, страхует себя от возможного повышения цен в будущем.

Хеджирование на понижение, или хеджирование продажей - это биржевая операция с продажей срочного контракта. Хеджер, осуществляющий хеджирование на понижение, предполагает совершить в будущем продажу товара, и поэтому, продавая на бирже срочный контракт или опцион, он страхует себя от возможного снижения цен в будущем. Предположим, что цена товара (курс валюты, ценных бумаг) через три месяца снижается, а товар нужно будет продавать через три месяца. Для компенсации предполагаемых потерь от снижения цены хеджер продает срочный контракт сегодня по высокой цене, а при продаже своего товара через три месяца, когда цена на него упала, покупает такой же срочный контракт по снизившейся (почти настолько же) цене. Таким образом, хедж на понижение применяется в тех случаях, когда товар необходимо продать позднее.

Хеджер стремится снизить риск, вызванный неопределенностью цен на рынке, с помощью покупки или продажи срочных контрактов. Это дает возможность зафиксировать цену и сделать доходы или расходы более предсказуемыми. При этом риск, связанный с хеджированием, не исчезает. Его берут на себя спекулянты, т.е. предприниматели, идущие на определенный, заранее рассчитанный риск.

Спекулянты на рынке срочных контрактов играют большую роль. Принимая на себя риск в надежде на получение прибыли при игре на разнице цен, они выполняют роль стабилизатора цен. При покупке срочных контрактов на бирже спекулянт вносит гарантийный взнос, которым и определяется величина риска спекулянта. Если цена товара (курс валюты, ценных бумаг) снизилась, то спекулянт, купивший ранее контракт, теряет сумму, равную гарантийному взносу. Если цена товара возросла, то спекулянт возвращает себе сумму, равную гарантийному взносу, и получает дополнительный доход от разницы в ценах товара и купленного контракта.

Заключение

Актуальность темы рисков определяется процессами, происходящими в экономике России и направленными на реформирование всего хозяйственного механизма в связи с его переориентацией на рыночный тип хозяйствования. В подобной ситуации стремление экономического субъекта стабильно и успешно развиваться сталкивается с только формирующимся (и зачастую нефункционирующим) аппаратом управления деятельностью субъекта. Особенно ярко это проявляется в условиях непрерывных изменений, происходящих в политической и социально-экономической сферах жизни общества на предприятиях реального сектора. Это объясняется, с одной стороны, производственным характером их деятельности, а с другой — неразвитостью механизма снижения воздействия негативных факторов на состояние предприятий, что не позволяет им своевременно и адекватно реагировать на динамику процессов, определяющих социальную и экономическую ситуацию в стране.

На Западе, даже в относительно стабильных экономических условиях, субъекты хозяйствования уделяют пристальное внимание вопросам управления рисками. В то же время, в российской экономике, где факторы экономической нестабильности и без того усложняют вопросы эффективного управления предприятиями, проблемам анализа и управления всем комплексом рисков, возникающих в процессе их экономической деятельности, уделяется явно недостаточное внимание.

До недавнего времени подобный подход доминировал не только на предприятиях реального сектора экономики, но и в финансовокредитных организациях. Пристальное внимание вопросу управления рисками стало уделяться только после финансового кризиса, который отчетливо обозначил всю остроту данной проблемы в России.

Понятие «риск» известно с давних времен. В отечественной экономике исследование вопросов теории риска было в определенной степени востребовано лишь до конца 20-х годов 20 в. В дальнейшем, по мере становления социалистической системы хозяйствования усиливалась роль командно-административных методов управления. Все это в соединении с устранением рыночной мотивации экономики привело к отрицанию проблемы хозяйственного и социального риска. Отдельные же разработки по вопросам производственных, хозяйственных рисков не могли претендовать на право считаться научным направлением.

Таким образом, и в монетарном, и реальном секторах экономикипроблема риска попросту игнорировалась.

Таким образом можно дать определение риску – это вероятность возникновения потерь, убытков, недопоступлений планируемых доходов, прибыли.

Риск – это действие, совершаемое в надежде на счастливый исход по принципу «повезет - не повезет». Конечно риска можно избежать, т.е. просто уклониться от мероприятия, связанного с риском. Однако для предпринимателя избежание риска зачастую означает отказ от возможной прибыли. Хорошая поговорка гласит : «Кто не рискует, тот ничего не имеет».

Поэтому и существуют методы управления финансовыми рисками: упразднение, предотвращение потерь и контроль, страхование, поглощение. При выборе конкретного средства разрешения финансового риска инвестор должен исходить из следующих принципов:

1. нельзя рисковать больше, чем это может позволить собственный капитал;
2. нельзя рисковать многим ради малого;
3. следует предугадывать последствия риска;

Применение на практике этих принципов означает, что всегда необходимо рассчитать максимально возможный убыток по данному виду риска, потом сопоставить его с объемом капитала предприятия, подвергаемое данному риску, и затем сопоставить весь возможный убыток с общим объемом собственных финансовых ресурсов.

Список литературы

1. Бабин В.А. Практические аспекты оценки риска в бизнесе / В.А. Бабин // Управление риском. 2004. № 3. С. 18-20.
2. Багиев Г.Л. Маркетинг: Учебник / Г.Л. Багиев. В.М. Тарасевич, Х. Анн. М.: Экономика, 2001. 703 с.
3. Балабанов И.Т. Риск-менеджмент: Учебное пособие / И.Т. Балабанов. М.: ФиС, 1996. 192 с.
4. Бараненко С.П. Риски и управление ими в системе управления предприятием / С.П. Бараненко, В.В. Шеметов / Управление риском. 2004.№ 2. С. 32-35.
5. Бланк Н.А. Финансовый менеджмент: Учебныи курс / И.А. Бланк. К: Ника-Центр, 2002. 528 с.
6. Борисов А.Б. Большой экономический словарь / А.Б. Борисов. М.: Книжный мир, 2001.895 с.
7. Бусыги А.В. Предпринимательство. Основной курс: Учебник/ А.В. Бусыгин. М.: ИНФРА-М, 1998.608 с.
8. Буянов В.П. Анализ рисков в деятельности предприятия / В.П. Буянов // Вопросы экономики. 2004. № 8. С. 128-134.
9. Буянов В.П. Рискология (Управление рисками) /В.П. Буянов. М.: Экзамен, 2002. 620 с.
10. Викторов, М.Ю., Л.А. Роботова. Проблемы эффективного управления рисками предприятий инвестиционно-строительного комплекса
11. Грабовый П.Г. Риски в современном бизнесе / П.Г. Грабовый. М.: АЛАНС, 1994. 286 с.
12. Гранатуров В.М. Экономический риск: сущность, методы измерения, пути снижения: Учебное пособие / В.М. Гранатуров. М.: ДиС, 2002. 160 с.
13. Грунин О.А. Экономическая безопасность организации: Учебное пособие / О.А. Грунин, С.О. Грунин. СПб.: Питер, 2002. 160 с.
14. Егорова Е.Е. Еще раз о сущности риска в системном подходе ... / Е.Е. Егорова // Управление риском. 2002. № 2. С.9-12.
15. Енгалычев О.В. Риск ... на завтра: предпосылки и этапы развития риск-менеджмента / О.В. Енгалычев // Российское предпринимательство. 2004. № 6. С. 44-47; № 7 С. 51-54.
16. Ишутин Р.В. Еще раз о предпринимательстве / Р.В. Ишутин // Управление риском. 2002. № 3. С. 10-12.
17. Казанцев А.К. Менеджмент в предпринимательстве: Учебное пособие / А.К. Казанцев, А.А. Крупанин. М.: ИНФРА-М, 2003. 230 с.
18. Коломина М.Е. Инвестиционные риски / М.Е. Коломина. М., 1993. 160 с.
19. Курчеева Г.И. Информационное обеспечение управления риском / Г.И. Курчеева, В.А. Хворостав // Управление риском. 2003. № 4. С. 15-22.
20. Лавров А.С Риски высокотехнологичных предприятий при трансформации отношений собственности / А.С. Лавров // Управление риском. 2004. № 3. С. 21-24.
21. Лисицына Е.В. Технология риск-менеджмента / Е.В. Лисицына, Г.С. Токаренко // Управление риском. 2004. № 1.с.11-14.
22. Манахова И. Риски потребителя / И. Манахова // Управление риском. 2004. № 1. С. 43-50.

23. Минат В.Н. Финансовая среда предпринимательства и предпринимательские риски. Учебное пособие/"Экзамен"/2006

24. Минат В. Н. Корпоративные конфликты как форма проявления взаимоотношений между участниками корпоративного управления в России / В.Н. Минат // Проблемы корпоративного права и управления в современной России. Рязань: РФ МАЭП, 2003. С. 15-17.

25. Минат В.Н. Развитие фирмы и управление рисками / В.Н. Минат // Современные проблемы гуманитарных и естественных наук: Сборник научных трудов. Рязань: РИУП, 2004. С.55-60.

26. Миронов М.Г. Финансовый менеджмент: Учебное пособие / М.Г. Миронов, Е.А. Замедлина, Е.В. Жарикова. М.: Экзамен, 2004. 224 с.

27. Моделирование рисковых ситуаций в бизнесе / Под ред. Б.А. Лагоши. М.: Фис, 2001. 224 с.

28. Мур А.И. Руководство по безопасности бизнеса: Практическое пособие по управлению рисками: Пер. с англ. / А.И. Мур. М.: Филинч, 1998. 376 с.

29. Ожегов С.и. Словарь русского языка / С.И.Ожегов.М.:Русский язык,1978.900 с.

30. Основы предпринимательской деятельности. Финансовый менеджмент / Под ред. В.М. Власовой. М.: ФиС, 2000. 180 с.

31. Полоюва А,Н Угрозы, риски и неопределенности в бизнес-деятельности сложных организационных систем / А.Н. Полозова // Управление риском. 2004. № 1. С. 59-64.

32. Ревинский И.А. Предпринимательство: Учебное пособие / И.А. Ревинский. Новосибирск: НГПУ, 1996. 91 с.

33. Рэдхэд К. Управление финансовыми рисками / К. Рэдхэд. М.: Перспектива, 1996.646 с.

34. Смит А. Исследование о природе и причинах богатства народов / А. Смит. М.: Наука, 1992. 572 с.

35. Сычев А.Ю. История управления рисками / А.Ю. Сычев // Управление риском. 2003. № 4. С. 2-14.

36. Тэпман Л.Н. Риски в экономике: Учебное пособие / Л.Н. Тэпман / Под ред. В.А. Швандара. М.: ЮНИТИ-ДАНА, 2002.382 с.

37. Усов В.Н. Предупреждение неопределенности в управлении риском / В.Н. Усов // Управление риском. 2003. № 4. С.23-26.

38. Фадеев С. Не рисковать многим ради малого / С. Фадеев // РИСК. 2003. № 1. с. 59-64.

39. Финансовый менеджмент: теория и практика: Учебник / Под ред. Е.С. Стояновой. М.: Перспектива, 2002. 656 с.

40. Финансовый менеджмент: Учебное пособие / Под ред.Е.И. Шохина. М.: ИД ФБК·ПРЕСС, 2002. 408 с.

41. Черкасова В. Идентификация рисков / В. Черкасова // РИСК, 2004. № 2. С. 31-34.

42. Чупров С.В. Риск и управление устойчивостью промышленного предприятия / С.В. Чупров // Управление риском. 2004. № 2. С. 20-24.

43. Шинкаренко И.Э. Риск-менеджмент - философия управления рисками корпораций / И.Э. Шинкаренко, В.В. Храмов // Управление риском. 2004. № 2. С. 56-60.

44. Шутов П.В. Модель риска предпринимателя / П.В. Шутов // Управление риском. 2004. № 3. С. 56-61.

ЗАЩИТА КОММЕРЧЕСКОЙ ТАЙНЫ

(курс лекций)

А.Н. Кришталюк
(аспирант ФГБОУ ВПО «Госуниверситет – УНПК»)

СОДЕРЖАНИЕ

Введение

В русском языке общепринято, что слово «конфиденциальный» означает «не подлежащий оглашению, секретный».

Конфиденциальное делопроизводство распространяется на документы, которые содержат в себе сведения, составляющие коммерческую и служебную тайну. Коммерческая тайна прямо связана с коммерческой деятельностью, является необходимым условием ее существования.

Синонимом коммерческой деятельности является предпринимательская деятельность. Согласно Гражданскому кодексу Российской Федерации, предпринимательская деятельность – это «самостоятельная, осуществляемая на свой риск деятельность, направленная на систематическое получение прибыли от пользования имуществом, продажи товаров, выполнения работ или оказания услуг лицами, зарегистрированными в этом качестве в установленном порядке». Следовательно, коммерческими предприятиями являются те, для которых извлечение прибыли является основной целью деятельности. Ими могут быть как частные, так и государственные, а также муниципальные предприятия.

Предпринимательскую деятельность могут осуществлять и не-коммерческие предприятия, т.е. такие, которые в качестве основной цели имеют не извлечение прибыли, а достижение общественных благ: социальных, культурных, образовательных, здравоохранительных, благотворительных и др. Однако такие предприятия могут осуществлять предпринимательскую деятельность лишь постольку, поскольку это служит достижению целей, ради которых они созданы, и соответствующую этим целям. Отличительным признаком коммерческой деятельности является соизмерение затрат и результатов работы, получение максимальной прибыли.

Еще одной отличительной особенностью коммерческой деятельности является то, что она, как правило, осуществляется в

условиях конкуренции, соперничества, борьбы предприятий за получение выгод, преимуществ по сравнению с предприятиями аналогичного профиля.

Коммерческая деятельность может осуществляться и при отсутствии конкурентов, при монопольном положении предприятия в той или другой сфере деятельности, однако это, скорее, исключение, чем правило. Правилом же является то, что конкурентная борьба – спутник коммерческой деятельности и условие выживания коммерческих предприятий. Отсюда – стремление сохранить в секрете от конкурентов (соперников) те приемы и особенности своей деятельности, которые обеспечивают преимущество над ними, отсюда и стремление конкурентов выявить эти секреты, чтобы использовать их в своих интересах.

Получение, использование, разглашение таких секретов без согласия их владельцев отнесены законодательством к одной из форм недобросовестной конкуренции, называемой промышленным шпионажем. Защищаемые секреты коммерческой деятельности получили название коммерческой тайны.

Информация, составляющая коммерческую тайну, – научно-техническая, технологическая, коммерческая, организационная или иная используемая в экономической деятельности информация, в том числе ноу-хау, которая обладает действительной или потенциальной коммерческой ценностью в силу ее неизвестности третьим лицам, которые могли бы получить выгоду от ее разглашения или использования, к которой нет свободного доступа на законном основании и по отношению к которой принимаются адекватные ее ценности правовые, организационные, технические или иные меры охраны.

В свою очередь служебная тайна – это вид тайны, включающий полученную федеральными и муниципальными органами власти информацию, составляющую коммерческую тайну других субъектов, а также устанавливаемую и защищаемую органами власти и предприятиями собственную информацию, доступ к которой ограничивается служебной необходимостью.

Таким образом, коротко можно охарактеризовать коммерческую тайну как совокупность не являющихся государственной тайной сведений, представляющих действительную или потенциальную ценность для субъекта предпринимательства, разглашение которых может нанести ему ущерб и, в отношении которых приняты надлежащие меры по сохранению конфиденциальности.

Как видно из вышеуказанного определения одним из основных признаков сведений, составляющих коммерческую

тайну, является то, что в отношении этих сведений приняты меры по обеспечению конфиденциальности. Только при соблюдении этих условий может наступить предусмотренная законодательством дисциплинарная, материальная, административная и уголовная ответственность.

Исходя из этого положения, даже если сведения связаны с производством, технологией, управлением, финансовой и другой деятельностью вашего предприятия и их разглашение может нанести вам ущерб, но в отношении них вы не предприняли меры по сохранению тайны, то вы не можете рассчитывать на их правовую защиту. И, таким образом, лица, незаконно завладевшие вашей коммерческой тайной, не будут нести никакой юридической ответственности. И это, в принципе, справедливо, почему государство должно защищать ваши тайны, если вы сами не предпринимаете никаких мер по их защите? Вот почему необходимо на каждом предприятии с самого начала его деятельности разработать систему по обеспечению сохранности коммерческой тайны.

Организация и технология конфиденциального делопроизводства не регламентированы государственными нормативными актами. Их должен определять обладатель конфиденциальных документов, учитывая специфику деятельности предприятия. Однако при этом ему необходимую руководствоваться определенными нормами и правилами работы с конфиденциальными документами, обеспечивающими нужный уровень функционирования предприятия, сохранность документов и конфиденциальность содержащейся в них информации.

Нужно помнить, что чем быстрее эти меры будут разработаны, тем быстрее сведения, составляющие коммерческую тайну вашего предприятия, подпадут под правовую защиту. Этим вы обезопасите себя от недобросовестной конкуренции со стороны ваших конкурентов.

Лекция 1. Сущность, задачи и особенности конфиденциального делопроизводства и защиты коммерческой тайны

По уровню доступности документы подразделяются на две категории:

- общедоступные;
- с ограниченным доступом.

Общедоступными являются открытые документы. К документам с ограниченным доступом относятся документы, работа с которыми может производиться по специальному разрешению уполномоченных на то лиц. Документирование открытой информации и организация работы с открытыми документами входят в сферу действия открытого делопроизводства. Документы с ограниченным доступом относятся к сфере деятельности не одного, а нескольких типов делопроизводства, в зависимости от того, к какому виду тайны относится содержащаяся в документах информация. Нормативными документами установлено *шесть видов тайны*:

- государственная;
- коммерческая;
- служебная;
- личная;
- семейная;
- профессиональная.

Документы, содержащие государственную тайну, относятся к сфере секретного делопроизводства. Документы, содержащие личную и различные подвиды профессиональной тайны, являются предметом соответствующих типов специального делопроизводства.

Конфиденциальное делопроизводство, как уже было отмечено, распространяется на документы, содержащие коммерческую и служебную тайну. При этом к документам, составляющим служебную тайну, отнесены только документы с грифом «Для служебного пользования», т.к. документы, содержащие коммерческую тайну других субъектов, должны обрабатываться и защищаться в режиме коммерческой тайны. Объединение конфиденциальных документов, содержащих коммерческую и служебную тайну, одним делопроизводством обусловлено тем, что эти документы почти полностью идентичны по технологическим процедурам составления, обработки, обращения, хранения и защиты.

Доступ к коммерческой тайне имеют работники, круг которых определен субъектом предпринимательства. Государственные контролирующие и правоохранительные органы в соответствии с полномочиями, предоставленными им законодательством по контролю и надзору, имеют право, в пределах своей компетенции, на основании письменного заявления знакомиться со сведениями, являющимися коммерческой тайной и составлять соответствующие акты изъятия документов, свидетельствующих о нарушении законодательства. При этом должностные лица этих

органов несут предусмотренную законодательством ответственность за разглашение сведений, составляющих коммерческую тайну хозяйствующего субъекта.

Важным моментом является то, что иные органы и организации, в том числе средства массовой информации, правом истребования у хозяйствующего субъекта сведений, составляющих коммерческую тайну, не обладают.

Итак, какого рода сведения составляют коммерческую тайну? Вот лишь примерный список тех, которые содержат такие сведения:

-Производство;
-Управление;
-Планы;
-Финансы;
-Рынок;
-Партнеры;
-Переговоры;
-Контракты;
-Цены;
-Торги, аукционы;
-Наука и техника;
-Технология;
-Совещание;
-Безопасность.

Каждая из этих тем, в зависимости от специфики конкретного предприятия, может содержать различную информацию. В каждом случае эти сведения определяются индивидуально.

Важно, при определении объектов, которые составляют вашу коммерческую тайну, не включить в их список объектов, которые не могут составлять коммерческую тайну в соответствии с законодательством.

К *объектам коммерческой тайны* не могут относиться:

-учредительные документы, а также документы, дающие право на занятие предпринимательской деятельностью и отдельными видами хозяйственной деятельности, подлежащей лицензированию;

-сведения по утвержденным формам статистической отчетности, а также отчетности о финансово-экономической деятельности и иные данные, необходимые для проверки правильности исчисления и уплаты налогов и других обязательных платежей;

-документы об уплате налогов и других обязательных платежей;

-документы, удостоверяющие платежеспособность;

-сведения о численности, составе работающих, их заработной плате и условиях труда, а также о наличии свободных рабочих мест;

-сведения о загрязнении окружающей среды, нарушении антимонопольного законодательства, несоблюдении правил охраны труда, реализации продукции, причиняющей вред здоровью потребителей, а также о других нарушениях законодательства и размерах причиненного при этом ущерба.

Конфиденциальное делопроизводство следует определять как деятельность, обеспечивающую документирование конфиденциальной информации, организацию работы с конфиденциальными документами и защиту содержащейся в них информации. При этом под документированием информации понимается процесс подготовки и изготовления документов, под организацией работы с документами – их учет, размножение, прохождение, исполнение, отправление, классификация, систематизация, подготовка для архивного хранения, уничтожение, режим хранения и обращения, проверки наличия.

По сфере деятельности открытое делопроизводство распространяется на управленческие действия и включает в основном управленческие документы. Конфиденциальное делопроизводство в силу условий работы с конфиденциальными документами распространяется как на управленческую, так и на различные виды производственной деятельности, включает не только управленческие, но и научно-технические документы (научно-исследовательские, проектные, конструкторские, технологические и др.). Кроме того, конфиденциальное делопроизводство распространяется не только на официальные документы, но и на их проекты, различные рабочие записи, не имеющие всех необходимых реквизитов, но содержащие информацию, подлежащую защите.

По видам работ конфиденциальное делопроизводство отличается от открытого, с одной стороны, большим их количеством, с другой – содержанием и технологией выполнения многих видов.

Помимо этого, третья составляющая конфиденциального делопроизводства – защита содержащейся в конфиденциальных документах информации - вообще не предусмотрена в определении открытого делопроизводства, хотя определяемая собственником часть открытой информации должна защищаться от утраты. Конфиденциальная информация должна защищаться и от утраты, и от утечки.

Термин «утечка конфиденциальной информации», вероятно, не самый благозвучный, однако он более емко, чем другие термины, отражает суть явления, к тому же он давно уже закрепился в научной литературе и нормативных документах. Утечка конфиденциальной информации представляет собой неправомерный, т.е. неразрешенный выход такой информации за пределы защищаемой зоны ее функционирования или установленного круга лиц, имеющих право работать с ней, если этот выход привел к получению информации (ознакомлению с ней) лицами, не имеющими к ней санкционированного доступа, независимо от того, работают или не работают такие лица на данном предприятии обусловлены уязвимостью информации.

Уязвимость информации следует понимать как ее доступность для дестабилизирующих воздействий, т.е. таких воздействий, которые нарушают установленный статус информации. Нарушение статуса любой документированной информации включается в нарушении ее физической сохранности (вообще либо у данного собственника в полном или частичном объеме), логической структуры и содержания, доступности для правомочных пользователей. Нарушение статуса конфиденциальной документированной информации дополнительно включает нарушение ее конфиденциальности (закрытости для посторонних лиц).

Уязвимость документированной информации – понятие собирательное. Она не существует вообще, а проявляется в различных формах. К таким формам, выражающим результаты дестабилизирующего воздействия на информацию, относятся (в скобках указаны существующие варианты названий форм):

-хищение носителя информации или отображенной в нем информации (кража);

-потеря носителя информации (утеря);

-несанкционированное уничтожение носителя информации или отображенной в нем информации (разрушение);

-искажение информации (несанкционированное изменение, несанкционированная модификация, подделка, фальсификация);

-блокирование информации;

-разглашение информации (распространение, раскрытие).

Термин «разрушение» употребляется главным образом применительно к информации на машинных носителях.

Существующие варианты названий: модификация, подделка, фальсификация – не совсем адекватны термину «искажение», они имеют нюансы, однако суть их одна и та же –

несанкционированное частичное и полное изменение состава первоначальной информации.

Блокирование информации в данном контексте означает блокирование доступа к ней правомочных пользователей, а не злоумышленников.

Разглашение информации является формой проявления уязвимости только конфиденциальной информации.

Та или иная форма уязвимости документированной информации может реализоваться в результате преднамеренного или случайного дестабилизирующего воздействия различными способами на носитель информации или на саму информацию со стороны источников воздействий. Такими источниками могут быть люди, технические средства обработки передачи информации, средства связи, стихийные бедствия и др. Способами дестабилизирующего воздействия на информацию являются копирование (фотографирование), записывание, передача, съем, заражение программ обработки информации вирусом, нарушение технологии обработки и хранения информации, вывод (или выход) из строя и нарушение режима работы технических средств обработки и передачи информации, физическое воздействие на информацию и др.

Реализация форм проявления уязвимости документированной информации приводит или может привести к двум видам уязвимости:

-утрате информации;

-утечке информации.

К утрате документированной информации приводят хищение и потеря носителей информации, несанкционированное уничтожение носителей информации или только отображенной в них информации, искажение и блокирование информации. Утрата может быть полной или частичной, безвозвратной или временной (при блокировании информации), но в любом случае она наносит ущерб собственнику информации.

К утечке конфиденциальной документированной информации приводит ее разглашение. В литературе и даже в нормативных документах термин «утечка конфиденциальной информации» нередко заменяется или отождествляется с терминами; «разглашение конфиденциальной информации», «распространение конфиденциальной информации». Такой подход не является правомерным.

Разглашение или распространение конфиденциальной информации означают несанкционированное доведение ее до потребителей, не имеющих права доступа к ней. При этом такое

доведение должно осуществляться кем-то, исходить от кого-то. Утечка происходит при разглашении (несанкционированном распространении) конфиденциальной информации, но не сводится только к нему. Утечка может произойти и в результате потери носителя конфиденциальной документированной информации, а также хищения носителя информации либо отображенной в нем информации при сохранности носителя у его собственника (владельца). «Может произойти» не означает, что произойдет. Потерянный носитель может попасть в чужие руки, а может быть и «прихвачен» мусороуборочной машиной и уничтожен в установленном для мусора порядке. В последнем случае утечки конфиденциальной информации не происходит.

Хищение конфиденциальной документированной информации также не всегда связано с получением ее лицами, не имеющими к ней доступа. Имелось немало случаев, когда хищение носителей конфиденциальной информации осуществлялось у коллег по работе допущенными к этой информации лицами с целью «подсидки», причинения вреда коллеге. Такие носители, как правило, уничтожались лицами, похитившими их.

Но в любом случае потеря и хищение конфиденциальной информации если и не приводят к ее утечке, то всегда создают угрозу утечки. Поэтому можно сказать, что к утечке конфиденциальной информации приводит ее разглашение, и могут привести хищение и потеря. Сложность состоит в том, что зачастую невозможно определить, во-первых, сам факт разглашения или хищения конфиденциальности информации при сохранности носителя информации у ее собственника (владельца), во-вторых, попала ли информация вследствие ее хищения или потери посторонним лицам.

Суммируя соотношение форм и видов уязвимости защищаемой информации, можно констатировать:

1. Формы проявления уязвимости информации выражают результаты дестабилизирующего, воздействия на информацию, а виды уязвимости -конечный суммарный итог реализации форм проявления уязвимости.

2. Утрата информации включает в себя, по сравнению с утечкой, большее число форм проявления уязвимости информации, но она не поглощает утечку, т.к. не все формы проявления уязвимости информации, которые приводят или могут привести к утечке, совпадают с формами, приводящими к утрате.

3. Наиболее опасными формами проявления уязвимости конфиденциальной документированной информации являются потеря, хищение и разглашение – первые две одновременно могут

привести и к утрате, и к утечке информации, вторая (хищение информации при сохранности носителя) и третья могут не обнаружиться, со всеми вытекающими из этого последствиями.

4. Неправомерно отождествлять, как это нередко делается в научной литературе и нормативных документах, включая законы, виды и отдельные формы проявления уязвимости информации (утрата = потеря, утрата = хищение, утечка = разглашение (распространение)), а также формы проявления уязвимости информации и способы дестабилизирующего воздействия на нее.

5. Необходимо уделять одинаковое внимание предотвращению как утраты защищаемой документированной информации, так и ее утечки, т.к. ущерб собственнику информации наносится в любом случае.

Защита конфиденциальной документированной информации от утраты и утечки осуществляется в определенной мере в рамках и первой, второй составляющих конфиденциального делопроизводства, т.к. она взаимоувязана, «переплетена» с ними: документирование конфиденциальной информации и организация работы с конфиденциальными документами должны производиться в условиях обеспечения их защиты, и вместе с тем многие вопросы защиты решаются в ходе и путем осуществления систематических операций по учету и обработке документов. Однако защитные мероприятия охватывают не только сами документы, но и другие объекты, так или иначе связанные с защищаемыми документами (помещения, технические средства обработки и передачи информации и др.)

Поэтому в определении конфиденциального делопроизводства защита документированной информации выделена в самостоятельную составляющую.

Конфиденциальное делопроизводство шире открытого и по своим задачам. Если задачей открытого делопроизводства является документационное обеспечение управленческой деятельности, то конфиденциальное делопроизводство должно осуществлять решение двух задач:

1) документационное обеспечение всех видов конфиденциальной деятельности;

2) защита документированной информации, образующейся в процессе конфиденциальной деятельности.

Первая задача имеет своей целью организацию и бесперебойное функционирование конфиденциальной деятельности в сфере любого вида производства и управления. Это требует от делопроизводства обеспечения нужд конфиденциальной деятельности полной, своевременной и

достоверной документной информацией, организации исполнения и использования документов.

Полноту документной информации характеризует ее объем, который, с одной стороны, должен быть достаточным для принятия управленческих решений и выполнения производственных заданий, с другой стороны, являться действительно необходимым, не содержащим избыточной, не нужной для деятельности предприятия информации.

Достоверность документной информации заключается, во-первых, в ее соответствии объективному состоянию того или другого вопроса и, во-вторых, в ее юридической силе, характеризующейся наличием и правильностью оформления соответствующих реквизитов.

Своевременность документной информации означает, что за время обработки и передачи информации не изменилось состояние вопроса, к которому она относится.

Организация исполнения документов включает в себя и оперативное доведение их до исполнителей, и обеспечение своевременного и качественного решения содержащихся в документах вопросов.

Организация использования документов состоит в обеспечении как текущего, оперативного, так и последующего, ретроспективного использования документной информации.

Вторая задача имеет своей целью обеспечение сохранности и конфиденциальности документированной информации, что требует создания и поддержания специальных условий хранения, обработки и обращения документов, гарантирующих надежную защиту, как самих документов, так и содержащейся в них информации. Сущность конфиденциального делопроизводства обусловливает его организационные и технологические особенности, к числу основных из которых относятся:

-письменное нормативное закрепление общей технологии документирования, организации работы с документами и их защиты;

-жесткое регламентирование состава издаваемых документов и содержащейся в них информации, в том числе на стадии подготовки черновиков и проектов документов;

-обязательный поэкземплярный и полистный учет всех, без исключения, документов, проектов и черновиков;

-максимально необходимая полнота регистрационных данных о каждом документе;

-фиксация прохождения и местонахождения каждого документа;

-проведение систематических проверок наличия документов;

-разрешительная система доступа к документам и делам, обеспечивающая правомерное и санкционированное ознакомление с ними;

-жесткие требования к условиям хранения документов и обращения с ними, которые должны обеспечивать сохранность и конфиденциальность документированной информации;

-регламентация обязанностей лиц, допущенных к работе с конфиденциальной документированной информацией, к ее защите;

-персональная и обязательная ответственность за учет, сохранность документов и порядок обращения с ними.

Особенностью конфиденциального делопроизводства является и своеобразное переплетение некоторых функций, которые на первый взгляд как бы взаимоисключают друг друга. В частности, функциями по реализации задачи документационного обеспечения конфиденциальной деятельности являются создание документов, необходимых и достаточных для такой деятельности, предоставление каждому пользователю всех документов, требующихся для выполнения должностных обязанностей, параллельными им функциями по реализации задачи защиты конфиденциальной информации – предотвращение необоснованного издания и рассылки документов, исключение необоснованного ознакомления с документами.

На самом деле применительно к документированию это означает, что конфиденциальная деятельность должна обеспечиваться минимальным количеством документов при сохранении полноты и достоверности информации, применительно к организации документооборота – предоставление пользователям всех необходимых документов, но только тех, которые действительно требуются для выполнения должностных обязанностей.

Особенности конфиденциального делопроизводства одновременно выступают и в качестве требований к нему.

Лекция 2. Меры по обеспечению защиты коммерческой тайны

Меры по обеспечению защиты коммерческой тайны условно можно классифицировать на внутренние и внешние, которые в свою очередь делятся на правовые, организационные, технические и психологические. Некоторые источники выделяют

еще одну – страховую, т.е. страхование коммерческой тайны от ее разглашения. Однако в наших условиях такой метод защиты представляется нам малореальным. Кроме того, очень тяжело определить реальную стоимость принадлежащей предприятию коммерческой тайны. Меры по обеспечению защиты коммерческой тайны предприятия показаны на рисунке 1.

Рис. 1

Действие внутренних мер по обеспечению конфиденциальности в основном направлено на рабочий персонал вашего предприятия. Работники хозяйствующего субъекта, имеющие доступ к сведениям, составляющим коммерческую тайну, обязуются:

-сохранять коммерческую тайну, которая станет им известна по работе, и не разглашать ее без разрешения, выданного в установленном порядке, при условии, что сведения, составляющие коммерческую тайну, не были известны им ранее либо не были получены ими от третьего лица без обязательства соблюдать в отношении их конфиденциальность;

-выполнять требования инструкций, положений, приказов по обеспечению сохранности коммерческой тайны;

-в случае попытки посторонних лиц получить от них сведения, составляющие коммерческую тайну, немедленно сообщить об этом соответствующему должностному лицу или в соответствующее подразделение хозяйствующего субъекта;

-сохранять коммерческую тайну хозяйствующих субъектов, с которыми имеются деловые отношения;

-не использовать знание коммерческой тайны для занятий деятельностью, которая в качестве конкурентного действия может нанести ущерб хозяйствующему субъекту;

-в случае увольнения передать все носители информации, составляющие коммерческую тайну (рукописи, черновики, документы, чертежи, диски, «флешки», дискеты, распечатки на принтерах, кино-, фотопленки, модели, материалы и др.), которые находились в их распоряжении, соответствующему должностному лицу или в соответствующее подразделение хозяйствующего субъекта.

Данные обязательства даются в письменной форме при заключении трудового или иного договора либо в процессе его исполнения.

Внешние меры по обеспечению конфиденциальности коммерческой тайны необходимы при осуществлении вами торгово-экономических, научно-технических, валютно-финансовых и других деловых связей, в том числе с иностранными партнерами. Для этого договаривающиеся стороны специально оговаривают характер, состав сведений, составляющих коммерческую тайну, а так же взаимные обязательства по обеспечению её сохранности в соответствии с законодательством. Однако нужно помнить, что при заключении договора с иностранными партнерами условия конфиденциальности деятельности должны соответствовать законодательству страны, где заключается договор, если иное не предусмотрено межгосударственными соглашениями. В данном случае применяется принцип, сформулированный еще в римском праве – «locus regit actum».

Locus regit actum (место руководит актом) – начало частного международного права, в силу которого внешние формы и обряды совершения актов (договоров, завещаний, браков) определяются законами факультативно того места, где они совершены.

Правовые меры обеспечения сохранности коммерческой тайны являются первоочередными, т.к. они призваны обеспечить эффективное функционирование остальных мер обеспечения конфиденциальности информации. С этой точки зрения правовые меры являются первичными по отношению к остальным мерам.

Первым шагом по реализации правовых мер является принятие на предприятии Положения (Инструкции) по обеспечению сохранности коммерческой тайны, в которых определяются:

-состав и объем сведений, составляющих коммерческую тайну;

-порядок присвоения грифа «Секрет предприятия» сведениям, работам и изделиям и его снятия;

-процедура допуска работников хозяйствующего субъекта, а также лиц, привлекаемых к его деятельности, к сведениям, составляющим коммерческую тайну;

-порядок использования, учета, хранения и маркировки документов и иных носителей информации, изделий, сведения о которых составляют коммерческую тайну;

-организация контроля за порядком использования сведений, составляющих коммерческую тайну;

-процедура принятия взаимных обязательств хозяйствующими субъектами по сохранению коммерческой тайны при заключении договоров о проведении каких-либо совместных действий;

-порядок применения предусмотренных законодательством мер дисциплинарного и материального воздействия на работников, разгласивших коммерческую тайну;

-возложение ответственности за обеспечение сохранности коммерческой тайны на должностное лицо хозяйствующего субъекта.

После принятия Положения можно приступать к разработке организационных мер обеспечения конфиденциальности вашей коммерческой тайны.

Одним из наиболее важнейших вопросов, требующих разрешения является вопрос, кто будет осуществлять все перечисленные меры по защите. Естественно, исполнение этих обязанностей должно быть поручено специалистам, обладающим необходимыми теоретическими и практическими знаниями. Не рекомендуется использование для этих целей услуг частных охранных и детективных агентств, так как: во-первых, перед ними стоят несколько иные задачи (физическая охрана и техническая безопасность объекта), а, во-вторых, вряд ли здравомыслящий бизнесмен разрешит доступ к своей коммерческой тайне посторонним лицам, пусть даже представляющим охранное агентство.

Для обеспечения защиты коммерческой тайны на крупных хозяйствующих объектах могут создаваться специальные

режимно-секретные подразделения, функции, полномочия которых отражаются в соответствующих инструкциях, положениях, приказах.

Такие подразделения должны быть созданы не только на крупных объектах, но и на всех остальных, занимающихся коммерческой деятельностью. На любом предприятии имеются сведения, подлежащие защите, разница только в объеме мер защиты. Если на крупных хозяйствующих объектах, таких как банки, финансовые корпорации, заводы, специализированное подразделение представлено в виде разветвленной, отлично материально и технически оснащенной структуры, в которой может работать несколько десятков сотрудников, то на средних и малых предприятиях такое подразделение может быть представлено в виде нескольких ответственных сотрудников. В крайнем случае, если предприятие не может себе позволить содержать таких сотрудников в своем штате, то следует прибегнуть к услугам консультантов по вопросам безопасности и защиты информации. Они помогут разработать необходимую систему защиты, а также решить возникающие в ходе практической деятельности вопросы.

Лекция 3. Организация конфиденциального делопроизводства

Организация конфиденциального делопроизводства означает создание необходимых условий для изготовления и получения конфиденциальных документов, организации работы с ними и предотвращения утраты и утечки документированной конфиденциальной информации.

Организация конфиденциального делопроизводства включает создание подразделения, обеспечивающего изготовление, учет, хранение, обработку и использование конфиденциальных документов, установление его статуса, структуры, численного и должностного состава, разработку положения о подразделении и должностных инструкций сотрудников, выделение для подразделения служебного помещения, обеспечение необходимых условий труда, разработку или приобретение нормативных документов и методической литературы по организации и ведению конфиденциального делопроизводства, создание постоянно действующей экспертной комиссии, оформление допуска сотрудников к коммерческой и служебной тайне и

обучение их правилам работы с конфиденциальными документами.

Конфиденциальное делопроизводство в силу небольшого по сравнению с открытым делопроизводством объема документов и в целях обеспечения условий для сохранности и конфиденциальности документов должно быть централизованным, т.е. сосредоточенным в едином подразделении предприятия. Подразделение конфиденциального делопроизводства может быть самостоятельным структурным подразделением предприятия, подчиненным непосредственно руководителю предприятия, или входить в состав других подразделений, как правило, осуществляющих защиту конфиденциальной информации: службу безопасности, службу защиты информации и др. В «Положении о порядке обращения со служебной информацией ограниченного распространения» сказано: «Прием и учет (регистрация) документов, содержащих служебную информацию ограниченного распространения, осуществляются, как правило, структурными подразделениями, которым поручен прием и учет несекретной документации», однако это целесообразно лишь при незначительном объеме таких документов и при отсутствии документов, содержащих коммерческую тайну.

Наименование подразделения конфиденциального делопроизводства, статус и при необходимости структуру определяет руководитель предприятия, исходя из объема конфиденциального делопроизводства и общей структуры предприятия.

Подразделение конфиденциального делопроизводства является составной частью системы защиты коммерческой и служебной тайны, органом, осуществляющим, координирующим и контролирующим работу с конфиденциальными документами. Оно должно рассматриваться как структурное подразделение, непосредственно участвующее в основной деятельности предприятия. Численный состав сотрудников подразделения конфиденциального делопроизводства должен определяться объемом выполняемой работы с учетом норм времени на ее выполнение.

Должностной состав сотрудников подразделения конфиденциального делопроизводства должен определяться характером и сложностью выполняемой работы. Для более многообразной и более сложной работы следует устанавливать и более высокие должности.

При незначительном объеме конфиденциального делопроизводства специальное подразделение конфиденциального делопроизводства может не создаваться. В этом случае издание, обработка и хранение конфиденциальных документов возлагается на специально назначенных приказом руководителя предприятия нескольких либо одного сотрудников других подразделений, как правило, службы безопасности или, как было сказано, службы открытого делопроизводства, если документы содержат сведения, составляющие только служебную тайну. На этих лиц распространяются все задачи, функции, права и ответственность, возлагаемые на подразделение конфиденциального делопроизводства.

Если ведение конфиденциального делопроизводства возложено на одного сотрудника, то для выполнения отдельных делопроизводственных операций, в которых требуется участие двух лиц (проверки наличия, уничтожение документов), необходимо привлекать (лучше на постоянной основе) второго сотрудника данного или другого подразделения, имеющего доступ к этим документам. Такое привлечение оформляется приказом по предприятию. Следует подчеркнуть, что в целях более надежного обеспечения сохранности и конфиденциальности документов на подразделение конфиденциального делопроизводства или на специально выделенных для ведения конфиденциального делопроизводства сотрудников должны быть возложены все операции по печатанию, учету, размножению, хранению, передаче, отправлению, систематизации, проверке наличия и уничтожению конфиденциальных документов. Функции исполнителей и пользователей конфиденциальных документов в сфере изготовления и обработки документов ограничиваются подготовкой документов и их исполнением. Допустимо и печатание документов исполнителями, если оно осуществляется в специально предназначенном для этого помещении подразделения конфиденциального делопроизводства.

Основные задачи и функции подразделения конфиденциального делопроизводства, а также права и ответственность его руководителя должны быть закреплены в положении о подразделении, а обязанности, права, ответственность сотрудников подразделения конфиденциального делопроизводства или специально назначенных для ведения конфиденциального делопроизводства лиц - в должностных инструкциях, разрабатываемых на конкретные должности. В должностных инструкциях устанавливаются и квалификационные требования к сотрудникам - образование и стаж работы на

аналогичной должности. Положение о подразделении конфиденциального делопроизводства и должностные инструкции сотрудников являются организационно-правовыми документами, регламентирующими статус подразделения в целом и каждого из его сотрудников.

При определении задач и функций подразделения конфиденциального делопроизводства необходимо исходить из того, что оно должно не только организовывать и осуществлять документационное обеспечение конфиденциальной управленческой и производственной деятельности предприятия, но и участвовать во всех мероприятиях по предотвращению утраты конфиденциальных документов и утечки содержащейся в них информации. Это участие не ограничивается разработкой и осуществлением соответствующих мероприятий только в рамках подразделения конфиденциального делопроизводства. Утрата и утечка конфиденциальной информации в большинстве случаев происходят по вине исполнителей и пользователей конфиденциальных документов, нарушающих по разным причинам правила обращения с такими документами. Поэтому значительная часть функций подразделения конфиденциального делопроизводства связана с обучением исполнителей и пользователей прав работы с конфиденциальными документами и осуществлением контроля за их выполнением. Этим обусловлены и соответствующие права подразделения конфиденциального делопроизводства, в том числе такие, участие в подборе кадров для работы с конфиденциальной информацией, внесение предложений об отстранении от конфиденциальных работ, поощрении и привлечении к ответственности исполнителей и пользователей конфиденциальных документов, участие в проведении расследований по фактам утраты и утечки конфиденциальной информации.

При разработке должностных инструкций следует учитывать, во-первых, необходимость специализации сотрудников по отдельным видам работ, что ускоряет их выполнение и повышает качество, и, во-вторых, нормативы времени на работы с тем, чтобы все сотрудники были загружены равномерно в соответствии с должностью, и не было перезагруженности, которая отрицательно сказывается на качестве работы. При установлении квалификационных требований к должностям необходимо иметь в виду сложность выполнения некоторых видов работ, требующих специальной подготовки. На соответствующие таким работам должности следует назначать специалистов с высшим образованием в области защиты информации. В

соответствии с законодательством сотрудники подразделения конфиденциального делопроизводства несут дисциплинарную, административную либо гражданско-правовую ответственность за утрату конфиденциальных документов или разглашение содержащейся в них информации, поэтому в должностных инструкциях должна быть установлена персональная ответственность сотрудников за сохранность конфиденциальных документов и содержащейся в них информации. В случаях особой конфиденциальности документов назначение сотрудников на соответствующие должности в подразделение конфиденциального делопроизводства целесообразно осуществлять после проведения в отношении их полномочными органами проверочных мероприятий при письменном согласии на это сотрудников.

Все сотрудники, принимаемые на работу в подразделение конфиденциального делопроизводства, а также при отсутствии подразделения, специально назначенные для ведения конфиденциального делопроизводства лица должны дать письменное обязательство по соблюдению режима конфиденциальности. Это обязательство фиксируется в трудовом договоре (контракте) или специальном соглашении. Сотрудники могут допускаться к работе только после изучения в части, их касающейся, требований действующих на предприятии нормативно-методических документов по вопросам организации и ведения конфиденциального делопроизводства, обеспечения режима конфиденциальности проводимых работ и проверки знаний этих требований соответствующим руководителем.

Подразделение конфиденциального делопроизводства должно быть обеспечено служебным помещением (при необходимости - несколькими помещениями) для хранения конфиденциальных документов и работы сотрудников подразделения, а также помещением для исполнителей, если работа с конфиденциальными документами не разрешена в служебных комнатах исполнителей.

Важной составной частью организации конфиденциального делопроизводства является создание постоянно действующей экспертной комиссии (ПДЭК). Задачами такой комиссии должны быть:

-разработка перечней сведений, составляющих коммерческую и служебную тайну;

-разработка перечней издаваемых предприятием конфиденциальных документов;

-снижение или снятие степени конфиденциальности сведений и грифа конфиденциальности документов;

-разработка Положения о системе доступа к конфиденциальным документам;

-экспертиза ценности конфиденциальных документов с целью установления сроков их хранения и отбора документов на основе этих сроков для архивного хранения и уничтожения;

-проведение аналитической работы по предотвращению утечки и утраты конфиденциальной информации.

Учитывая важность задач ПДЭК, в ее состав следует включать высококвалифицированных сотрудников, в первую очередь руководителей подразделений, имеющих доступ к конфиденциальной информации. Кроме того, в состав комиссии должны входить руководитель службы безопасности предприятия и руководитель подразделения конфиденциального делопроизводства, а также руководитель архива предприятия (при наличии архива). Председателем комиссии необходимо назначать одного из заместителей руководителя предприятия, допущенного ко всем конфиденциальным документам. ПДЭК создается приказом руководителя предприятия и должна работать на постоянной основе с заменой в необходимых случаях отдельных ее членов. Задачи, функции и порядок работы комиссии определяются положением о ней. На ПДЭК может быть возложено и проведение экспертизы ценности открытых документов с тем, чтобы она могла оценивать значение документов, образующихся в деятельности предприятия, в их совокупности и таким образом более правильно определять сроки их хранения. Сотрудники, работающие с конфиденциальными документами, должны иметь допуск к соответствующим видам тайны.

Допуск сотрудников предприятия к коммерческой и служебной тайне осуществляется с их согласия и предусматривает:

-принятие сотрудниками обязательств по соблюдению установленного на предприятии режима соответствующего вида тайны, которые закрепляются в трудовом договоре (контракте) или специальном соглашении;

-ознакомление сотрудников с положениями законодательства, предусматривающими ответственность за нарушение конфиденциальности;

-ознакомление сотрудников с перечнями сведений, составляющих коммерческую и служебную тайну предприятия, и к которым сотрудники имеют право доступа.

Порядок изготовления конфиденциальных документов, режим обращения с ними требуют определенных знаний, которые должны быть приобретены до начала работы с документами и постоянно пополняться. С этой целью необходимо организовывать

различные формы обучения сотрудников: техническую учебу, семинары, самостоятельную подготовку со сдачей зачетов и др.

Лекция 4. Определение состава конфиденциальных документов

Одной из особенностей конфиденциального делопроизводства является жесткое регламентирование состава издаваемых документов. Обусловлено это тем, что документ является потенциально существующим источником утечки содержащейся в нем информации, т.е. попадания ее в руки тех, кому она не предназначена. Поэтому конфиденциальные документы должны издаваться только при действительной необходимости в письменном удостоверении наличия и содержания управленческих, производственных и иных действий. При этом решение задач конфиденциальной деятельности должно обеспечиваться минимальным количеством документов при сохранении полноты необходимой информации.

Но установление состава издаваемых конфиденциальных документов направлено не только на предотвращение необоснованного их издания и на исключение избыточной конфиденциальной информации, но определение количества их экземпляров, адресатов, которым они должны направляться, т.к. не вызванная действительной необходимостью рассылка конфиденциальных документов также приводит к утечке информации. На стадии определения состава издаваемых документов решается вопрос и о придании им необходимой юридической силы путем установления должностных лиц, которые должны визировать, подписывать и утверждать тот или другой документ. В конечном итоге регламентация состава издаваемых конфиденциальных документов преследует цель не только исключения необоснованного, но и неконтролируемого их издания. Состав документированной конфиденциальной информации зависит от компетенции и функции предприятия, характера его деятельности, взаимосвязей с другими предприятиями, порядка разрешения вопросов. Такой состав закрепляется перечнями издаваемых предприятием конфиденциальных документов, раздельно по документам, отнесенных к коммерческой тайне, и документам, отнесенным к служебной тайне. Но эти перечни должны разрабатываться на основе и в рамках перечней сведений, составляющих коммерческую и служебную тайну. Вызвано это тем, что по

существующим нормам сначала определяются сведения, составляющие тот или другой вид тайны. Эти сведения могут быть зафиксированы как в документах, так и в других носителях: памяти человека, базе данных ЭВМ, выпускаемой продукции, технологических процессах, физических полях и др. Поэтому только после определения состава всех конфиденциальных сведений можно установить те из них, которые должны документироваться. Таким образом, определение состава издаваемых конфиденциальных документов должно начинаться с разработки перечней сведений, составляющих коммерческую и служебную тайну. Перечень сведений, составляющих коммерческую тайну, разрабатывается для каждого предприятия самим предприятием – обладателем информации. Это вытекает из действующего законодательства, которым установлено, что состав и объем таких сведений определяется собственником информации. Таким образом, право предпринимателя на состав коммерческой тайны является безусловным. Никто не может диктовать ему, какие сведения относить к коммерческой тайне, за исключением сведений, которые не могут составлять коммерческую тайну согласно государственным нормативным актам.

Следовательно, состав сведений, относимых к коммерческой тайне, должен устанавливаться и изменяться индивидуально, на уровне их обладателя. В этой связи следует обратить внимание на имеющиеся в научной литературе попытки разработки неких типовых перечней сведений, составляющих коммерческую тайну любой коммерческой структуры независимо от сферы и специфики ее деятельности. Такие попытки не могут иметь успех, поскольку состав конфиденциальной информации в коммерческой сфере определяется исходя из специфики деятельности данного конкретного предприятия: типа предприятия, характера его деятельности, технологии изготовления продукции, объема и себестоимости продукции, состава и количества поставщиков сырья, условий рынка сбыта, направленности интересов конкурентов и т.д. То, что для одних предприятий является коммерческой тайной, для других может не быть таковой и даже использоваться в рекламных целях. В целом тенденция развития коммерческой тайны направлена на сохранение значения производственной тайны, связанной с новизной и совершенствованием технологических процессов, т.е. с элементами творческой деятельности, и на падение значения тайны финансово-торговой, связанной не с элементами новизны, а с элементами индивидуальности и большей или меньшей

степенью исключительности. Правовым основанием для установления состава сведений, относимых к коммерческой тайне, являются действующие законы, а также определение понятия «коммерческая тайна», которыми предусмотрено, что сведения, составляющие коммерческую тайну, могут быть в любой сфере предпринимательской деятельности, следовательно, коммерческая тайна может распространяться на все направления и вид деятельности предприятия. Разработкой перечня сведений, составляющих коммерческую тайну должна заниматься ПДЭК.

На первом этапе работы на основе анализа задач, функций, компетенции, направлений деятельности предприятия необходимо установить вес состав циркулирующей на предприятии информации, отображенной любом носителе, любым способом и в любом виде, а также с учетом перспектив развития предприятия и его взаимоотношений с партнерами определить характер дополнительной информации, которая может возникнуть в результате деятельности предприятия. Эта информация классифицируется по тематическому признаку. На втором этапе определяется, какая из установленной информации должна быть конфиденциальной и отнесена к коммерческой тайне. Базовым критерием при этом является возможность получения преимуществ от использования информации за счет неизвестности ее третьим лицам. Этот критерий имеет как бы две составляющие: неизвестности информации третьим лицам и получение преимуществ в силу этой неизвестности. Данные составляющие взаимосвязаны и взаимообусловлены, поскольку, с одной стороны, неизвестность информации третьим лицам сама по себе ничего не значит, если не обеспечивает преимуществ с другой - преимущества можно получить только за счет такой неизвестности. Конфиденциальность является правовой формой и одновременно инструментом обеспечения неизвестности информации.

Преимущества от использования информации, не известной третьим лицам, могут состоять в получении выгоды или предотвращении ущерба иметь, в зависимости от областей и видов деятельности, экономические, моральные и другие характеристики, выражаться количественными и качественными показателями. В сфере коммерческой деятельности ценность информации обусловлена прежде всего рыночной потребностью в информации как источнике получения прибыли, поэтому отнесение информации к коммерческой тайне позволяет получить прибыль и предотвратить убытки. Конфиденциальность такой информации создает для ее обладателя преимущества в

конкурентной борьбе и выступает как средство защиты от не добросовестной конкуренции. Названный критерий является объективным показателем возможности отнесения информации к коммерческой тайне, мерилом придания информации статуса конфиденциальной. Это означает, что при отсутствии данного критерия нет оснований для перевода информации в категорию конфиденциальной. Но это не означает, что при его наличии информация во всех случаях может и должна быть отнесена к коммерческой тайне. Законодательством введены два ограничения на отнесение информации к коммерческой тайне. Первое ограничение состоит в том, что к коммерческой тайне не может быть отнесена информация, составляющая государственную тайну. Второе ограничение заключается в том, что к коммерческой тайне нельзя относить информацию, которая должна быть общедоступной в целях предупреждения сокрытия правонарушений и предотвращения нанесения ущерба законным интересам государства, физических или юридических лиц. Перечни такой информации содержатся в нескольких нормативных актах: законах «Об информации, информатизации и защите информации» (см. приложение 2), «О благотворительной деятельности и благотворительных организациях», постановлении Правительства РСФСР от 5 декабря 1991 г. «О перечне сведений, которые не могут составлять коммерческую тайну» (см. приложение 3) и др. Эти перечни в значительной мере дублируют друг друга и имеют различную правовую основу. В проекте Закона «О коммерческой тайне» имеется специальная статья 3 «Информация, которая не может составлять коммерческую тайну». В этой статье обобщены и дополнены сведения, содержащиеся в ранее изданных нормативных актах.

Запрещение относить к коммерческой тайне ту или иную информацию не означает, что всю ее может получить по требованию любое юридическое или физическое лицо. Часть ее, затрагивающая законные интересы этих лиц, безусловно, должна им предоставляться, а часть предоставляется лишь соответствующим органам власти, наделенным законодательством правом контроля такой информации. Должно быть и третье ограничение, которое хотя и не предусмотрено законодательством, но диктуется здравым смыслом. Оно состоит в том, что при переводе информации в разряд коммерческой тайны необходимо учитывать сопутствующие этому затраты на ее защиту. Если эти затраты превышают достигаемые в результате защиты количественные и качественные показатели, то придание информации статуса конфиденциальной теряет всякий смысл.

Следует иметь в виду, что в перечень сведений, составляющих коммерческую тайну, может включаться не только информация, создаваемая данным предприятием, но и информация, полученная им без использования неправомерных средств при проведении исследований по собственной инициативе, систематических наблюдений и сбора сведений. Такая информация считается полученной правомерно и самостоятельно независимо от того, что ее содержание может совпадать с содержанием коммерческой тайны другого юридического или физического лица. Кроме того, правомерно полученной считается конфиденциальная информация, полученная от ее обладателя на основании договора или в результате правопреемства. Предприятие, правомерно и самостоятельно получившее информацию, одновременно являющуюся коммерческой тайной другого юридического или физического лица, становится обладателем этой коммерческой тайны со всеми предусмотренными законодательством правами.

После установления состава конфиденциальной информации определяется степень ее конфиденциальности. Степень конфиденциальности - это показатель уровня закрытости информации. Уровень закрытости зависит от величины ущерба, который может наступить при утечка информации. Чем больше этот ущерб, тем выше должна быть и степень конфиденциальности. В практике работы предприятий применяются от одной до нескольких степеней конфиденциальности информации с различными их наименованиями. Наиболее распространенным является деление информации на две степени: конфиденциально и строго конфиденциально. Однако проектом Закона «О коммерческой тайне» установлена одна степень конфиденциальности с названием «Коммерческая тайна», свидетельствующая лишь о принадлежности информации к коммерческой тайне. Правда, в проекте Закона это названо не степенью, а грифом коммерческой тайны, но суть дела от этого не меняется, поскольку, по определению, гриф конфиденциальности - это реквизит, свидетельствующий о степени конфиденциальности сведений, содержащихся в их носителе, проставляемый на самом носителе и (или) в сопроводительной документации на него. Наименование грифа должно соответствовать наименованию степени конфиденциальности. Установление одной степени (одного грифа) конфиденциальности информации, составляющей коммерческую тайну, обусловлено, вероятно, тем, что степень конфиденциальности определяется собственниками информации,

которые могут иметь (а зачастую так и бывает) разные подходы к степени конфиденциальности однотипной по содержательной чести информации. В этом случае при рассмотрении в судебном порядке дел о неправомерном получении коммерческой тайны сложно определить, кто из собственников установил правильную степень конфиденциальности информации, т.к. критерии отнесения информации к той или другой степени конфиденциальности выбирает ее собственник. В то же время сведение информации, требующей разного уровня закрытости, к одной степени конфиденциальности не позволяет выделить наиболее значимую информацию с целью установления для нее более жесткого, по сравнению с менее значимой, режима защиты. Но закон есть закон, и если в окончательном варианте Закона «О коммерческой тайне» сохранится одна степень конфиденциальности, выход может быть в разделении информации по степеням конфиденциальности на внутреннюю и отправляемую. Информация, не подлежащая отправлению на другие предприятия, может иметь несколько степеней и наименований конфиденциальности, а отправляемая - одну степень «Коммерческая тайна». При использовании на предприятии одной степени конфиденциальности этот этап работы ПДЭК выпадает. Следующий этап - определение конкретных сроков конфиденциальности информации либо обстоятельств и событий, при наступлении которых конфиденциальность снимается. Продолжительность конфиденциальности информации должна соответствовать срокам действия условий, необходимых и достаточных для признания данной информации конфиденциальной в соответствии с законодательством. Результаты работы оформляются перечнем сведений, составляющих коммерческую тайну, который может иметь форму, приведенную в таблице 1.

Таблица 1

Пример формы перечня сведений, составляющих коммерческую тайну

№ п/п	Наименование сведений	Степень конфиденциальности	Срок конфеденциальности
1	2	3	4

Если сведениями установлена одна степень конфиденциальности, то графа 3 опускается. При значительном объеме конфиденциальных сведений они классифицируются в перечне по разделам, соответствующим сферам деятельности

предприятия. Перечень подписывается председателем и всеми членами ПДЭК, утверждается и вводится в действие приказом руководителя предприятия. В приказе должны быть определены мероприятия по обеспечению функционирования перечня и контролю его выполнения. С приказом и перечнем необходимо ознакомить под расписку всех сотрудников пред, приятия, работающих с конфиденциальной информацией. Копии перечня или выписки из него должны быть направлены конфидентам (владельцам) данной коммерческой тайны. Ими являются физические или юридические лица, которым в силу служебного положения, договора либо на ином законном основании известна коммерческая тайна ее обладателя. Дополнения и изменения состава включенных в перечень сведений а также изменение степени их конфиденциальности могут осуществляться с разрешения руководителя предприятия и вноситься в перечень за подписями руководителя подразделения по принадлежности сведений и руководителя службы безопасности. При существенном изменении состава сведений перечень должен составляться заново. Об изменениях в составе коммерческой тайны обладатель информации обязан в письменной форме известить конфидентов данной информации. Что касается состава информации, являющейся служебной тайной, то следует иметь в виду, что такая информация предусмотрена для органов государственной и муниципальной власти и подведомственных им предприятий, в коммерческих структурах она используется главным образом лишь при переписке с органами власти. В «Положении о порядке обращения со служебной информацией ограниченного распространения» сказано, что руководитель федерального органа исполнительной власти в пределах своей компетенции определяет категории должностных лиц, уполномоченных относить служебную информацию к разряду ограниченного распространения, а эти лица несут персональную ответственность за обоснованность такого отнесения. Как видно из этой нормы, она не содержит технологии определения состава информации, относимой к служебной тайне.

На практике, которая существует уже несколько десятилетий, используются обычно два варианта определения состава такой информации. В первом варианте министерства и ведомства разрабатывают единые для отрасли перечни сведений ограниченного распространения и направляют их на подведомственные предприятия. Во втором варианте полномочия по разработке перечней передаются руководителям подведомственных предприятий, и перечни разрабатываются

применительно к каждому конкретному предприятию. Иногда используется и третий, комбинированный вариант, при котором перечни разрабатывают и министерства (ведомства), и на основе этих перечней - подведомственные предприятия. Технология разработки перечней сведений ограниченного распространения практически не отличается от технологии разработки перечней сведений, составляющих коммерческую тайну. Служебная тайна может быть в любой области деятельности органа власти или предприятия, однако в упомянутом Положении определен состав сведений, которые не могут быть отнесены к служебной информация ограниченного распространения. Сведениям, составляющим служебную тайну, установлена одна степень конфиденциальности: «Для служебного пользования». Перечень таких сведений имеет форму перечня сведений, составляющих коммерческую тайну, без графы 3. Перечни сведений, составляющих коммерческую и служебную тайну, раскрывают тематическое содержание включенных в них сведений. Но эти сведения, как уже отмечалось, фиксируются в различном виде на различных носителях и могут быть как документированными, так и недокументированными. В сферу конфиденциального делопроизводства входит только документированная информация (документы), поэтому из всей совокупности информации, включенной в перечни сведений, отнесенных к коммерческой и служебной тайне, нужно выделить состав документируемой информации и установить виды документов, в которых она должна быть зафиксирована. Определение состава конфиденциальных документов должно осуществляться также ПДЭК. При этом следует руководствоваться определенными критериями документирования информации. К ним относятся:

- необходимость документированной информации для правового обеспечения деятельности предприятия, регламентирующего статус предприятия, права, обязанности и ответственность его сотрудников;
- необходимость документированной информации для производственной деятельности: научно-исследовательской, конструкторской, проектной, технологической и др.;
- необходимость документированной информации для управленческой деятельности;
- необходимость документированной информации как доказательного источника на случаи возникновения конфликтных ситуаций;
- необходимость передачи информации в официальном виде;

• важность информации как исторического источника, раскрывающего направления и особенности деятельности предприятия.

В рамках критериев документирования определение состава документируемой информации должно увязываться с решением конкретных задач. В зависимости от назначения документируемой информации определяются конкретные виды документов, в которых эта информация должна быть зафиксирована. В процессе определения необходимых конфиденциальных документов следует проводить работу по сокращению их количества за счет разработки интегральных документов, в которые можно включить показатели нескольких документов, в том числе путем замены разовых первичных документов накопительными. Однако объединение документов ИВ осуществляться с таким расчетом, чтобы в итоге не создавалась возможность необоснованного ознакомления со всем документом лиц имеющих доступ только к части содержания (показателей) документа. Виды конфиденциальных документов необходимо устанавливать с учетом оптимального объема содержащейся в них информации, исключающего избыточную, в том числе дублетную информацию, поскольку избыточная информация - это конфиденциальные данные, утечка которых может нанести ущерб предприятию. После установления состава документов определяются круг лиц, имеющих право составлять, визировать и подписывать (утверждать) тот или другой вид документа, а также предприятия, которым данный документ должен направляться. Перечни издаваемых конфиденциальных документов составляются раздельно по каждому виду тайны и могут иметь следующую форму (таблица 2):

Таблица 2

Пример формы перечня издаваемых конфиденциальных документов

№ п/п	Наименование документов	Гриф конфиденциальности	Срок конфиденциальности	ФИО лиц, имеющих право составлять документы	ФИО лиц, визирующих документы	ФИО лиц, имеющих право подписывать и утверждать документы	Количество изготовляемых экземпляров документов	Куда направляется документ	Примечания
1	2	3	4	5	6	7	8	9	10

Грифы и сроки конфиденциальности документов должны соответствовать степеням и срокам конфиденциальности включаемых в документы сведений, определенным перечнями

сведений, составляющих коммерческую и служебную тайну. При установлении таким сведениям одной степени конфиденциальности графа «Гриф конфиденциальности» опускается. Если документ подлежит утверждению, то в графе 7 сначала проставляются инициалы и фамилия лица (лиц), подписывающего документ, затем после слова «утв.» - инициалы и фамилия лица, утверждающего документ. При значительном количестве утверждаемых документов Графа 7 может быть разделена на две графы: «Инициалы и фамилии лиц, имеющих право подписывать документы» и «Инициалы и фамилии лиц имеющих право утверждать документы». К числу документов, подлежащих утверждению в соответствии с существующими нормативными актами, относятся: уставы, положения о представительствах, филиалах и структурных подразделениях предприятия, структура, штатное расписание, должностные инструкции, акты проверок (ревизий), сметы, расценки на проведение работ и оказание услуг и некоторые другие. Если при направлении документов другим предприятиям каждый адресат не должен знать, кому еще направлен данный документ, то в графе 9 по соответствующему виду документа после внесения адресатов делается пометка «раздельное адресование», означающая, что на каждом экземпляре документа должен проставляться лишь адресат, которому направляется данный экземпляр. Графу 10 следует использовать (при необходимости) для указания периодичности составления документов, а также для пометки о проставлении оттиска печати на соответствующих документах. Перечни издаваемых документов подписываются председателем и всеми членами ПДЭК и утверждаются руководителем предприятия. С перечнями под расписку должны быть ознакомлены все лица, наделенные правом составлять, визировать, подписывать и утверждать соответствующие документы. Внесение возможных последующих частичных уточнений или изменений в перечни может быть возложено на руководителя службы безопасности.

При изменении перечней сведений, составляющих коммерческую и служебную тайну, соответствующие изменения вносятся и в перечни издаваемых конфиденциальных документов. О снятии грифа конфиденциальности с отправленных документов должны быть письменно оповещены предприятия-адресаты. В случаях возникновения необходимости издания разовых документов, не включенных в перечни, или дополнительных экземпляров документов, не предусмотренных перечнями, их изготовление может производиться по совместному разрешению

руководителей соответствующего подразделения и службы безопасности (или подразделения конфиденциального делопроизводства). Одновременно определяется целесообразность включения таких документов (дополнительных экземпляров) в соответствующий перечень.

Лекция 5. Понятия и принципы организации конфиденциального документооборота

В открытом делопроизводстве документооборот предприятия определяется как движение документов с момента их создания или получения до завершения исполнения или отправки. В соответствии с этим определением движение поступивших документов начинается с момента их получения, однако до регистрации документы проходят стадии предварительного рассмотрения, распределения, определения состава документов, не подлежащих регистрации, доклада документов руководству, передачи части из них в структурные подразделения. В конфиденциальном делопроизводстве предварительное рассмотрение, передача по назначению и другие работы с поступившими документами осуществляются тоже с момента их получения, но до начала движения они должны быть учтены. Следовательно, движение поступивших конфиденциальных документов начинается после того, как они учтены. Изданные на предприятии открытые документы включаются в документооборот с момента их создания. Документ считается созданным только тогда, когда он подписан (утвержден). После подписания производится регистрация и начинается движение документа. Поэтому фактически документ включается в документооборот с момента его регистрации. В конфиденциальном делопроизводстве изданные документы включаются в документооборот тоже с момента их учета. Но учет документов осуществляется не после подписания, а на стадии подготовки их проектов. С момента учета до подписания документы находятся в движении (прием-передача между исполнителями и подразделением конфиденциального делопроизводства, визирование), то есть они уже включены в Документооборот. Поэтому применительно к конфиденциальным документам неправомерно говорить, что они включаются в документооборот с момента их создания. Движение документов выделенного хранения также начинается после их учета. В

приведенном определении открытого документооборота движение документов завершается окончанием исполнения или отправкой.

В конфиденциальном делопроизводстве движение поступивших и изданных документов завершается их отправлением, подшивкой в дело или переводом на учет документов выделенного хранения. Движение документов выделенного хранения заканчивается их отправлением, уничтожением или передачей на архивное хранение. С учетом всего сказанного, можно дать определение конфиденциального документооборота как движение конфиденциальных документов, момента их учета до отправления, подшивки в дело или перевода на учет выделенного хранения поступивших и изданных документов и до отправления, уничтожения или передачи на архивное хранение документов выделенного хранения. Целью и открытого, и конфиденциального документооборота является обеспечение исполнения и использования документов. В процессе движения документов нужно создавать условия для сохранности документов, ибо их утрата исключает возможность исполнения и использования. Вместе с тем важной отличительной чертой и особенностью конфиденциального документооборота является необходимость защиты документов от несанкционированного доступа к ним с целью предотвращения утечки конфиденциальной информации. Поэтому организация конфиденциального документооборота должна строиться на основе следующих принципов:

- разрешительной системы доступа к конфиденциальным документам;
- исключения несанкционированного доступа к конфиденциальным документам;
- целенаправленного регулирования процессов движения конфиденциальных документов;
- исключения инстанций прохождения конфиденциальных документов и действий с ними, не обусловленных характером и порядком исполнения документов;
- фиксированной передачи конфиденциальных документов;
- обеспечения своевременного и качественного исполнения конфиденциальных документов;
- персональной и обязательной ответственности за выдачу неправомерных разрешений на ознакомление с конфиденциальными документами и на их отправление.

Система доступа к конфиденциальным документам.

Конфиденциальные документы являются документами ограниченного доступа. Это означает, что знакомиться и работать с ними могут только лица получившие на то соответствующие разрешения. Порядок получения и оформления таких разрешений устанавливается на каждом предприятии системой доступа к конфиденциальным документам, которая представляет собой совокупность норм и правил, определяющих, кто из руководителей предприятия и структурных подразделений, кому из пользователей и с какими категориями конфиденциальных документов может давать разрешение на ознакомление, а также, каким образом оформляются такие разрешения в зависимости от вида учета документов.

При разработке системы доступа к конфиденциальным документам необходимо руководствоваться следующими подходами.

1. Доступ к конфиденциальным документам может предоставляться только лицам, имеющим оформленный в установленном порядке (контрактом, приказом) допуск к соответствующему виду тайны и давшим письменное обязательство (в контракте или специальной подписке) о неразглашении ставших им известными конфиденциальных сведений. Допуск к соответствующему виду тайны является основанием для доступа к конкретным документам в пределах этого вида тайны.

2. Доступ к конфиденциальным документам должен быть обоснованным и правомерным, т.е. базироваться на служебной необходимости ознакомления с конкретным документом именно данного лица.

3. Система доступа должна давать возможность обеспечивать пользователей всеми необходимыми им в силу служебных обязанностей конфиденциальными документами, но только теми, которые действительно необходимы для выполнения конкретных видов работ. К сожалению, этот подход не всегда четко соблюдается. С одной стороны, стремясь максимально сократить количество лиц, допускаемых к конфиденциальным документам, на некоторых предприятиях не знакомят часть пользователей с необходимой им для служебной деятельности информацией и тем самым снижают качество этой деятельности, с другой стороны - знакомят пользователей с конфиденциальными документами, не связанными напрямую с их функциональными обязанностями, но, как выражаются, необходимыми им «для общего развития» или «расширения кругозора», что приводит к разглашению

информации, т.е. неправомерному доведению информации до лиц, которые не должны ее знать.

4. Доступ к конфиденциальным документам должен быть санкционированным, т.е. осуществляться только по соответствующему разрешению.

5. Доступ к конфиденциальным документам могут предоставлять только уполномоченные на то должностные лица, при этом соответствующее должностное лицо может давать разрешение на ознакомление с входящими в сферу его деятельности конфиденциальными документами, только установленному кругу лиц и только по служебной необходимости.

6. Доступ должен оформляться письменно по каждому конкретному конфиденциальному документу. При необходимости ознакомления пользователя только с частью документа в разрешении на ознакомление должны быть указаны разделы, пункты или страницы, с которыми можно знакомить пользователя. Составители (исполнители) документов и лица, которые визировали, согласовывали, подписывали, утверждали документы, а также лица, указанные в тексте распорядительных документов, допускаются к таким документам без оформления дополнительных разрешений, если они продолжают выполнять те же функциональные обязанности. В первом случае э то обусловлено тем, что перечисленные лица как бы автоматически в силу своего служебного положения уже получили доступ к документам на стадии их подготовки, во втором - тем, что с поручением, содержащимся в распорядительном документе, исполнитель должен быть ознакомлен обязательно, чтобы знать, что ему поручено, поэтому оформление дополнительного доступа теряет всякий смысл.

Поскольку система доступа к конфиденциальным документам содержит в себе значительное количество правовых положений, а нарушение ее требований, приводящее, как правило, к разглашению конфиденциальной информации, влечет за собой дисциплинарную, гражданско-правовую и в некоторых случаях уголовную ответственность виновных лиц, то ее следует закреплять в специальном нормативном документе, который обычно называется «Положение о системе доступа к конфиденциальным документам».

Положение должно основываться на вышеизложенных подходах и может включать в себя следующие разделы.

1. Общие положения.

2. Полномочия должностных лиц по разрешению доступа к конфиденциальным документам.

3. Порядок оформления разрешений на доступ к конфиденциальным документам.

В первом разделе указываются: назначение Положения; нормативные документы, на которых оно базируется; сфера его распространения; основные задачи и принципы системы доступа; на кого возлагается ответственность за невыполнение требований Положения; кем осуществляется контроль над соблюдением норм Положения. При этом следует отразить, что ответственность за невыполнение требований Положения несут все должностные лица, имеющие право давать разрешение на доступ к конфиденциальным документам, а также все пользователи конфиденциальных документов. Контроль над выполнением норм Положения должен возлагаться на руководителей службы безопасности, подразделения конфиденциального делопроизводства и управленческо-производственных подразделений в пределах их компетенции.

Во втором разделе должны быть перечислены все должностные лица, которые могут давать разрешение на доступ к конфиденциальным документам, с указанием, какой категории пользователей и к какому составу документов. Основополагающими подходами при этом должны быть следующие:

- руководитель предприятия имеет право давать разрешение на доступ к соответствующим конфиденциальным документам всем категориям пользователей;
- заместители руководителя предприятия по отдельным направлениям имеют право давать разрешение на доступ к соответствующим конфиденциальным документам всем пользователям, но в пределах своей сферы деятельности;
- руководителям подразделений дается право разрешать доступ к конфиденциальным документам всем сотрудникам своих подразделений по тематике работы подразделений; для осуществления доступа к конфиденциальным документам данного подразделения сотрудников других подразделений необходимо разрешение соответствующего заместителя руководителя предприятия или руководителя предприятия;
- первые заместители руководителей, а также должностные лица, временно исполняющие ту или иную должность, могут, как правило, разрешать доступ к конфиденциальным документам в объеме всех прав, предусмотренных для замещаемых ими лиц.

В третьем разделе определяется порядок оформления разрешений на доступ к конфиденциальным документам, зарегистрированным по различным видам учета. Разрешение на

ознакомление с конфиденциальными документами должно оформляться: по поступившим и изданным документам в форме резолюции на документе; по документам, зарегистрированным по учету документов выделенного хранения, в форме резолюции на документе или подписанного соответствующим руководителем списка пользователей на внутренней стороне обложки документа, титульном листе либо в карточке учета выдачи документа. Разрешение на доступ к конфиденциальным делам оформляется в номенклатуре дел.

Отдельным разделом Положения может быть предусмотрен порядок доступа к конфиденциальным документам лиц, не работающих на данном предприятии (при выполнении совместных работ и др.). При этом следует иметь в виду, что сотрудники органов государственной власти, иных государственных органов и органов местного самоуправления имеют право на доступ к конфиденциальной информации в пределах компетенции, определенной для этих органов законодательством Российской Федерации, поэтому предприятия обязаны не только знакомить сотрудников таких органов с конфиденциальными документами, но и предоставлять документы в распоряжение органов в случаях, установленных законодательством. В соответствии с законодательством названные органы обязаны обеспечить защиту полученных ими документов от разглашения и неправомерного использования должностными лицами и иными служащими этих органов, которые ознакомились с документами в связи с выполнением служебных обязанностей. За разглашение или неправомерное использование содержащейся в документах конфиденциальной информации данные органы несут предусмотренную законодательством ответственность.

Положение может разрабатываться подразделением конфиденциального делопроизводства или ПДЭК. Оно подписывается разработчиками, визируется всеми лицами, имеющими право давать разрешение на доступ к конфиденциальным документам, и утверждается приказом руководителя предприятия. В приказе определяются и мероприятия по введению Положения в действие (порядок изучения Положения пользователями, технология осуществления контроля над его выполнением и др.). С утвержденным Положением должны быть ознакомлены под расписку все сотрудники предприятия, работающие с конфиденциальными документами.

Лекция 6. Патентование бизнес-методов

Коммерческая тайна в современных условиях рыночной экономики является главным сокровищем любой компании. От расхищения информации огромные убытки несут предприятия не только в России, но и во всем мире. Работа с информацией, которая содержит коммерческую тайну, - одна из обязанностей большинства менеджеров. О том, как защитить коммерческую тайну компании, какие правовые нормы существуют для этого в России, что именно должен знать менеджер, чтобы защитить те идеи, которые родились в компании, - это те вопросы, которые рассматриваются в данном пособии.

Яркие идеи являются основой эффективных рационализаторских предложений, изобретений, открытий. Менеджеры компаний должны знать основы правового регулирования этого процесса, подводные камни, которые могут встретиться им на пути в связи с обеспечением охраны и защиты рожденных идей. В "чистом виде" идея не является предметом правовой охраны. Рассмотрим более подробно, как же закон может охранять идеи?

В соответствии с п. 4 ст. 6 Закона "Об авторском праве" оно не распространяет свое действие на идеи, методы, процессы, системы, способы, открытия, факты.

Некоторые из перечисленных результатов интеллектуальной деятельности охраняются, например, патентным правом. Возможные способы охраны иных достижений являются предметом обсуждения ученых и специалистов практиков.Но авторское право не охраняет идеи, принципы, факты и подобные им результаты интеллектуальной деятельности. Наряду с подобными объектами существуют произведения, обладающие всеми необходимыми для охраны признаками, но не охраняемые авторским правом в силу прямого указания закона.

Во-первых, это произведения, срок охраны которых истек, но истечение срока охраны на которые не влияет на охрану авторства, имени автора и неприкосновенности произведения.

Во-вторых, в сферу правовой охраны не включены государственные символы и знаки, а также официальные документы, их официальные переводы. К числу государственных символов и знаков относятся флаги, гербы, гимны, ордена, денежные знаки и т. п. К официальным документам относятся законы и другие акты нормативного характера - уставы юридических лиц, стандарты, инструкции, правила, судебные

решения и другие акты правовых органов, а также иные официальные документы, исходящие от организаций и должностных лиц.

В-третьих, в число охраняемых авторским правом объектов не включены произведения народного творчества, поскольку их автор не может быть установлен, так как им является народ.

В-четвертых, не охраняются авторским правом сообщения о событиях, фактах, имеющие информационный характер, кроме тех случаев, когда такое сообщение сопровождается оценкой значимости происшедшего, авторским комментарием, мнением эксперта, прогнозом дальнейшего развития событий, анализом или иным "расцвечиванием", интерпретацией происшедших событий.

Наряду с объектами авторского права, идеи воплощаются в иных объектах, являющихся предметами промышленной собственности и регулируемых патентным правом. В частности, охраняются идеи, воплощенные в изобретениях. Напомним, что п. 1. ст. 4 Патентного закона РФ предъявляет к изобретениям следующие требования: новизна, изобретательский уровень и промышленная применимость.

Таким образом, изобретение в течение многих лет в нашей стране рассматривалось как техническое решение задачи. Поэтому организационные, организационно-технические и организационно-управленческие либо экономические новации изобретениями не признавались. Соответственно этим воззрениям формировались правовые нормы.

Современный Патентный закон, как и ранее действовавшее законодательство, хотя и не применяет сам термин "техническое решение задачи", но конкретные требования такого характера, критерии, предъявляемые к изобретению, в нем сохранены. В частности, Патентный закон прямо указывает на возможные объекты изобретений, лишь расширяя их состав за счет штаммов микроорганизмов, культур клеток растений и животных.

Что относит Патентный закон к объектам изобретений? Это - устройства, способы, вещества, а также предложения по применению уже известных устройств, способов и веществ по новому назначению. Российский Патентный закон не признает изобретениями, в силу их не технического характера: научные теории и математические методы; методы организации и управления хозяйством; условные обозначения, расписания, правила; методы выполнения умственных операций; алгоритмы и программы для вычислительных машин; проекты и схемы планировки сооружений, зданий, территорий; решения,

касающиеся только внешнего вида изделий, направленные на удовлетворение эстетических потребностей; топологии интегральных микросхем; сорта растений и породы животных и др.

Большинство названных достижений охраняются правом, но не как изобретения, а в качестве иных объектов интеллектуальной собственности, подпадая под действие либо норм авторского права (например, программы для вычислительных машин, проекты зданий и сооружений), либо норм иных правовых институтов (например, топологии интегральных микросхем, новые сорта растений и порода животных).

Не охраняемая правовой нормой идея может быть безнаказанно "позаимствована". Поэтому именно на данной стадии важна не правовая охрана и защита, которые, как мы отметили, невозможны, но возможно и необходимо соблюдение конфиденциальности. Такая мера получила мировое распространение в процессе заключения различных договоров, где на стадии преддоговорной процедуры сторона, владеющая идеей, ноу-хау, вынуждена раскрывать эти секреты другой стороне, чтобы разъяснить их механизм действия и преимущества. Это имеет место при заключении договора коммерческой концессии, франчайзинга. Еще до заключения договора либо при его заключении франчайзи уплачивает франчайзеру сумму, называемую "паушальным взносом", за сам факт раскрытия информации.

Отдельные идеи очень сложно внедрить кому-либо другому, кроме автора. Как говорит Герберт Кэссон, автор книги "Аксиомы бизнеса", если собрать 50 человек и подробно рассказать им о том, как в Африке охотиться на львов, то после этого там охотников на львов не прибавится.

Одним из перспективных направлений менеджмента - **патентование идей**, легализованных в форме бизнес-методов. В последние годы в связи с тем, что идеи, знания становятся главным оружием в конкурентной борьбе, все активнее предпринимаются попытки запатентовать не только технические решения, но и бизнес-методы, сугубо управленческие, интеллектуальные находки менеджеров. В отдельных странах такая практика уже сложилась и продолжает успешно развиваться. В настоящее время в чистом виде методы ведения бизнеса патентуются уже в США, Японии и некоторых других странах. В США и Японии в последние годы зарегистрированы патенты на разнообразные методы ведения бизнеса,

всевозможные организационные и управленческие приемы. Зарегистрировано несколько подобных изобретений и в России.

Некоторые из изобретений регистрируются для того, чтобы, получив патент, предъявить претензии к крупным компаниям, применяющим в своей деятельности похожие бизнес-схемы, бизнес-методы, но не успевших их запатентовать.

Известно, что по действующему законодательству, если патент выдан, например, в Японии, то его действие распространяется исключительно только на ее территории. Если же японский патент не имеет патента-аналога в России, то ничто не мешает российским предпринимателям производить товар или оказывать услуги, сходные с описанными в таком зарубежном патенте. Но собственный патент российские предприниматели получить вряд ли смогут, поскольку у их изобретения будет отсутствовать один из основных обязательных признаков - признак новизны.

На сегодняшний день в российской правовой доктрине нет однозначного ответа на вопрос, можно или нельзя охранять как патент разнообразные методы ведения бизнеса и всевозможные организационные приемы. Существуют мнения как допускающие возможность охраны, так и полностью ее отрицающие. И это естественно, поскольку любое новое, непривычное явление вначале подвергается жесткому противодействию. Требуется, как мы уже подчеркивали, время, чтобы это новое пробило себе дорогу.

В США, где действует прецедентное право, сложился такой подход: суды толкуют нормы существующего патентного законодательства в пользу возможности патентования организационных приемов и методов ведения бизнеса. В настоящее время зарегистрированные в США "business method patents" составляют уже значительную долю в общем объеме патентов. И этот процесс нарастает.

В США можно получить патент, например, на разработку программы тренинга по повышению личной эффективности. В частности, в конце 1980-х гг. в США был разработан один из таких тренингов под названием Forum. Сегодня в США существуют две американские компании, владеющие соответствующими правами: Landmark Education, организующая обучение личного развития, и Tekniko, реализующая лицензии на право работать бизнес-консультантами и на использование технологии Forum в процессе консультирования. Цена каждой лицензии индивидуальна, в среднем составляет $25 тыс. Кроме того, лицензиат-консультант, приобретший лицензию, ежегодно должен выплачивать проценты (роялти) - около 2% от дохода,

полученного от использования прав на патент. Компания Landmark Education работает и в США, и в других странах. Если она предпринимает экспансию в какую-либо другую страну, то, как правило, она избирает такую организационно-правовую форму осуществления предпринимательской деятельности, как представительство, и для зондирования ситуации направляют своих тренеров для проведения тренингов, а затем подготавливает таковых из числа местных специалистов.

Известно, что в России применяется подход почти полного отрицания патентов на организационные, управленческие и бизнес-процессы. Свой прочный отпечаток на мышление россиян наложил индустриальный век и административно-командная система управления. И для изменения сознания, убеждений и воззрений, осознания новой роли идей в современном обществе понадобится, видимо, еще немало времени. Поскольку в основе российского патентного права лежат технические решения или способы действий по отношению к неким техническим объектам, то существующие нормы и определяют подход регистраторов к оценке представляемых для патентования объектов. Обязательное условие для получения патента - это наличие определенного технического объекта либо технических составляющих. Но в чистых организационных приемах и методах ведения бизнеса технические объекты практически не встречаются. Поэтому в большинстве европейских стран если и выдаются патенты, то в них должна идти речь о такой формуле изобретения, в которой объект заведомо подлежит патентованию.

Среди признаков такого объекта может быть один, не признаваемый патентоспособным, но, по сути, самый важный, "под который" и писалась вся формула изобретения. Станет или нет изобретение патентом - во многом зависит от мастерства и опыта патентного поверенного, составляющего описание, поскольку именно его искусство на данном этапе приобретает решающее значение. А если организация или отдельный менеджер сможет получить патент на организационные, управленческие процессы, то она вправе заняться выдачей лицензий, взимать роялти, запрещать конкурентам производить товары и услуги, подпадающие под описание ее патента, а в случае нарушения своих прав - требовать их защиты в судебном порядке.

Активное патентование в США всевозможных организационных, управленческих, бизнес-методов и приемов можно объяснить преобладанием в высокотехнологичных странах объектов, основанных на новых идеях, которые авторы всеми силами и средствами, в первую очередь правовыми, стремятся

защитить. Постепенно трансформация практики, сложившейся в Америке, Японии, формирует идеологические предпосылки для создания подобного подхода в других странах, а соответственно, и в России.

Следует подчеркнуть, что на Западе и в России стремительно развиваются отношения на основе договора франчайзинга.Суть этого метода та же, что при экспорте бизнес-методов, защищенных патентом, - экспорт форм и методов управления. Однако этот экспорт, включающий в себя целый комплекс организационных, управленческих, психологических и иных методов, обобщаемых понятием "комплекс исключительных прав", охраняется товарным знаком. На этом уровне защита бизнес-методов в России уже существует. Можно предположить, что и патентная форма защиты бизнес-методов пробьет себе дорогу в России и станет правовой формой опосредования идей еще в одной важной сфере - организационно-управленческой.

Срок охраны авторских прав в России - 50 лет, сроки действия патентов - 15-20 лет, в течение которых автор может получать свое вознаграждение. Эта "охранная грамота" призвана стимулировать научный поиск.

А задача всех участников предпринимательских отношений, соприкасающихся с рассматриваемыми вопросами, - овладеть правовым инструментарием и знаниями о защите коммерческой тайны (КТ) компании, воплощенной в идеях от стадии их рождения до разработки и внедрения.

Лекция 7. Коммерческая тайна компании

Коммерческая тайна (КТ) является сокровищем любой компании в условиях рыночной экономики. В процессе осуществления предпринимательской и управленческой деятельности образуется и накапливается значительное количество разнообразной информации, имеющей ключевое значение для успешного развития бизнеса. Ведь именно с информацией, в том числе содержащей тайну, приходится постоянно работать менеджерскому корпусу. В связи с этим понятно стремление лиц, обладающих такого рода информацией, сохранить эту информацию за собой, предотвратить ее получение третьими лицами.

Известно, что деловой мир России несет весьма существенные потери от расхищения информации. Конкуренция на современном рынке начинается уже в сфере научных разработок.

По данным мировой статистики, утрата 20% информации ведет к разорению 65% фирм и компаний.Информационная "живучесть" - один из важнейших показателей надежности организации. И в современных условиях жесткой конкурентной борьбы правовая защита различного рода информации - неотъемлемая часть менеджмента.

В течение продолжительного периода времени институт КТ был неизвестен советскому законодательству. Это вполне понятно: в условиях отсутствия конкуренции, полного огосударствления экономики просто не было необходимости в подобных правовых институтах. Понятия, близкие по содержанию к КТ, встречались только в нормативно-правовых актах, посвященных регулированию внешнеэкономической деятельности советских организаций.

Правовой статус коммерческой тайны.

Менеджер, постоянно работающий с информацией, обязан знать правовой режим, основания и условия регулирования КТ с тем, чтобы активно использовать эти нормы в борьбе за сохранение информации и недопущения ее хищения конкурентами. С этой целью необходимо всесторонне проанализировать действующее в этой части российское законодательство, чтобы вооружиться против самой сильной угрозы - хищения или утечки информации, содержащей КТ.

Центральное место среди источников правового регулирования отношений, определяющих правовой статус КТ, занимает ГК РФ, где в ст. 139 дается определение коммерческой тайны. Нормы о КТ содержатся более чем в 30 законодательных актах, среди которых: Порядок отнесения информации к конфиденциальной и виды конфиденциальной информации установлены Указом Президента РФ N 188 от 6 марта 1997 г. "Об утверждении перечня сведений конфиденциального характера". В соответствии с данным Указом к конфиденциальной информации относятся:

- сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в СМИ в установленных федеральными законами случаях;

- служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с ГК РФ и федеральными законами (служебная тайна);

- сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и

федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т. д.);

- сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с ГК РФ и федеральными законами;

- сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них и некоторые другие.

Таким образом, коммерческая тайна является одним из видов конфиденциальной информации.

Практикам, соприкасающимся с этим феноменом, необходимо учитывать особенность, присущую российскому законодательству, отличающую его в этой части от законодательств многих зарубежных стран, которая состоит в том, что к КТ может быть отнесена только документированная информация, то есть информация, которая зафиксирована на каких-либо материальных носителях: документах, материальных объектах, в том числе физических полях, где информация, составляющая КТ, находит свое отображение в виде символов, образов, сигналов, технических решений и процессов.

Другой важнейшей особенностью действующего законодательства является то, что идеи, замыслы, сведения и иные данные, какую бы коммерческую ценность для их обладателя они не представляли (в том числе, озвученные на переговорах, совещаниях, предварительные условия сделок, технические предложения и т. п.), если они не зафиксированы в какой-либо материальной форме, остаются не защищенными. (Хотя в отношении информации главным является не форма, в которой она существует, а то, какова ценность содержащихся в ней сведений.)

Действующий ГК РФ не содержит указаний на характер сведений, относимых к КТ, поэтому КТ в настоящее время могут составлять любые сведения (за исключением сведений, которые не могут составлять КТ в силу закона), соответствующие критериям, предъявляемым указанной нормой.

Признаки коммерческой тайны.

Чтобы четко разграничивать информацию, которая может или не может, является или не является КТ организации, менеджер должен знать основные положения законодательства в этой части. Основные требования, предъявляемые законодательством к КТ, чтобы квалифицировать ее в качестве таковой, закреплены в ст. 139 ГК РФ, где говорится, что информация, чтобы считаться

коммерческой тайной, должна соответствовать одновременно трем признакам.

1. Коммерческая ценность информации и ее неизвестность третьим лицам.

В соответствии со ст. 139 ГК РФ, информация, для того чтобы она могла считаться КТ, должна иметь действительную или потенциальную коммерческую ценность в силу ее неизвестности третьим лицам.

Неизвестность третьим лицам означает, что информация не должна быть общеизвестна. Под общеизвестностью можно понимать то, что "известно неопределенно большому кругу лиц и доступно восприятию каждого желающего". Общеизвестная информация, даже если она имеет большую коммерческую ценность, в принципе не может считаться КТ. Однако в исключительных случаях такая информация все-таки будет признаваться КТ, "если секретом будет тот факт, что предприятие использует именно этот способ или устройство и в связи с этим добивается наибольшего успеха". КТ считается информация, имеющая коммерческую ценность в силу ее неизвестности третьим лицам. Если какие-то знания, используемые предпринимателем, позволяют ему добиваться коммерческих успехов и неизвестен тот факт, что эти знания могут приносить выгоду, то такие знания могут считаться КТ лица, обнаружившего их полезный эффект.

Кроме того, такой критерий, как коммерческая ценность, может быть рассмотрен с разных точек зрения.

Во-первых, под коммерческой ценностью исследователи данного вопроса понимают способность информации быть объектом рыночного оборота.

Во-вторых, к КТ относится информация, использование которой предоставляет ее обладателю определенные экономические преимущества в силу того, что его конкуренты такой информацией не обладают. Коммерческая ценность в этом случае может выражаться в возможности получения прибыли от реализации продукции, произведенной с использованием секретных технологий, секретов торговли, от расширения рынков сбыта и т. п. Если же информация не представляет для ее обладателя экономической ценности, она не может считаться КТ.

В-третьих, к КТ относятся сведения, представляющие интерес для третьих лиц, которые могли бы получить определенную выгоду, если бы они этой информацией обладали. Хотя это условие может выполняться не всегда. Например, какая-то технология настолько сложна и требует таких уникальных условий

производства, что фактически лицами иными, чем обладатель данной технологии, использоваться не может, а следовательно, никакой ценности для них не представляет. Однако было бы не правильным отказывать в признании за такой технологией статуса КТ, поскольку она представляет очевидную экономическую ценность для ее обладателя, кроме того, такая технология представляет для конкурентов ее обладателя потенциальную коммерческую ценность.

В-четвертых, информация, составляющая КТ, может иметь не только действительную, но и потенциальную коммерческую ценность. Поэтому к КТ относятся не только знания и сведения, активно используемые в предпринимательской деятельности, но и такие, которые не используются, но могут быть использованы в будущем, то есть несущие в себе коммерческий потенциал.

2. Отсутствие доступа к информации на законном основании.

Второй критерий, о котором должен знать менеджер и которому должна соответствовать информация, чтобы считаться КТ, состоит в том, что к этой информации не должно быть свободного доступа на законном основании.

Для профилактики спорных ситуаций, которые могут возникнуть в практической деятельности, важно уяснить возможные варианты толкования понятия "доступ", поскольку его можно понимать как в широком, так и в узком смыслах. В широком смысле под доступом имеется в виду доступность сведений, возможность их свободного получения любыми лицами. В узком смысле под доступом можно понимать возможность получения сведений, составляющих КТ, от их обладателя, основанную на законодательных либо договорных нормах для использования в определенных целях, которые должны быть оговорены в этих нормах. Такого рода доступ представляет собой своего рода изъятие из монополии субъекта информации. Он может осуществляться добровольно либо в обязательном порядке.

Особое внимание менеджеры должны обратить на то, что им дано право добровольно предоставить доступ к секретной информации своим контрагентам по договорам.

Это может иметь место, когда информация передается по договору заинтересованным лицам. Примером может служить лицензионный договор, в рамках которого оформляются отношения между правообладателем (лицензиаром) и пользователем (лицензиатом). Типичным является договор на передачу готовых научно-технических разработок: технологий, конструкций, содержащих незапатентованные технические

решения, дизайн и т. п. Право на коммерческую информацию может передаваться по договору коммерческой концессии (франчайзинга). Элементы лицензионного договора могут включаться в другие гражданско-правовые договоры (например, на выполнение научно-исследовательских и опытно-конструкторских работ, совместной деятельности, подряда, о создании акционерного общества). Во всех договорах, предусматривающих передачу прав на использование сведений, являющихся КТ, на пользователя должна быть возложена обязанность по соблюдению ее конфиденциальности. И менеджеры должны позаботиться о том, чтобы все необходимые меры по сохранности информации были отражены в соответствующем договоре.

Законными способами получения информации являются самостоятельное получение информации и "деконструирование", или "обратный инжиниринг". Суть "обратного инжиниринга" состоит в том, что приобретается какой-либо продукт, выпущенный в широкую продажу конкурентом, и подвергается различного рода исследованиям - разборке-сборке, тестированию, различным исследованиям с целью выяснения всех его составляющих, характеристик и параметров для создания своего, аналогичного конкурентному продукта. Поскольку сведения были получены из законного источника (товара, находящегося в широкой продаже), то такое их получение и последующее использование не рассматриваются законом как нарушение КТ первоначального производителя.

Законным способом получения информации является ее получение из общедоступных источников (рекламных проспектов, публикаций в периодической печати, научных выступлений и т. п.). Каким способом можно защитить свою продукцию от подобного рода копирования?

Многие зарубежные компании стремятся обезопасить себя от раскрытия своих торговых секретов третьими лицами путем включения в контракты с покупателями своей продукции оговорку о запрещении подобного рода операций.

Бывают случаи, когда правообладатели вынуждены раскрывать информацию потенциальным партнерам до заключения договора, поскольку требуется убедить его в том, что ноу-хау "работает".

Например, при заключении договора франчайзинга предусмотрен "паушальный" взнос, включающий в себя компенсацию на тот случай, если франчайзи после ознакомления с ноу-хау откажется от его заключения.

Предоставление доступа в обязательном порядке связано с возможностью истребования информации, составляющей КТ, различными госорганами в ходе выполнения возложенных на них функций.

В свое время Закон о предпринимательской деятельности содержал норму о том, что предприятие имело право не представлять информацию, составляющую КТ. На тот момент в российском праве отсутствовало законодательное определение КТ (что позволяло отказывать в предоставлении любых сведений) и ничего не говорилось о том, распространяется это право на отношения со всеми сторонними лицами или нет.

В настоящее время все чаще можно встретить нормы, предоставляющие работникам соответствующих органов право истребовать разного рода информацию, в том числе и составляющую КТ.

Это обстоятельство менеджеры должны учитывать в своей практической деятельности. Под видом налоговой или иной проверки иногда изымаются буквально все документы, часто и не относящиеся к ее предмету. Цели такой проверки могут быть самыми различными. Гарантировать же, что не произойдет утечки информации в современных условиях российской действительности, крайне сложно. Поэтому менеджер должен хорошо знать законодательство в этой части и предоставлять только необходимые документы, а также принимать все меры к сохранению конфиденциальных данных и составляющих коммерческую информацию в той мере, в которой он считает это возможным.

Налоговые органы имеют право:

- осматривать (обследовать) любые используемые налогоплательщиком для извлечения дохода либо связанные с содержанием объектов налогообложения производственные, складские, торговые и иные помещения и территории;
- изымать при проведении налоговых проверок у налогоплательщика или иного обязанного лица документы, свидетельствующие о совершении налоговых правонарушений;
- требовать от налогоплательщика или иного обязанного лица документы, подтверждающие правильность исчисления и своевременность уплаты налогов.

Таким образом, прослеживается тенденция обязательности предоставления информации, в том числе и составляющей КТ, по требованиям компетентных органов. Очевидно, необходим механизм, который бы защищал интересы обладателя КТ в таких ситуациях. В самих нормативных актах, предоставляющих

соответствующим органам право требовать предоставления информации, должна быть предусмотрена обязанность этих органов по неразглашению полученной информации. Так, Налоговый кодекс предусматривает, что производственная тайна или КТ налогоплательщика, ставшая известной должностному лицу налогового органа, привлеченному специалисту или эксперту при исполнении ими своих обязанностей, является налоговой тайной и не подлежит разглашению.

Как представляется, требования государственных органов предоставить им информацию, составляющую КТ, являются законными в той мере, в какой они предъявляются в ходе выполнения ими функций, возложенных на них законом, и в объеме, оправданном для их выполнения. Однако грань здесь весьма тонкая.

Следует отметить, что возможность получения госорганами и их работниками сведений, составляющих КТ, не влечет за собой утрату этими сведениями статуса КТ: информация от этого не становится "свободно доступной", поскольку доступом к ней обладают только конкретные лица в конкретных объемах и это не делает ее доступной для широкой публики.

Возможность свободного доступа не всегда означает, что как только та или иная информация становится доступной для получения третьими лицами, она теряет статус КТ. Классический пример - формула "Кока-колы". Все ингредиенты этого напитка известны, он повсеместно продается, однако его формула представляет собой КТ производящей его компании, поскольку никому еще не удавалось ее раскрыть.

3. Меры по охране конфиденциальности информации.

Третьим критерием, о котором должен знать менеджер и которому должна соответствовать информация, составляющая КТ, является принятие обладателем информации мер по охране ее конфиденциальности.

Невыполнение требования по охране конфиденциальности сводит на нет и первые два признака КТ. Если информация не содержится в секрете, то она доступна, по крайней мере, доступ к ней существенно облегчен. Таким образом, перестает выполняться условие о том, что "к информации нет свободного доступа на законном основании". А если информация становится доступной, то она теряет и качество коммерческой ценности.

Все меры по поддержанию секретности информации можно условно разделить на три вида мер: технические, организационные и юридические (правовые).

Совокупность правовых, организационных, технических и иных мер, применяемых обладателем КТ для обеспечения ограниченного доступа к конфиденциальной информации, называется режимом КТ.

1. В соответствии с Положением о лицензировании деятельности по технической защите конфиденциальной информации, под технической защитой конфиденциальной информации понимается комплекс мероприятий и (или) услуг по защите ее от несанкционированного доступа, в том числе и по техническим каналам, а также от специальных воздействий на нее в целях уничтожения, искажения или блокирования доступа к ней. К техническим относятся меры, связанные с использованием различных технических средств, препятствующих несанкционированному доступу к информации:

- кодирование сообщений, передаваемых по каналам электронной или факсимильной связи;
- установление различных устройств, препятствующих снятию информации в процессе ее прохождения по каналам связи, сигнализационных устройств;
- использование аппаратов для уничтожения документов и т.д.

2. К организационным относятся меры по ограничению доступа к секретной информации работников организации и третьих лиц, включающие:

- порядок оформления доступа к сведениям, составляющим КТ;
- введение пропускного режима на предприятии;
- ограничение доступа на отдельные участки производства лиц, не участвующих непосредственно в производственных процессах на данных участках;
- специальное делопроизводство, установление различных режимов секретности документов;
- инструктаж работников и контроль их работы и т. д.

3. К юридическим (правовым) мерам можно отнести федеральное законодательство в сфере информационной безопасности и различные правовые акты предприятия:

- перечень сведений, составляющих КТ;
- положение о КТ;
- контракты, соглашения о конфиденциальности и т. п.

Такова совокупность мер, которые призваны обеспечить конфиденциальность информации.

Договор как форма охраны коммерческой информации.

Мы уже упоминали о том, что одним из инструментов, которым должен научиться искусно пользоваться менеджер,

является договор, призванный формализовать меры по охране КТ. Иногда его называют соглашением. Подобным соглашениям следует уделять самое серьезное внимание, поскольку в случае разглашения работником информации, составляющей КТ работодателя, такие соглашения составят юридическую основу для привлечения работника к ответственности и взыскания причиненного ущерба. Подобные соглашения могут заключаться как в виде отдельного документа, так и в виде условия в трудовом договоре.

При заключении подобных соглашений следует иметь в виду, что в соответствии со ст. 57 ТК РФ условия договоров о труде, ухудшающие положение работника по сравнению с законодательством о труде, являются недействительными. Под условиями, ухудшающими положение работника, в частности, можно понимать установление обязанностей, введение дополнительных мер ответственности, не предусмотренных трудовым законодательством. Поэтому если данное условие будет неправильно сформулировано, это потенциальный повод для подачи искового заявления.

Какие же меры может включить менеджер в договор, чтобы максимально обеспечить сохранность КТ организации? Представляется, что профилактикой разглашения КТ в этом случае могут служить следующие обязательства, принимаемые на себя работником:

- не разглашать составляющую КТ организации информацию, которая будет ему доверена или станет известна по работе;
- не передавать третьим лицам и не раскрывать публично информацию, составляющую КТ организации, без согласия администрации организации;
- сохранять информацию, составляющую КТ тех организаций, с которыми поддерживаются деловые отношения;
- выполнять относящиеся к работнику требования приказов, инструкций и положений по обеспечению сохранности КТ организации;
- не использовать информацию, составляющую КТ организации, для занятия другой деятельностью, которая в качестве конкурентного действия может нанести ущерб организации;
- в случае попытки посторонних лиц получить от работника информацию, составляющую КТ организации, незамедлительно известить об этом соответствующее должностное лицо;
- незамедлительно сообщать соответствующему должностному лицу организации об утрате или недостаче носителей

информации, составляющей КТ, удостоверений, пропусков, ключей от режимных помещений, хранилищ, сейфов, личных печатей и о других актах, которые могут привести к разглашению КТ организации, а также о причинах и условиях возможной утечки информации, составляющей КТ;

- в случае увольнения все носители информации, составляющие КТ организации (документы, чертежи, рукописи, магнитные ленты, перфокарты, перфоленты, диски, дискеты, распечатки, кино- и фотоматериалы, изделия и др.), которые находились в распоряжении работника в связи с выполнением им служебных обязанностей во время работы в организации, передать соответствующему должностному лицу организации.

Менеджер должен под расписку предупредить работника об ответственности за нарушение этих положений (невыполнение взятых на себя обязательств). Кроме того, в трудовом договоре либо в его неотъемлемой части (обязательстве о неразглашении информации, составляющей КТ) следует предусмотреть порядок ознакомления работника с действующими в организации положениями и инструкциями по обеспечению сохранности КТ. Кроме того, следует определять объем информации, передаваемой каждому конкретному работнику, за которую он должен нести ответственность.

Другой категорией субъектов КТ является непосредственно сам руководитель организации. В силу своих должностных обязанностей и предоставленных ему собственником полномочий (если такой руководитель сам не является собственником организации, а значит, и обладателем КТ) руководитель организации может быть наделен исключительными правами по организации защиты информации, составляющей КТ. Руководитель обладает также особыми возможностями в части информированности об охраняемых законом коммерческих секретах, в том числе и о коммерческой КТ руководимой им организации. На руководителя организации должны быть возложены обязанности по обеспечению сохранности КТ организации. В связи с этим в контракт, заключаемый с руководителем при его найме, назначении или избрании, целесообразно включить положения, обуславливающие порядок сохранения КТ руководителем.

При формулировании предлагаемых нами положений нужно исходить из следующих критериев:

- необходимо обязать руководителя строго хранить КТ организации и не использовать ее для занятия любой другой деятельностью в ущерб организации;

- возложить на руководителя организации персональную ответственность за создание необходимых условий для обеспечения сохранности КТ организации;

- предупредить об ответственности за нарушение режима КТ и о том, что последствиями этого могут стать расторжение контракта, а также наступление предусмотренной законом юридической ответственности.

Соглашения о неразглашении могут заключаться с работниками и при прекращении трудовых отношений. Возможность их заключения вытекает из п. 1 ст. 8 ГК РФ, устанавливающего, что гражданские права и обязанности возникают из договоров и сделок, предусмотренных законом, а также из иных договоров и сделок, хотя и не предусмотренных законом, но не противоречащих ему. В соответствии с п. 1 ст. 307 ГК РФ в силу обязательства одно лицо (должник) обязано совершить в пользу другого лица (кредитора) определенное действие либо воздержаться от определенного действия, а кредитор имеет право требовать от должника исполнения его обязанности. Предметом таких соглашений будет являться обязательство увольняющегося работника не разглашать определенную информацию, составляющую КТ, ставшую ему известной во время работы у данного работодателя, а также не использовать ее в своей последующей деятельности. Как представляется, эта информация в соглашениях должна оговариваться как можно конкретнее, чтобы не ограничивать работника в его будущей деятельности.

Соглашения о неразглашении могут заключаться и с контрагентами по различным гражданско-правовым договорам, связанным с раскрытием сторонами по договору различной секретной информации. Для отдельных видов договоров такое условие прямо предусмотрено ГК РФ.

Аналогичная практика получила широкое распространение за рубежом, где показала свою эффективность в ходе ряда судебных процессов, где был возмещен ущерб, причиненный раскрытием коммерческой информации после увольнения работников из организации.

Лекция 8. Свойства коммерческой тайны

Является ли коммерческая тайна (КТ) объектом интеллектуальной собственности? Точное определение здесь очень важно, поскольку существенно меняется режим и возможности

использования в коммерческих целях. Одни исследователи считают, что КТ может считаться объектом интеллектуальной собственности, другие - что нет. Такому расхождению во взглядах в большой степени способствует то, что позиция законодателя в этом вопросе не постоянна. Так, Закон РСФСР "О собственности в РСФСР" в ст. 2 прямо указывают на ноу-хау и торговые секреты как на объекты интеллектуальной собственности.

Основы гражданского законодательства хотя и содержали в ст. 151 развернутую характеристику секретов производства (ноу-хау), но ничего не говорили по поводу их соотношения с объектами интеллектуальной собственности, что ставило под сомнение принадлежность секретов производства к объектам интеллектуальной собственности.

Эта тенденция еще более усилилась с принятием первой части ГК РФ. Ни в ст. 138 ГК РФ, посвященной интеллектуальной собственности, ни в ст. 139 ГК РФ, посвященной КТ, не содержится ответа на вопрос, можно ли считать КТ объектом исключительных прав.

Однако прежде чем ответить на вопрос, может ли рассматриваться КТ в качестве объекта интеллектуальной собственности, нужно выяснить, что представляет собой понятие "интеллектуальная собственность".

В соответствии со ст. 138 ГК РФ под интеллектуальной собственностью признается исключительное право гражданина или юридического лица на результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации юридического лица, индивидуализации продукции, выполняемых работ или услуг. Таким образом, несмотря на то, что наше законодательство использует понятие "интеллектуальная собственность", фактически под ним понимается совокупность личных и имущественных прав не на саму собственность, а на ее результаты. Обе группы Иран - на саму и собственность и право на права па нее - "теснейшим образом взаимосвязаны и переплетены, образуя между собой неразрывное единство".

Всем объектам *интеллектуальной собственности присущи следующие признаки*:

- эти объекты являются результатами интеллектуальной деятельности;
- это нематериальные объекты, которые лишь воплощаются в определенных материальных объектах, являющихся их материальными носителями;
- это объекты, на которые за кем-либо закреплено исключительное право владения и пользования ими.

Понятие "результат интеллектуальной деятельности" детализируется в законодательных актах, посвященных регулированию отношений, связанных с конкретными объектами интеллектуальной собственности. Так, например, в соответствии со ст. 6 Закона РФ "Об авторском праве и смежных правах" от 9 июля 1993 г., объектом авторских прав считаются произведения науки, литературы и искусства, являющиеся результатом творческой деятельности. Патентный закон РФ от 23 сентября 1992 г. предоставляет изобретению правовая охрану в том случае, если оно является новым, имеет изобретательский уровень и промышленно применимо; промышленному образцу - если он является новым и оригинальным; полезной модели - если она является новой.

Новизна предполагает определенный элемент творчества, созидания. Следовательно, общность различных объектов интеллектуальной собственности состоит в том, что все они связаны с творческой, креативной, созидательной деятельностью человека. Однако ГК РФ определяет объект интеллектуальной собственности как "результат интеллектуальной деятельности", а не как "результат творческой деятельности". Понятие "результат интеллектуальной деятельности" шире понятия "результат творческой деятельности" и вполне может включать в себя все то, что создано в результате интеллектуальных (умственных) усилий человека, то есть им может быть и информация.

Второй признак заключается в том, что под объектом интеллектуальной собственности во всех случаях подразумевается нематериальный объект, который лишь воплощается в определенных материальных объектах, являющихся его материальными носителями. КТ как информация подпадает и под этот признак объектов интеллектуальной собственности.

Информация не может монопольно принадлежать одному лицу. Одни и те же сведения могут являться КТ различных лиц, и все они будут считаться ее законными обладателями (при условии, что они получили эти сведения законным образом).

В отличие от интеллектуальной собственности, где запрет устанавливается на незаконное использование объекта исключительных прав без согласия правообладателя, в случае с КТ запрещается незаконное получение информации, составляющей КТ.

Таким образом, мы приходим к выводу, что КТ, по крайней мере, при сегодняшнем уровне правовой регламентации, не может рассматриваться в качестве объекта интеллектуальной

собственности, поскольку права обладателя КТ не могут рассматриваться в качестве исключительных.

В этой связи нуждается в особом комментарии ст. 1027 ГК РФ о договоре коммерческой концессии. По этому договору правообладатель передает пользователю комплекс исключительных прав, в том числе право на фирменное наименование, товарный знак, знак обслуживания, а также на охраняемую коммерческую информацию. Подчеркнем: если речь идет об охраняемой КТ информации, то она является объектом нрава на информацию, а не объектом исключительных прав. Другими словами, если бы КТ являлась объектом исключительных нрав, то ее нужно было квалифицировать как результат интеллектуальной собственности. Возможно, в будущем это произойдет, когда практика и законодатель найдут приемлемые формы ее материализации и обоснования.

На практике правообладатель в целях распространения сферы своего влияния предпочитает передавать права на использование своей интеллектуальной собственности и ноу-хау различным пользователям, сохраняя свое исключительное право и право на охраняемую КТ информацию. Каждый из пользователей обязан не разглашать секреты производства правообладателя и другую полученную от него конфиденциальную информацию.

Ст. 128 ГК РФ рассматривает объекты интеллектуальной собственности и информацию в качестве различных объектов гражданских прав. Итак, для руководства в практической деятельности важно, что КТ пока не является объектом интеллектуальной собственности, а представляет собой особую разновидность такого объекта гражданских прав, как информация. Иными словами, КТ - это сама информация, дающая основание отнесения ее к тайне.

Хотя КТ непосредственно и не является объектом интеллектуальной собственности, она имеет коммерческую ценность и право пользования ею может быть оценено, в том числе по соглашению сторон при заключении, например, договора о совместной деятельности, других договоров и передана (внесена) в качестве вклада для последующего извлечения прибыли от ее совместного использования. Эти детали должны быть оговорены при заключении договоров, ибо их отсутствие - это упущенная выгода и просчет менеджера.

Объект и субъект коммерческой тайны.

Поскольку управленческая деятельность всегда направлена на управление конкретными объектами, будет правильным проанализировать их состав.

В соответствии с действующим законодательством КТ является объектом хозяйственного, гражданского оборота наряду с такими материальными объектами, как здания, сооружения, машины, механизмы, работы, услуги, результаты интеллектуальной деятельности, нематериальные блага, вещи. Чтобы экономическая деятельность была прибыльной, менеджеру нужно знать как можно больше о потребителях того или иного товара. Ему также необходимы сведения о конкурентах на рынке производимой продукции.

Ст. 20 Закона об информации по сравнению со ст. 139 ГК РФ охватывает собой более широкий круг сведений конфиденциального свойства, характеризующих специальную сферу общественных отношений. Это отношения и в области предпринимательской деятельности, и информационные отношения в иных областях общественной деятельности, регулируемые другими отраслями права.

Примечательным является факт, что ученые ведущих государств мира с конца XX в. пытаются сформулировать понятие объекта КТ. К примеру, Конгрессу США пришлось на неопределенный срок отложить принятие Закона о защите КТ из-за невозможности четко сформулировать сам предмет защиты, то есть содержание объекта КТ.

Ст. 139 ГК РФ определяет КТ как информацию, имеющую действительную или потенциальную коммерческую ценность в силу ее неизвестности третьим лицам, к которой нет доступа на законном основании и обладатель которой принимает меры к охране ее конфиденциальности. В ГК РФ объект КТ определен лишь в обобщенном виде. Упоминавшийся Перечень сведений конфиденциального характера также не разрешает всех возникающих вопросов. Иными словами, получается, что под информацией, составляющей КТ, можно понимать любые сведения, отнесение которых к такой тайне не запрещено законом и иными правовыми актами.

В повседневной практике часто можно, задав вопрос менеджеру, услышать в ответ: "Этого говорить не могу, это коммерческая тайна", хотя запрашиваемые сведения часто таковой не являются. Например, во время проведения занятий по корпоративной программе в г. Нижнем Новгороде среди топ-менеджеров автор задал одному из ведущих финансовых специалистов несколько вопросов, касающихся финансового

положения ОАО "ГАЗ". На что тот ответил, что не вправе отвечать, поскольку эти данные являются КТ предприятия. Автор здесь же в учебном классе взял со стенда отчет о результатах хозяйственной деятельности общему собранию ОАО "ГАЗ", в котором значились все испрашиваемые данные.

Информация, не являющаяся коммерческой тайной.

Ответ на этот вопрос дает Перечень сведений, которые не могут составлять коммерческую тайну, N 35, утвержденный Постановлением Правительства РФ. В документе сказано, что "Правительство РСФСР постановляет:

1. Установить, что КТ предприятия и предпринимателя не могут составлять:

- учредительные документы (решение о создании предприятия или договор учредителей) и Устав;

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

- сведения по установленным формам отчетности о финансово-хозяйственной деятельности и иные сведения, необходимые для проверки правильности исчисления и уплаты налогов и других обязательных платежей в государственную бюджетную систему РСФСР;

- документы о платежеспособности;

- сведения о численности, составе работающих, их заработной плате и условиях труда, а также о наличии свободных рабочих мест;

- документы об уплате налогов и обязательных платежах;

- сведения о загрязнении окружающей среды, нарушении антимонопольного законодательства, несоблюдении безопасных условий труда, реализации продукции, причиняющей вред здоровью населения, а также других нарушениях законодательства РСФСР и размерах причиненного при этом ущерба;

- сведения об участии должностных лиц предприятия в кооперативах, малых предприятиях, товариществах, акционерных обществах, объединениях и других организациях, занимающихся предпринимательской деятельностью.

2. Запретить государственным и муниципальным предприятиям до и в процессе их приватизации относить к КТ данные:

- о размерах имущества предприятия и его денежных средствах;

- о вложении средств в доходные активы (ценные бумаги) других предприятий, в процентные облигации и займы, в уставные фонды совместных предприятий;

- о кредитных, торговых и иных обязательствах предприятия, вытекающих из законодательства РСФСР и заключенных им договоров;

- о договорах с кооперативами, иными негосударственными предприятиями, творческими и временными трудовыми коллективами, а также отдельными гражданами.

3. Предприятия и лица, занимающиеся предпринимательской деятельностью, руководители государственных и муниципальных предприятий (обязаны представлять сведения, перечисленные в пп. 1 и 2 настоящего Постановления, по требованию органов власти, управления, контролирующих и правоохранительных органов, других юридических лиц, имеющих на это право в соответствии с законодательством РСФСР, а также трудового коллектива предприятия".

КТ также не могут быть сведения, обладающие коммерческой ценностью, использование которых нарушает закон. Например, не охраняется правом информация о применяемых способах и методах оптимизации налоговых платежей: информация о переориентации типа и предмета договора на деятельность, которая более благоприятна с точки зрения налогообложения; сведения о диверсификации, реструктуризации производства: методика увеличения затрат, относимых на себестоимость производимой продукции, услуг и товаров, информация и др.

Информация, составляющая коммерческую тайну.

Попытаемся определить перечень сведений, которые могут составлять КТ организации. К числу сведений, составляющих КТ, можно отнести:

1. Производство.

1.1. Сведения о структуре производства, производственных мощностях, типе оборудования, запасах, сырье и готовой продукции.

2. Управление.

2.1. Сведения об оригинальных методах управления предприятием (фирмой).

2.2. Сведения о подготовке, принятии и исполнении решений руководства по производственным, научно-техническим, коммерческим и организационным вопросам.

3. Планы.

3.1. Сведения о планах расширения или свертывания производства различных видов продукции и их технико-экономических обоснованиях.

3.2. Сведения о планах инвестиций, закупок, продаж, импорта, экспорта.

4. Совещания.

4.1. Сведения о целях, рассматриваемых вопросах, результатах, фактах проведения совещаний и заседаний органов управления предприятия (фирмы).

5. Информация о рынке.

5.1. Сведения о применяемых методах изучения рынка.

5.2. Сведения о маркетинговых исследованиях и их результатах, содержащие оценки состояния и перспективы развития рыночной конъюнктуры.

5.3. Сведения о рыночной стратегии предприятия (фирмы).

5.4. Сведения о применяемых методах осуществления продаж.

5.5. Сведения об эффективности коммерческой деятельности.

5.6. Сведения о регионах сбыта готовой продукции.

5.7. Сведения о заинтересованности в приобретении товара.

6. Партнеры.

6.1. Сведения о внутренних и зарубежных заказчиках, подрядчиках, поставщиках, клиентах, потребителях, покупателях, компаньонах, спонсорах, посредниках и других партнерах, а также конкурентах, которые не содержатся в открытых источниках (справочниках, каталогах и др.).

6.2. Методика организации работы с деловыми связями, с ключевыми партнерами.

7. Переговоры.

7.1. Сведения о целях, задачах, тактике и стратегии ведения переговоров с деловыми партнерами, деловая переписка.

8. Контракты.

8.1. Условия коммерческих контрактов, платежей и услуг.

9. Цены.

9.1. Сведения о методах расчета, структуре, уровне цен на продукцию и размерах скидок.

Сведения о предельно допустимой (либо запланированной) цене, на которую намерена согласиться противоположная сторона, широко используются для разработки стратегии и тактики

предполагаемых переговоров либо для опережения конкурента в заключении выгодных контрактов.

Российская сторона, например, понесла убытки на многие миллионы долларов при заключении нескольких контрактов на закупку технологического оборудования для производства минеральных удобрений у ряда зарубежных фирм. Причиной потерь стала утечка (через подкупленного иностранцами российского участника переговоров) информации о предельно допустимой цене контракта, которую была готова заплатить российская сторона,

10. Торги, аукционы.

10.1. Сведения о подготовке к торгам или аукциону и их результатах.

11. Наука и техника.

11.1. Сведения о целях, задачах и программах научных исследований.

11.2. Ноу-хау, торговые секреты, оригинальные идеи НИР и ОКР, готовящиеся проекты.

11.3. Конструкционные характеристики создаваемых изделий и параметры разрабатываемых технологических процессов (размеры, объемы, конфигурация, процентное содержание компонентов, температура, давление, время и т. д.).

11.4. Аналитические и графические зависимости, отражающие найденные закономерности и взаимосвязи.

11.5. Данные об условиях экспериментов и оборудовании, на котором они проводились.

11.6. Сведения о материалах, из которых изготовлены детали.

11.7. Отведения об особенностях конструкторско-технологического и художественно-технического решения изделия (дизайн).

11.8. Сведения о методах защиты от всевозможных подделок.

11.9. Сведения о состоянии программного и компьютерного обеспечения.

11. 10. Незапатентованные изобретения.

12. Технология.

12.1. Сведения об особенностях используемых и разрабатываемых технологий и специфике их применения.

13. Безопасность.

13.1. Сведения о порядке и состоянии защиты КТ.

13.2. Сведения о порядке и состоянии организации охраны, пропускном режиме, системе сигнализации, средствах связи и оповещения.

13.3. Сведения, составляющие КТ предприятий-партнеров и переданные на доверительной основе предприятию (фирме).

13.4. Списки персонала и информация о сотрудниках (их характеристики). Персональные данные сотрудников. Перечень вводится специальным приказом руководителя предприятия (фирмы) в виде приложения к нему. Сотрудники должны под расписку ознакомиться с этим документом.

14. Страхование.

15. Негосударственное пенсионное обеспечение.

КТ может быть и так называемая негативная информация (например, сведения, позволяющие избежать вложения средств фирмы в бесперспективные разработки). К сведениям, составляющим КТ, некоторые предприниматели могут относить и собственные просчеты в коммерческой деятельности, которые могут отрицательно сказаться на деловой репутации. Этим обстоятельством часто пользуются недобросовестные конкуренты, вымогающие деньги у правопослушных предпринимателей под угрозой огласки допущенных ими просчетов и судебных споров. Особенно уязвимы в подобных случаях российские субъекты экономической деятельности, не имеющие опыта работы на внешнем рынке.

Кто может являться владельцем права на информацию, составляющую коммерческую тайну?

Осуществляя процесс управления отношениями, складывающимися в процессе использования КТ и конфиденциальной информации, управляющий этими процессами должен знать, что основными субъектами права на КТ являются обладатели КТ и их правопреемники.

Обладатель КТ - это лицо, обладающее на законном основании информацией, составляющей КТ, и соответствующими правами в полном объеме.

Существует также понятие "конфидент коммерческой тайны". Им является лицо, которому в силу служебного положения, договора или на законном основании известна КТ другого лица.

В период с 1 января 1991 г. и по 1 января 1995 г. (период действия ст. 33 Закона СССР от 4 июня 1990 г. "О предприятиях в СССР") по законодательству России субъектами права на КТ могли быть только юридические лица. С принятием части первой ГК РФ ситуация изменилась. Теперь обладателями КТ могут быть как физические, так и юридические лица. Правда, ст. 139 ГК РФ не дает прямого ответа на вопрос, какие конкретно лица (физические или юридические) здесь имеются в виду. Однако применение такого широкого понятия, как "лица", дает основания

полагать, что законодатель определяет состав субъектов права на КТ в широком смысле слова, то есть это не только категории лиц, относящихся к хозяйствующим субъектам.

Таким образом, субъектами права на КТ могут быть как коммерческие, так и некоммерческие организации.

Физические лица как субъекты права на информацию, составляющую коммерческую тайну

В процессе управления нередко возникает вопрос: все ли лица, причастные в той или иной мере к КТ или конфиденциальной информации, могут пользоваться ею и нести ответственность за ее разглашение. Следует подчеркнуть, что к ним относятся граждане, занимающиеся предпринимательской деятельностью без образования юридического лица. Категории физических лиц - субъектов права на КТ - законодательством России не установлены. Но это не значит, что они не могут иметь доступа к ней. И этот фактор следует особо учитывать менеджерам организаций.

Много веков знает российское законодательство институт наследования, а с ним и наследственное право. Поэтому нельзя забывать о такой категории субъектов права, как физические лица, не занимающиеся предпринимательской деятельностью, но получившие, скажем, в наследство предприятие как имущественный комплекс, и это имущество продолжает использоваться (либо посредством института опекунов и попечителей, либо института доверительного управления имуществом или патронажа для осуществления предпринимательской деятельности), Наследники указанного имущества также являются субъектами права на КТ в той части, в которой наследуемое имущество может включать и право на охраняемую законом информацию.

Субъектами права на информацию, составляющую КТ, являются иностранные граждане и лица без гражданства. В соответствии с Конституцией РФ указанные лица пользуются в России правами и несут обязанности наравне с гражданами РФ кроме случаев, установленных ФЗ или международным договором РФ. Имеющиеся в российском законодательстве изъятия немногочисленны, и они не касаются прав иностранных граждан и лиц без гражданства на КТ. Ни Конституция РФ, ни ГК РФ не содержат каких-либо ограничений на этот счет.

Следовательно, эти лица также могут быть субъектами права на КТ в соответствии с нормами гражданского законодательства РФ.

Таким образом, круг субъектов права на КТ составляют:

- коммерческие организации;

- некоммерческие организации, осуществляющие предпринимательскую деятельность, служащую достижению целей, ради которых они были созданы и соответствующую этим целям (за исключением тех некоммерческих организаций, которым законом не предоставлено право осуществлять предпринимательскую деятельность);

- граждане, зарегистрированные в качестве индивидуальных предпринимателей;

- граждане - обладатели КТ;

- иностранные лица и лица без гражданства, обладающие сведениями, составляющими КТ.

Информация, коммерческая и служебная тайна.

Следует обратить внимание менеджеров на сложность, связанную с использованием в управленческой деятельности множества терминов, относящихся к той или иной разновидности конфиденциальной информации. Содержание большинства из них в законодательстве не раскрыто. Отсутствует и понятийный аппарат, позволяющий уяснить их содержание. Учитывая то, что в законодательстве часто встречается слово "тайна", в целях практического применения следует уяснить его содержание и соотношение с термином "конфиденциальная информация". Закон, употребляя термин "тайна", часто не раскрывает его содержание.

В русском языке "тайна" традиционно означает "все сокрытое, неизвестное, неведомое", а также "нечто скрытно хранимое, что скрывают от кого-либо". Таким образом, "тайна" имеет два смысловых значения: нечто абсолютно неизвестное всем и нечто относительно неизвестное для какого-либо круга лиц.

В. Даль толковал слово "тайна" как все сокрытое, неизвестное, неведомое или нечто скрываемое, секретное, не оглашаемое.

Известно, что один из героев известного мультфильма о коте Леопольде под тайной подразумевал: "Клад, клад, клад..."

Термин "нарушение целостности и конфиденциальности" широко используется в специальной литературе, когда рассматривается проблема безопасности информационных систем, базирующихся на применении информационной техники. Под конфиденциальностью же понимается предотвращение возможности использования информации лицами, которые не имеют к ней отношения. Появление в законодательстве об информации термина "конфиденциальность" наряду с термином "тайна", по-видимому, оправдано. Слово "конфиденциальный"

происходит от латинского слова confidentia (доверие) и означает "доверительный, не подлежащий огласке". Сравнивая смысл названных терминов, можно увидеть, что они в принципе обозначают одно и то же.

Режим защиты информации устанавливается:

- в отношении сведений, отнесенных к государственной тайне, - уполномоченными органами на основании Закона РФ от 21 июля 1993 г. "О государственной тайне";

- в отношении конфиденциальной документированной информации - собственником информационных ресурсов или уполномоченным лицом на основании ФЗ "Об информации, информатизации и защите информации";

- в отношении персональных данных - ФЗ.

Определен также статус информации с ограниченным доступом. Документированная информация с ограниченным доступом по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную.

Запрещено привлекать к ответственности за разглашение и относить к информации с ограниченным доступом:

- законодательные и другие нормативные акты, устанавливающие правовой статус органов государственной власти, органов местного самоуправления, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;

- документы, содержащие информацию о чрезвычайных ситуациях, экологическую, метеорологическую, демографическую, санитарно-эпидемиологическую и другую информацию, необходимую для обеспечения безопасного функционирования населенных пунктов, производственных объектов, безопасности граждан и населения в целом;

- документы, содержащие информацию о деятельности органов государственной власти и органов местного самоуправления, об использовании бюджетных средств и других государственных и местных ресурсов. о состоянии экономики и потребностях населения, за исключением сведений, отнесенных к государственной тайне;

- документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах органов государственной власти, органов местного самоуправления, общественных объединений, организаций, представляющие общественный интерес или необходимые для реализации прав, свобод и обязанностей граждан.

Отнесение информации к государственной тайне осуществляется в соответствии с Законом РФ от 21 июля 1993 г. "О государственной тайне".

Отнесение информации к конфиденциальной осуществляется в порядке, установленном отраслевым законодательством РФ (гражданским, административным и т. д.).

Разрозненность применяемых в законодательстве терминов, характеризующих сведения конфиденциального характера, и отсутствие унификации такой информации порождают бессистемный, неконтролируемый процесс введения в правовые акты совершенно новых, ничем не обоснованных терминов. Поэтому управляющим, составляющим документы в этой сфере, следует учитывать, что применять такие термины на практике нецелесообразно, поскольку их гражданский оборот не обеспечен необходимым правовым регулированием по нормам законодательства России и международного частного права.

Современное законодательство России содержит следующие термины, характеризующие разновидности конфиденциальной информации:

- тайна следствия;
- тайна судопроизводства;
- тайна мер безопасности участников уголовного процесса;
- тайна мер безопасности, применяемых в отношении должностных лиц правоохранительных или контролирующих органов;
- тайна частной жизни граждан;
- семейная и личная тайна;
- налоговая тайна;
- профессиональная тайна;
- адвокатская тайна;
- нотариальная тайна;
- медицинская тайна;
- тайна усыновления (удочерения);
- тайна связи (тайна переписки, тайна телефонных переговоров, тайна почтовых сообщений, тайна телеграфных сообщений);
- журналистская тайна;
- тайна записей актов гражданского состояния;
- тайна завещания;
- врачебная тайна;
- служебная тайна;
- КТ;
- секреты производства;

- предпринимательская и промышленная тайна;
- торговая, научно-техническая и производственная тайна;
- технологическая тайна;
- тайна изобретения, полезной модели, промышленного образца (п. 6 названного выше Перечня сведений конфиденциального характера);
- тайна селекционного достижения (по моему мнению, по аналогии с п. б Перечня);
- тайна научного опыта и тайна торгового процесса;
- банковская тайна, тайна банковского счета, тайна операций по счету и тайна сведений о клиенте;
- тайна страхования (тайна сведений о страхователе, тайна сведений о состоянии здоровья страхователя, тайна сведений об имущественном положении страхователя, тайна сведений о застрахованном лице, тайна сведений о состоянии здоровья застрахованного лица, тайна сведений об имущественном положении застрахованного лица. предотвращении уклонения от налогообложения в отношении налогов на доходы и имущество);
- банковская тайна сведений о выгодоприобретателях, тайна сведений о состоянии здоровья выгодоприобретателей, тайна об имущественном положении выгодоприобретателей;
- инсайдерская тайна;
- тайна исповеди.

Следует помнить, что этот перечень далеко не исчерпывающий.

Интересными и нетрадиционными для российской экономики являются, например, тайна научного опыта и тайна торгового процесса, что закреплено в ст. 12 и 29 Соглашения между Правительством РФ и Правительством Королевства Нидерландов об избежании двойного налогообложения и предотвращения уклонения от налогообложения в отношении налогов на доходы и имущество от 16 декабря 1996 г. Этот факт свидетельствует о постепенной трансформации норм зарубежного права в этой части и постепенной интеграции их в российское законодательство и отечественную предпринимательскую практику.

Соотношение коммерческой и служебной тайны.

Вопрос о соотношении служебной и коммерческой тайны имеет своеобразный аспект. ГК РФ в ст. 139 оперирует этими двумя понятиями, не раскрывая, в чем их отличие, и иногда сложно провести разграничения в практической деятельности

менеджеров при составлении соответствующих документов, регламентирующих порядок работы с этими видами тайн.

По словарю В. Даля термин "служебный" означает "...ко служенью, во всех значениях относящийся". Иными словами, термин "служебный" подразумевает не равные отношения между их участниками, а некую вертикаль, основанную на власти и подчинении. Участниками таких отношений являются индивидуальные и коллективные субъекты административного нрава, то есть граждане и организации. Этимологическое значение термина "служебный" указывает на неравенство позиций участников подразумеваемых отношении.

Уточнению ситуации способствует п. 3 Перечня сведений конфиденциального характера. В соответствии с ним служебную тайну составляют сведения, доступ к которым ограничен органами государственной власти. Приведенная в нем норма имеет четыре существенных момента:

1) разграничиваются такие объекты гражданского права, как служебная и коммерческая тайны;

2) уточняется содержание правила ст. 139 ГК РФ в части разграничения правовых режимов служебной и коммерческой тайны;

3) этой нормой вводится ограничение, в соответствии с которым устанавливается определенный порядок доступа к служебной тайне; этот порядок устанавливается органами государственной власти и федеральными законами;

4) данное правило следует рассматривать как ограничение возможности использовать в гражданском обороте служебную тайну для иных. кроме государства, субъектов.

Если исходить из требований п. 2 ст. 3 ГК РФ, то первые два момента следует рассматривать как развитие положений ГК РФ. Они направлены на урегулирование информационных отношений. В характеристику объектов служебной н коммерческой тайны они вносят некоторую определенность.

Институт служебной тайны занимает особое положение в законодательстве России. К служебной тайне, за исключением информации, составляющей государственную тайну, относятся:

- информация о деятельности государственных органов (управления, контролирующих. правоохранительных н т. д.) и их служащих. Речь идет об информации представляющей не коммерческий, а государственный интерес:

- информация, составляющая КТ субъекта. Будучи получена государственным органом в пределах своей компетенции для выполнения возложенных на него функций, она приобретает

статус служебной тайны, за разглашение которой служащий должен нести ответственность.

Именно эти различия и диктуют необходимость надлежащего правового регулирования института служебной тайны.

Де-юре правовой институт служебной тайны оформлен в рамках ГК РФ. Но де-факто в нормах действующего законодательства России он складывается как конфиденциальная информация, ставшая известной определенному кругу работников в силу выполнения ими своих служебных (должностных) обязанностей.

В отличие от нормы ст. 139 ГК РФ, определяющей объект служебной тайны как информацию, имеющую действительную или потенциальную коммерческую ценность, федеральные законы определяют его как объект совершенно иного содержания, то есть как информацию, имеющую действительную или потенциальную служебную ценность. В этих законах под объектом служебной тайны понимают информацию, имеющую не коммерческую ценность, а ценность иного рода, вытекающую из интересов физических и юридических лиц, государства и общества в целом. Это обстоятельство, а также универсальность функций института служебной тайны позволяют говорить о нем, как об объекте, в установлении правового режима которого заинтересовано государство.

К **категории служебной тайны** может быть отнесена конфиденциальная информация, которая составляет: тайну следствия; тайну судопроизводства; тайну мер безопасности участников уголовного процесса; налоговую тайну; тайну мер безопасности, применяемых в отношении должностных лиц правоохранительных или контролирующих органов.

Кроме того, существует правовой режим служебной информации на рынке ценных бумаг. Он представляет собой особый вид более широкого объекта гражданских прав - информации.

Данный вид тайны особенно важен, поскольку в России более 90% всех коммерческих организаций - хозяйственные общества, а значительная часть из них - акционерные общества. Кроме того, судя по опыту зарубежных стран, фондовый рынок постепенно наберет обороты, и многие граждане будут инвестировать свои средства в ценные бумаги. Исходя из этого, каждый менеджер будет вынужден либо лично, либо опосредованно вовлечен в указанные отношения. И будет активно влиять на эти процессы. Следовательно, уже сейчас необходимо изучать основы этих знаний.

Запрет разглашения служебной тайны основывается на законодательстве, регламентирующем определенные сферы деятельности. Определенные категории работников такой сферы деятельности обязаны сохранять в тайне сведения, к которым они имеют доступ в связи с выполняемой работой.

При правовой оценке служебной информации следует учитывать, что она может иметь различные правовые режимы в зависимости от содержания и назначения использования. Среди таких правовых режимов необходимо рассмотреть следующие: режим общедоступной и открытой информации: режим информации, подлежащей обязательному сообщению; режим информации с ограниченным доступом.

Общедоступной информацией на рынках ценных бумаг признается информация, не требующая привилегий для доступа к ней или подлежащая раскрытию в соответствии с Федеральным законом о рынке ценных бумаг,

Служебная информация является одним из видов информации, обладающей ограниченным доступом. Подчиняясь общим правилам, использование служебной информации на рынке ценных бумаг регламентируется на законодательном уровне посредством установления специальных правил ее использования и распространения.

Федеральный закон о рынке ценных бумаг запрещает использование служебной информации для заключения сделок, а также ее передачу для совершения сделок третьим лицам.

Служебной информацией на рынке ценных бумаг, в соответствии со ст. 31 ФЗ о рынке ценных бумаг, признается любая не являющаяся общедоступной информация об эмитенте и выпущенных им эмиссионных ценных бумагах, которая ставит лиц, обладающих в силу служебного положения, трудовых обязанностей или договора, заключенного с эмитентом, такой информацией, в преимущественное положение по сравнению с другими субъектами рынка ценных бумаг.

К лицам, располагающим служебной информацией, в соответствии с указанным законом, относятся: члены органов управления эмитента или профессионального участника рынка ценных бумаг, связанного с этим эмитентом договором; профессиональные участники рынка ценных бумаг - физические лица; аудиторы эмитента или профессионального участника рынка ценных бумаг, связанного с этим эмитентом договором.

Под членами органа управления эмитента и профессионального участника рынка ценных бумаг - юридического лица - понимаются лица, занимающие постоянно

или временно в этих организациях должности, связанные с выполнением организационно-распорядительных или административно-хозяйственных обязанностей, а также выполняющие такие обязанности по специальному полномочию.

Перечисленные разновидности позволяют дать примерную характеристику содержания объекта данной тайны.

Итак, служебная тайна включает и себя: информацию о следствии и судопроизводстве: мерах безопасности участников уголовного процесса; данные, получаемые в результате деятельности налоговых органов; меры безопасности, применяемые в отношении должностных лиц правоохранительных или контролирующих органов: меры по организации профессиональной деятельности и т. д.

Объект служебной тайны при обстоятельствах, определенных в законном порядке, может включать информацию, составляющую тайну частной жизни граждан, коммерческую и банковскую тайны.

Исходя из вышесказанного, понятие служебной тайны может быть дано в следующем виде. Служебная тайна - это информация, которая имеет действительную или потенциальную служебную либо иную ценность и сохраняется как тайна в силу неизвестности се третьим лицам: к цен нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности, утечка которой может привести к нежелательным последствиям, в том числе и убыткам.

Лекция 9. Создание защищенной системы

Создание защищенной системы - задача комплексная, и решается она путем применения программно-технических методов и средств, а также с помощью организационных мероприятий. Конкретные средства защиты информации реализуют только типовые функции по ее защите, реальная же защитная система строится исходя из возможных угроз и выбранной политики безопасности.

В условиях развивающейся рыночной экономики и самостоятельности ее субъектов все большее значение для российских компаний приобретает защита информации, позволяющая поддерживать конкурентоспособность товаров, организовывать защиту материальных ценностей, снижать риск корпоративного захвата и т. д.

Одним из эффективных средств защиты коммерчески значимой информации является введение в компании режима коммерческой тайны, т. е. принятие правовых, организационных, технических и иных мер по охране конфиденциальности информации.

Несмотря на то, что термин «коммерческая тайна» у всех на слуху, многие руководители и специалисты не в полной мере понимают, что он в действительности означает и как именно добиться сохранения конфиденциальности сведений, составляющих коммерческую тайну.

В соответствии со ст. 3 Федерального закона от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне» под коммерческой тайной понимается конфиденциальность информации, которая позволяет ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Под информацией, составляющей коммерческую тайну в соответствии с указанным законом, понимается научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства — «ноу-хау»), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны. Таким образом, если в организации не введен режим коммерческой тайны, то отсутствует и сама коммерческая тайна.

Любые сведения об организации, полученные законным путем, самостоятельно и добросовестно, из независимых источников, не связанных со служебной деятельностью, коммерческой тайной не являются, как и сведения, сообщаемые самой организацией публично, например в рекламных публикациях, в ходе PR-мероприятий и т. д.

Синдром «повышенной секретности».

Вводя режим коммерческой тайны, многие организации стремятся «засекретить» все что можно, порой создавая анекдотические ситуации. Так, например, в одной из компаний Волгограда в перечне информации, составляющей коммерческую тайну, значатся даже цены на собственные товары. В итоге у работников и партнеров компании складывается впечатление, что работают и сотрудничают они как минимум со сверхсекретной, транснациональной разведывательной организацией.

С одной стороны, комичная история, а с другой — такое состояние дел моментально сказывается на морально-психологическом климате в коллективе: у работников неминуемо возникают нервозность, подозрительность и тому подобные чувства.

Федеральный закон от 29 июля 2004 г. № 98-ФЗ "О коммерческой тайне" в ст. 5 содержит перечень сведений, которые не могут составлять коммерческую тайну. Это информация:

- содержащаяся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;
- содержащаяся в документах, дающих право на осуществление предпринимательской деятельности;
- о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;
- 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 населения в целом;
- о численности, составе работников, системе оплаты и условиях труда (в том числе об охране труда), показателях производственного травматизма и профессиональной заболеваемости, наличии свободных рабочих мест;
- о задолженности работодателя по выплате заработной платы и иным социальным выплатам;
- о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих правонарушений;
- об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;
- о размерах и структуре доходов некоммерческих организаций, размерах и составе их имущества, расходах, численности и оплате труда их работников, использовании безвозмездного труда граждан в деятельности некоммерческой организации;
- о перечне лиц, имеющих право действовать без доверенности от имени юридического лица.

Такова информация, обязательность раскрытия которой или недопустимость ограничения доступа к которой установлена федеральными законами.

Что касается перечня сведений, составляющих коммерческую тайну, то он законодательно не определен и должен устанавливаться каждой организацией, вводящей режим коммерческой тайны, самостоятельно, исходя из специфики бизнеса и особенностей самой компании. Исходя из практического опыта в области разработки положений о коммерческой тайне, можно привести следующий примерный перечень:

- информация об условиях сотрудничества (порядок, форма оплаты, предоставляемые скидки, условия доставки и т. д.) с действительными и потенциальными контрагентами, а также информация, составляющая базу данных о контрагентах организации, включая их наименования, адреса, банковские, почтовые, телефонные, телеграфные, отгрузочные и другие реквизиты, имена руководителей, главных бухгалтеров и других должностных лиц, а также их контактные телефоны;

- информация о сделках (текущих и планируемых), включая сведения о предварительных переговорах, условиях договоров и любых дополнениях к ним, порядке заключения и исполнения договоров, а также о достигнутых результатах по сделкам;

- данные оперативного бухгалтерского учета и регистры бухгалтерского учета, включая содержание аналитических счетов и проводок;

- бухгалтерские и планово-финансовые документы, а также выписки из документов, копии, дубликаты, дополнения и приложения, включая финансовые планы, сметы, лимиты, нормативы и т. д.;

- документы внутреннего и внешнего делопроизводства, а также выписки из документов, копии, дубликаты, дополнения и приложения, включая:

а) организационные документы (структуры, процедуры, положения, документы системы менеджмента качества);

б) распорядительные документы (приказы, распоряжения и указания, инструкции, задания, поручения, требования;

в) информационно-справочные документы (протоколы, акты, отчеты, планы, программы, обзоры, сводки, перечни и т. д.);

сведения, раскрывающие содержание программ обучения, программ и материалов семинаров, курсов, методических материалов, предназначенных для служебного пользования, и т. д.;

- детализированные сведения об имуществе, в том числе его стоимости, включая информацию о наличии денежных средств на расчетном счете, а также дебиторской и кредиторской задолженности;

- сведения, содержащие информацию о методах, средствах и способах анализа конъюнктуры рынка, а также данные (полученные и расчетные) по проведенному анализу (спроса, предложения и конкуренции), ценовой политике и планированию цен, анализу потребителей, планированию сбыта и продвижения товаров (услуг), определению стратегии и тактики коммерческой деятельности предприятия;

- информация о методах и средствах поиска новых контрагентов и партнеров (покупателях, поставщиках, посредниках и т. д.);

- информация о содержании телефонных переговоров, переписки, факсимильных и иных сообщений, имеющих отношение к хозяйственной деятельности компании. Информация о содержании непосредственных переговоров в устной или любой письменной форме, проводимых администрацией и сотрудниками с действительными или потенциальными партнерами и контрагентами;

- информация о краткосрочных и долгосрочных планах, направлениях и прогнозах развития;

- сведения, раскрывающие систему, средства и методы обработки и защиты информации от несанкционированного доступа на средствах вычислительной техники, а также значения действующих кодов, шифров и паролей;

- сведения, раскрывающие организацию, средства и методы обеспечения безопасности компании, охраны ее имущества, а также жизни и здоровья ее сотрудников;

- сведения о проектировании, разработке, сооружении, установке и эксплуатации специальных охранных средств, средств пропуска и безопасности;

- сведения о местах расположения, назначении, степени готовности или защищенности объектов (земельных участков, зданий, помещений, складов, гаражей, офисов, кабинетов, подсобных помещений и др.), составляющих инфраструктуру компании, а также сведения о планируемых или проводимых изыскательских работах по созданию, приобретению, аренде или переоборудованию таких объектов;

- сведения о юридических лицах и индивидуальных предпринимателях, их коммерческой деятельности, полученные сотрудниками организации законным путем в процессе

организационного, экономического, коммерческого или иного мониторинга и анализа.

К конфиденциальным сведениям, составляющим коммерческую тайну, может быть отнесена и иная информация, связанная с хозяйственной деятельностью организации, разглашение которой может причинить вред ее интересам.

Создавая и вводя режим коммерческой тайны, важно четко определить, конфиденциальность каких сведений необходимо охранять. Засекречивание лишней информации будет создавать неудобства в работе и порождать лишний документооборот, связанный с получением разрешения у руководителя (либо начальника службы безопасности) на использование сведений, составляющих коммерческую тайну.

Кроме того, перед тем как создавать и вводить режим коммерческой тайны, необходимо оценить, насколько он вообще актуален для компании в данный момент.

Также важно помнить, что введение режима коммерческой тайны не может быть причиной отказа в предоставлении соответствующей информации по мотивированному требованию государственных (муниципальных) следственных, судебных, контрольно-надзорных, статистических и иных органов.

Руководство по введению режима коммерческой тайны.

Для того чтобы ввести в организации *режим коммерческой тайны*, необходимо разработать определенный пакет документов и провести ряд организационных мероприятий.

Во-первых, следует четко определить в виде перечня совокупность сведений конфиденциального характера, которые будут составлять коммерческую тайну организации.

Во-вторых, необходимо определить в виде положения, каким образом будет осуществляться защита коммерческой тайны, как будут маркироваться ее носители, кто будет иметь право с ними работать, как это будет учитываться, на кого будет возложена функция контроля, какова будет ответственность за разглашение коммерческой тайны и т. д.

В-третьих, на основе разработанных документов следует внести соответствующие изменения в должностные инструкции, положения об отделах (структурных подразделениях) и иную организационно-распорядительную документацию компании. В договоры с контрагентами необходимо внести пункт о том, что все сведения, связанные с договором и его исполнением, являются конфиденциальными и подлежат передаче и разглашению третьим лицам (за исключением государственных

(муниципальных) контрольно-надзорных, судебных и других органов) только по обоюдному соглашению сторон.

В-четвертых, необходимо обеспечить ознакомление под роспись всех сотрудников организации (работающих в настоящее время и вновь принимаемых) с разработанными и вводимыми документами и взять у каждого письменное обязательство по сохранению конфиденциальности составляющих коммерческую тайну сведений, которые стали известны в процессе работы в организации.

В этом документе желательно указать обязанность по неразглашению коммерческой тайны как во время работы в организации, так и в течение определенного времени после увольнения.

В-пятых, следует создать работникам все необходимые условия для соблюдения установленного компанией режима коммерческой тайны. Как правило, такими условиями являются создание возможности хранить документы, содержащие конфиденциальные сведения в запираемом месте, обеспечение доступа к персональному компьютеру, локальной сети и сети Интернет по персональному логину и паролю и т. д.

В-шестых, весьма желательно сразу после введения режима коммерческой тайны, а также в дальнейшем проводить с работниками обучающие мероприятия, в процессе которых рассказывать и объяснять, зачем нужен режим коммерческой тайны, в чем он состоит и т. д. Полезно также раздать сотрудникам памятки о важности сохранения коммерческой тайны организации. Необходимость данных мероприятий обусловлена тем, что многие работники порой с трудом воспринимают новшества, вводимые руководством компании. Кроме того, следует помнить, что наличие подписи работника на листе ознакомления с положением о коммерческой тайне (перечне сведений, обязательстве) не гарантирует понимания сути и важности данных документов, а также серьезного к ним отношения.

Практика показывает, что защита конфиденциальных сведений, составляющих коммерческую тайну, равно как и интересов фирмы в целом, наилучшим образом осуществляется, когда каждый работник четко понимает требования, содержащиеся в организационно-распорядительных документах компании, и осознает важность их выполнения.

В подобном случае можно говорить о наличии в коллективе высокой деловой и правовой культуры, корпоративного режима

конфиденциальности и быть уверенным, что интересы фирмы защищены наилучшим образом.

Последствия разглашения.

Общие последствия незаконного получения и разглашения конфиденциальных сведений, составляющих коммерческую тайну, определены действующим законодательством.

В соответствии с ч. 2. ст. 139 Гражданского кодекса РФ лица, незаконными методами получившие информацию, которая составляет служебную или коммерческую тайну, обязаны возместить причиненные убытки. Такая же обязанность возлагается на работников, разгласивших служебную или коммерческую тайну вопреки трудовому договору, в том числе контракту, и на контрагентов, сделавших это вопреки гражданско-правовому договору.

В соответствии с подп. «в» п. 6 ст. 81 Трудового кодекса РФ работодатель имеет право расторгнуть трудовой договор с работником в случае разглашения последним сведений, составляющих коммерческую тайну.

Кроме того, возможна и уголовная ответственность лиц, виновных в незаконном получении и разглашении сведений, составляющих коммерческую тайну, в соответствии со ст. 183 Уголовного кодекса РФ.

Подводя итоги, важно отметить следующие ключевые моменты:

- под коммерческой тайной понимаются защищаемые организацией путем введения режима коммерческой тайны сведения, имеющие потенциальную или действительную коммерческую ценность, представляющие собой конфиденциальную информацию, связанную с хозяйственной деятельностью компании, разглашение которой третьим лицам может нанести ущерб ее интересам;

- введение режима коммерческой тайны позволяет эффективно защищать конфиденциальность сведений, имеющих для компании коммерческую ценность. Отсутствие в организации режима коммерческой тайны по смыслу законодательства означает отсутствие самой коммерческой тайны;

- введение режима коммерческой тайны обязательно сопряжено с разработкой соответствующего пакета документов и проведением определенных организационных мероприятий;

- необходимо ознакомление под роспись всех сотрудников с документами, регламентирующими порядок охраны коммерческой тайны компании, желательно проведение обучающих занятий для

сотрудников с целью формирования корпоративной культуры конфиденциальности;

- за незаконное получение и разглашение коммерческой тайны наступает ответственность в соответствии с действующим законодательством.

Лекция 10. Категорирование конфиденциальной информации

Владение информацией о конкуренте – один из наиболее действенных способов конкурентной борьбы на рынке. Необходимость решения проблемы утечки конфиденциальной информации связана с выживанием и успешным ведением бизнеса компании.

Ущерб от раскрытия конфиденциальной информации может выражаться в потере конкурентных преимуществ, упущенной коммерческой выгоде, санкциях со стороны регулирующих органов, административной и уголовной ответственности за раскрытие персональных данных, ухудшении морального климата в коллективе вследствие раскрытия информации о заработной плате работников, планируемых кадровых перестановках и т. п. Например, американская компания Victoria Secrets была оштрафована на 50 тыс. долл. за то, что не обеспечила надлежащей защиты своего Web-сайта электронной коммерции, в результате чего пострадали 560 клиентов, персональные данные которых оказались скомпрометированными.

Несмотря на то что несанкционированное раскрытие информации является во многих случаях административно и уголовно наказуемым деянием, в условиях, когда информационное законодательство РФ еще полностью не сформировано, а процессы законотворчества сильно отстают от уровня развития информационных технологий, возникают существенные трудности в обеспечении юридической защиты интересов собственников конфиденциальной информации. Однако приемлемое решение всегда существует, и поиск этого решения должен осуществляться в рамках стандартной схемы «объекты – угрозы – контрмеры».

Состав сведений с грифом «конфиденциальная информация» варьируется в зависимости от предприятия и должен приводиться в «Перечне сведений ограниченного распространения», который утверждается руководителем организации. Информация, не попавшая в данный перечень, считается открытой. Опираясь на опыт защиты информации в коммерческих организациях и

положения действующего законодательства, можно выделить следующие основные категории конфиденциальной информации:

- сведения, составляющие коммерческую тайну организации;
- персональные данные сотрудников организации (информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника);
- сведения, составляющие конфиденциальную информацию третьих лиц (партнеров, клиентов, подрядчиков, контрагентов);
- любые другие сведения, разглашение и/или неправомерное использование которых может нанести ущерб интересам организации.

К *открытой информации* относятся, например, сведения:

- содержащиеся в сообщениях и отчетах, официально опубликованных компанией в соответствии с действующим российским законодательством;
- содержащиеся в официальных пресс-релизах, а также рекламных сообщениях компании;
- опубликованные в средствах массовой информации по инициативе третьих лиц и с разрешения руководства компании;
- любая информация, не попадающая в категории, определяемые «Перечнем сведений ограниченного распространения», принятым в организации, и не являющаяся конфиденциальной по законодательству РФ.

В коммерческой организации наиболее остро стоит вопрос о защите коммерческой тайны, однако не менее важными являются сведения, составляющие конфиденциальную информацию третьих лиц, к которым могут относиться коммерческая тайна третьих лиц, персональные данные, служебная тайна и т. п., включая государственную тайну.

Важной категорией конфиденциальной информации являются персональные данные сотрудников организации. Например, в США законодательство предусматривает строгое наказание за раскрытие персональных данных граждан. Соответствующие вопросы отражены в Privacy Act и HIPPA, последний определяет наказание до десяти лет лишения свободы или 200 тыс. долл. штрафа за умышленное раскрытие персональных данных.

В нашей стране вопросы защиты персональных данных пока недостаточно хорошо проработаны как на законодательном, так и на технологическом уровне. Однако правовая база все же была заложена в законе РФ «Об информации, информатизации и защите информации».

Помимо определения состава конфиденциальных сведений, информационные ресурсы организации нуждаются также в категорировании по уровню конфиденциальности. Это позволяет ввести дифференцированный подход к реализации защитных мер. Знания о составе информационных ресурсов организации и соответствующих уровнях конфиденциальности формализуются в виде единого «Реестра информационных ресурсов организации».

Каналы утечки информации.

Количество потенциальных каналов утечки информации достаточно велико. Наиболее распространенные из них относятся к категории неумышленного раскрытия информации сотрудниками по причине неосведомленности или недисциплинированности. Отсутствие представлений о правилах работы с конфиденциальными документами, неумение определить, какие документы являются конфиденциальными, и просто обычные разговоры между сотрудниками — все это может привести к рассекречиванию данных.

Умышленный «слив» информации встречается значительно реже, зато осуществляется целенаправленно и с наиболее опасными последствиями для организации.

Хорошим примером утечки конфиденциальной информации из организации из-за технической неосведомленности сотрудников может служить ситуация, возникающая вокруг повсеместно используемого текстового редактора MS Word. По данным британской компании Workshare, специализирующейся в области обеспечения защиты документов, текстовый редактор Word компании Microsoft сам по себе представляет огромную опасность. Речь идет о заложенной в нем возможности извлечения информации, вносившейся в документ по ходу его подготовки, правки и согласования, пусть даже удаленной впоследствии. Внимательный читатель, недобросовестный конкурент или мошенник могут, если не предпринять определенные меры, почерпнуть немало интересного о том, как, к примеру, варьировались по мере подготовки финального текста контракта его ключевые положения.

По данным консалтинговой компании Vanson Bourne, в целом до 31% файлов в формате Word содержат весьма «щекотливую» информацию. В некоторых компаниях дела обстоят особенно неблагополучно – до трех четвертей всех документов попадают в группу «высокого риска». Больше того, 90% компаний не имеют ни малейшего представления о том, каким именно образом уже

утекает или может утекать от них закрытая и служебная информация.

Компания Microsoft выпустила специальное программное расширение для MS Word под названием Remove Hidden Data, с помощью которого пользователь может удалить персональные данные либо скрытую информацию, которая не должна быть выявлена при просмотре документа. Однако очень немногие организации добавили соответствующие правила «зачистки» в существующие регламенты работы с документами.

Система мер по защите.

С учетом множественности категорий и каналов утечки информации становится очевидно, что в большинстве случаев проблему утечки нельзя решить каким-либо простым способом, тем более избавиться от нее окончательно. Кроме того, реализация любых мер по ограничению доступа к информации или ее распространению потенциально снижает эффективность основных бизнес-процессов организации. Это означает, что требуется система организационно-технических мероприятий, позволяющих перекрыть основные каналы утечки информации с определенной степенью надежности и минимизировать существующие риски без значительного снижения эффективности бизнес-процессов. Без такой системы права на юридическую защиту интересов организации как собственника информации нереализуемы.

Система предотвращения утечки конфиденциальной информации включает в себя три основных составляющих: работу с персоналом, политику безопасности, сервисы безопасности.

Работа с персоналом.

Основным источником утечки информации из организации является ее персонал. Человеческий фактор способен «свести на нет» любые самые изощренные механизмы безопасности. Это подтверждается многочисленными статистическими данными, свидетельствующими о том, что подавляющее большинство инцидентов безопасности связано с деятельностью сотрудников организации. Неудивительно, что работа с персоналом — главный механизм защиты.

Ключевые принципы и правила управления персоналом с учетом требований информационной безопасности определены в международном стандарте ISO/IEC 17799:2000 и сводятся к необходимости выполнения определенных требований

безопасности, повышения осведомленности сотрудников и применения мер пресечения к нарушителям.

Основные требования.

При работе с персоналом необходимо соблюдать следующие требования безопасности:

Ответственность за информационную безопасность должна быть включена в должностные обязанности сотрудников, включая ответственность за выполнение требований политики безопасности, за ресурсы, процессы и мероприятия по обеспечению безопасности.

Должны проводиться соответствующие проверки сотрудников при приеме на работу, включая характеристики и рекомендации, полноту и точность резюме, образование и квалификацию, а также документы, удостоверяющие личность. Для критичных должностей должна проверяться также кредитная история кандидата.

Подписание соглашения о неразглашении конфиденциальной информации кандидатом должно быть обязательным условием приема на работу. Требования информационной безопасности, предъявляемые к сотруднику, должны быть отражены в трудовых соглашениях. Там же должна быть прописана ответственность за нарушение безопасности.

Повышение осведомленности.

Важную роль для обеспечения информационной безопасности играет осведомленность пользователей в вопросах безопасности и правилах безопасного поведения. Согласно ст. 139 Гражданского кодекса РФ, обладатель конфиденциальной информации имеет право на правовую защиту от незаконного ее использования только при условии, что он принимает надлежащие меры к соблюдению ее конфиденциальности, поэтому правила политики безопасности и ответственность, предусмотренная за их нарушение, должны быть документированы и доведены до сведения всех сотрудников под роспись. Контроль осведомленности должен осуществляться на регулярной основе. Основную роль здесь играют HR-менеджеры организации.

Необходимо проводить обучение и контролировать знания пользователей по следующим вопросам:

- правила политики безопасности организации;
- правила выбора, смены и использования паролей;
- правила получения доступа к ресурсам информационной системы;

- правила обращения с конфиденциальной информацией;
- процедуры информирования об инцидентах, уязвимостях, ошибках и сбоях программного обеспечения и др.

Меры пресечения.

В организации должен быть разработан соответствующий дисциплинарный процесс, проводимый в отношении нарушителей безопасности и предусматривающий расследование, ликвидацию последствий инцидентов и адекватные меры воздействия.

При определении мер пресечения следует ориентироваться на положения действующего законодательства. Отношения между работником и работодателем и ответственность за нарушение информационной безопасности организации регулируются прежде всего Трудовым кодексом РФ. В определенных случаях возможно применение положений Кодекса об административных правонарушениях и Уголовного кодекса.

Так, на основании ст. 192 Трудового кодекса РФ сотрудники, нарушающие требования политики безопасности организации, могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговор и увольнение с работы за неоднократное грубое нарушение дисциплины. Согласно ст. 238 Трудового кодекса РФ все сотрудники несут персональную (в том числе материальную) ответственность за прямой действительный ущерб, причиненный компании в результате нарушения ими правил политики безопасности. Сотрудник компании несет материальную ответственность как за прямой действительный ущерб, непосредственно причиненный им работодателю, так и за ущерб, возникший у работодателя в результате возмещения им ущерба иным лицам. Сотрудники несут материальную ответственность в пределах своего среднего месячного заработка (ст. 241 Трудового кодекса РФ). Согласно ст. 243 Трудового кодекса РФ, за умышленное причинение ущерба, а также за разглашение сведений, составляющих охраняемую законом тайну (служебную, коммерческую или иную), в случаях, предусмотренных федеральными законами, сотрудники компании несут материальную ответственность в полном размере причиненного ущерба.

Роль HR-менеджеров.

Роль менеджеров по персоналу в обеспечении информационной безопасности организации весьма значима, хотя и не является определяющей. HR-менеджеры должны принимать участие в разработке и внедрении политик безопасности, организации обучения пользователей, контроле осведомленности и

расследовании нарушений. HR-менджеры в организации также выполняют функции владельцев персональных данных сотрудников компании и несут административную ответственность за разглашение или незаконное распространение этих данных.

Соответствующая организация процесса внутрифирменной коммуникации, позволяет избежать утечек информации и ненадлежащего ее использования. Она включает в себя определение уровней доступа к информации, механизмов контроля и функциональных ролей.

В организации должно быть разработано положение по защите конфиденциальной информации и соответствующие инструкции. Эти документы должны определять правила и критерии для категорирования информационных ресурсов по степени конфиденциальности (например, открытая информация, конфиденциальная, строго конфиденциальная), правила маркирования конфиденциальных документов и правила обращения с конфиденциальной информацией, включая режимы хранения, способы обращения, ограничения по использованию и передаче третьей стороне и между подразделениями организации.

Должны быть определены правила предоставления доступа к информационным ресурсам, внедрены соответствующие процедуры и механизмы контроля, в том числе авторизация и аудит доступа.

Ответственность за информационную безопасность организации несет ее руководитель, который делегирует эту ответственность одному из менеджеров. Обычно эти функции выполняет директор по информационной безопасности (CISO) или директор по безопасности (CSO), иногда директор информационной службы (CIO).

Решение о предоставлении доступа к конкретным информационным ресурсам должны принимать владельцы этих ресурсов, назначаемые из числа руководителей подразделений, формирующих и использующих эти ресурсы. Кроме того, вопросы предоставления доступа конкретным сотрудникам должны быть согласованы с их непосредственными руководителями.

Многие правила политики безопасности понятны сотрудникам и выполняются ими в большинстве случаев на интуитивном уровне. Остальные требуют обучения.

Жизнь по правилам.

Как показывает практика, значительного ограничения утечки информации из организации можно добиться путем применения шести основных правил. Основная задача состоит в том, чтобы добиться интуитивного применения этих правил всеми сотрудниками организации.

Правило №1. Маркирование документов.

Документы (бумажные и электронные), содержащие конфиденциальную информацию, подлежат обязательному маркированию путем проставления грифа конфиденциальности в правом верхнем углу титульного листа.

Маркирование конфиденциальных документов осуществляется ответственным за их подготовку или ответственным за работу с данными документами. Маркирование сообщений электронной почты осуществляется пользователем, выполняющим отправку (распространение) данных сообщений.

В документах, содержащих конфиденциальную информацию и передаваемых третьей стороне, на обороте титульного листа в обязательном порядке должно быть «заявление о конфиденциальности».

Правило №2. Закрытое обсуждение.

Не следует обсуждать конфиденциальную информацию с посторонними лицами (или в их присутствии), с друзьями, родственниками, сотрудниками организации, не допущенными к работе с данной информацией, и т. п. Также не следует обсуждать конфиденциальную информацию в общественных местах в присутствии посторонних (не допущенных к данной информации) лиц, включая столовую и места для курения, расположенные на территории компании.

Правило №3. Шифрование информации при хранении и передаче.

Для обеспечения надлежащего уровня защиты шифрование должно применяться как при хранении, так и при передаче конфиденциальной информации. Электронный обмен конфиденциальной информацией с внешними респондентами должен вестись в зашифрованном виде, при наличии соответствующих технических возможностей.

Правило №4. Использование соглашения о конфиденциальности.

Передача сведений, содержащих конфиденциальную информацию, третьей стороне должна осуществляться только после заключения с этой стороной «Соглашения о конфиденциальности».

Правило №5. Ограничение доступа к информации.

Не хранить электронные документы, содержащие конфиденциальную информацию, в общедоступных местах, включая общие папки файловых серверов, Web, почтовые папки и т. п.

Правило №6. Информирование.

Требуется не только самим овладеть методами защиты информации, но также следить за их выполнением другими сотрудниками и вести разъяснительную работу. Обо всех фактах утечки информации следует незамедлительно сообщать своему непосредственному руководителю.

Сервисы безопасности.

Сервисы безопасности используются для ограничения доступа к информации, протоколирования фактов осуществления доступа и контроля информационных потоков. Они позволяют обеспечить предупреждение, предотвращение, обнаружение и реагирование на инциденты, связанные с утечкой информации.

К числу сервисов безопасности относят аутентификацию, управление доступом, шифрование, фильтрацию контента и аудита безопасности.

Аутентификация и управление доступом. Традиционные схемы аутентификации и управления доступом во многих случаях уже не обеспечивают адекватного уровня защиты. В дополнение к ним целесообразно использовать специализированные сервисы управления правами доступа к электронным документам, которые уже начинают появляться на рынке.

Примерами соответствующих коммерческих продуктов являются Microsoft RMS (впервые появившийся в Windows Server 2003) и программно-аппаратный комплекс Sentinel RMS, производимый компанией SafeNet.

RMS (Rights Management Services, сервисы управления правами доступа) – это технология, используемая для защиты электронных документов от несанкционированного использования. Она позволяет при распространении информации определять ограничения по использованию последней. Например, автор документа может ограничить «время жизни» документа, а

также возможность для определенных пользователей открывать, изменять, копировать в буфер обмена, печатать или пересылать документ. Основное отличие данной технологии от традиционных способов разграничения доступа к информации заключается в том, что права доступа и дополнительные ограничения по использованию хранятся в теле самого документа и действуют независимо от его местонахождения. Шифрование документов, реализованное в технологии RMS, не позволяет получать доступ к их содержанию каким-либо обходным путем.

Фильтрация контента. Использование RMS, конечно, не решает всех проблем. Например, эта технология не защищает от умышленного «слива» информации по электронной почте, что на практике встречается довольно часто, и заставляет руководство организации вводить правила по фильтрации исходящих из корпоративной сети сообщений по их содержанию. Анализ содержания сообщений по ключевым словам может быть достаточно эффективным, однако требует проведения серьезной работы по «тюнингу» системы фильтрации контента, так как ни одна из подобных систем не работает «прямо из коробки». Даже хорошо отлаженная система фильтрации требует постоянного внимания со стороны администратора безопасности.

Шифрование информации. Шифрование — один из наиболее надежных способов обеспечения конфиденциальности информации. Криптографические методы давно и успешно развиваются во всем мире, поэтому в настоящее время механизмы шифрования являются сильным звеном в любой системе обеспечения информационной безопасности.

Так, например, доступный и распространенный способ шифрования информации при хранении для пользователей ОС Microsoft Windows — применение встроенного в NTFS сервиса Encrypted File System (EFS). Во всех распространенных почтовых клиентах поддерживаются функции шифрования сообщений, что позволяет без дополнительных усилий производить обмен конфиденциальной информацией с внешними респондентами в зашифрованном виде.

Аудит безопасности. Последним рубежом в комплексной системе предотвращения утечки информации из организации является подсистема аудита информационной безопасности, которая позволяет оперативно обнаруживать и реагировать на нарушения безопасности, а также производить расследование инцидентов, связанных с утечкой информации. Она должна охватывать все виды событий, связанных с получением доступа к конфиденциальным данным и выполнением действий, способных

привести к их несанкционированному раскрытию, включая изменение прав доступа, копирование и вывод на печать.

СУИБ. Успешная реализация намеченных подходов к предотвращению утечки информации крайне затруднительна в том случае, если в организации отсутствует действующая система управления информационной безопасностью (СУИБ), которая характеризуется прежде всего наличием работающей политики безопасности и организационной структуры, выстроенной в соответствии с этой политикой, а также наличием процессов, процедур и механизмов контроля. Основными руководящими документами в этой области могут служить международный стандарт ISO/IEC 17799:2000, который описывает 127 механизмов контроля, обеспечивающих функционирование СУИБ, а также британский стандарт BS 7799-2:2002, определяющий спецификацию СУИБ, руководство по ее использованию для создания СУИБ и прохождения процедуры сертификации.

Лекция 11. Действующее информационное законодательство

Действующее информационное законодательство Российской Федерации представлено целым блоком нормативно-правовых актов самого различного уровня, начиная с Конституции, Гражданского, Уголовного и Административного кодекса РФ и заканчивая узкоспециализированными, фундаментальными источниками, регулирующими вопросы защиты информации. К последним относятся законы РФ «Об информации, информатизации и защите информации», «Об участии в международном информационном обмене», вступивший в силу с 24 декабря 2004 года «Закон о коммерческой тайне». На рассмотрении в Государственной думе в настоящее время находится еще ряд проектов законов, включая законы о защите персональной и служебной информации.

Однако большой объем актов правового регулирования и наличие основополагающих профильных нормативных актов не означают совершенства действующего законодательства в этой сфере. Сегодняшние законодательство и наука не позволяют четко отграничить информацию от других объектов права, установить ее правовую природу, обозначить круг информационных правоотношений, однозначно определить субъектный состав и содержание информационных отношений и т. д. В частности, своего скорейшего разрешения требует проблема правового регулирования оборота недокументированной информации.

Законодательство о защите коммерческой тайны. Предметом защиты коммерческой информации являются все свойственные предприятиям компании особенности и детали коммерческой деятельности, деловые связи, закупка сырья и товаров, сведения о поставщиках, предполагаемой прибыли, методики установления цен, результаты маркетинговых исследований, счета, договоры и т. п.

По гражданскому законодательству (ст. 139 Гражданского кодекса РФ) обладатель технической, организационной или коммерческой информации, составляющей секрет производства, имеет правовую защиту от незаконного ее использования при условии, что:

- информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам;
- к информации нет свободного доступа на законном основании;
- обладатель информации принимает надлежащие меры к соблюдению ее конфиденциальности.

Отношения, возникающие между субъектами гражданского общества, связанные с отнесением информации к коммерческой тайне, передачей такой информации и охраной ее конфиденциальности, регулируются законом «О коммерческой тайне». Согласно этому закону права обладателя информации, составляющей коммерческую тайну, возникают с момента установления им в отношении такой информации режима коммерческой тайны, под которым понимаются «правовые, организационные, технические и иные принимаемые обладателем информации, составляющей коммерческую тайну, меры по охране ее конфиденциальности».

Нормативные документы. В основе системы защиты информации лежат внутренние нормативные документы, устанавливающие ответственность и определяющие правила по защите информации, обязательные для исполнения всеми сотрудниками организации. К ним относятся: положение о коммерческой тайне; руководство по защите конфиденциальной информации; правила работы пользователей в корпоративной сети; инструкции по использованию сервисов безопасности; регламент предоставления доступа к информационным ресурсам.

Хорошей практикой является разработка и внедрение нескольких небольших документов вместо одного объемного, который все равно никто не сможет дочитать до конца и тем более запомнить все, что там написано. Можно рекомендовать

следующий состав документов, ориентированных на всех сотрудников организации:

- правила работы пользователей в корпоративной сети;
- правила выбора, хранения и использования паролей;
- инструкция по защите от компьютерных вирусов;
- правила использования мобильных устройств для работы в корпоративной сети;
- правила работы в сети Internet.

Состав документов может варьироваться. При определении состава и содержания документов можно опираться на требования ISO/IEC 17799:2000.

Лекция 12. Каналы утечки сведений составляющих коммерческую тайну предприятия

После определения сведений, составляющих коммерческую тайну предприятия, предстоит разработать и осуществить мероприятия по обеспечению их сохранности.

Сущность защитных мероприятий сводится к перекрытию возможных каналов утечки защищаемой информации, которые появляются в силу объективно складывающихся условий ее распространения и возникающей у конкурентов заинтересованности в ее получении.

Следует исходить из того, что научные, научно-производственные и учебные центры нашей страны, в которых ведутся фундаментальные и прикладные НИР и НИОКР, уже в течение продолжительного времени являются объектами постоянного интереса иностранных частных фирм и организаций. При этом особое значение придается НИОКР, результаты которых открывают новые направления в развитии науки и техники и могут быть использованы в создании принципиально новых изделий и технологических процессов в различных отраслях промышленности. Известно, что особую роль в НТП играют фундаментальные исследования. Именно они первоисточник радикального обновления и расширения номенклатуры выпускаемой продукции. В результате фундаментальных исследований появился целый ряд новых областей техники и промышленности, атомная техника и промышленность, ракетно-космическая техника, ВТ, полупроводниковая техника, микроэлектроника, лазеры, микробиологическая промышленность, новые материалы, искусственные алмазы и пр. Именно фундаментальные исследования становятся источником новых

оригинальных решений, которые появляются в процессе их проведения.

Следует также ожидать, что по мере развития у нас рыночных отношений и расширения внешнеэкономических связей предприятий у иностранных партнеров и конкурентов появятся устремления к сведениям о планах предприятий, их финансовом положении, методах управления, рыночной стратегии и др. упоминавшихся нами структурных элементах коммерческой тайны. Кроме того, возникновение конкуренции между предприятиями внутри государства породит и между ними подобные взаимные устремления.

Для построения системы защиты коммерческой тайны предприятия очень важно определить источник и соответствующие им возможные официальные каналы утечки защищаемой информации. На каждом конкретном предприятии перечень таких каналов носит индивидуальный характер, что определяется спецификой его производственной, научно-технической, коммерческой и иной деятельности и степенью развития связей с деловыми партнерами внутри государства и за рубежом.

Может быть полезным следующий обобщенный перечень официальных каналов передачи информации за границу, в который входят:

- публичные лекции по научно-технической тематике, организуемые разными обществами;
- пресс-конференции ведущих специалистов, видных ученых и инженеров для отечественных и иностранных корреспондентов;
- чтение лекций на различных курсах для иностранцев, организуемых по соглашению с международными организациями на территории России и за рубежом, а также в зарубежных учебных заведениях;
- обучение иностранных студентов и аспирантов в вузах России;
- обучение иностранных специалистов эксплуатации экспортированного из России оборудования или сооружаемых за рубежом объектов;
- выступления отечественных специалистов с докладами и в дискуссиях на международных конгрессах, конференциях и симпозиумах, проводимых в России и за рубежом;
- публичная защита открытых диссертаций на соискание ученых степеней;
- передача информации в процессе общения с иностранными журналистами, аккредитованными в России;

- демонстрация научно-технических фильмов;

- демонстрация действующих объектов научно-технических достижений (оборудования, изделий, технологий) на предприятиях;

- демонстрация научно-технических достижений на выставках;

- все виды рекламы экспортной продукции в форме печатных произведений – брошюр, пристендовой литературы для выставок и ярмарок;

- международный обмен научно-технической литературой (книгами, журналами), осуществляемый библиотеками и отдельными научными учреждениями с библиотеками и другими организациями зарубежных стран в соответствии с заключенными между ними соглашениями;

- обмен с зарубежными научными организациями отчетами о НИОКР в соответствии с соглашениями, в т.ч. межправительственными, о научно- техническом сотрудничестве или о совместном выполнении исследований и разработок;

- публикация отечественными специалистами и учеными научных, технических и др. материалов в зарубежных и международных изданиях;

- передача технической документации (в т.ч. товаросопроводительной) иностранным фирмам (организациям) при выполнении экспортных операций, включая проектирование и строительство объектов за рубежом, а также продажу лицензий;

- передача информации при переписке отечественных учреждений и отдельных специалистов с зарубежными научными учреждениями и специалистами;

- вывоз за границу книг и журналов научно-технического и экономического характера, а также газет гражданами, выезжающими за границу в командировки, по линии туризма или по частным делам;

- книготорговля внутри страны, обеспечивающая свободный доступ ко всем открытым научно-техническим изданиям, поступающим в книжные магазины и киоски;

- библиотечное обслуживание иностранных граждан в массовых и специальных научных и научно-технических библиотеках страны;

- передача сведений представителям иностранных фирм в процессе переговоров или при заключении экспортных или импортных соглашений;

- прием иностранных специалистов в научных учреждениях, в вузах и на предприятиях;

- проведение совместных разработок (проектов, экспериментов) в рамках осуществления научно-технических связей.

Каждый из вышеуказанных каналов характеризуется весьма значительными объемами передачи информации за рубеж.

Так, ежегодно только по книгообмену в промышленно развитые страны отправляются сотни тысяч экземпляров изданий: книги, журналы, выпуск продолжающихся изданий. Значительное число наших библиотек, научных учреждений и организаций осуществляют книгообмен с различными зарубежными организациями, в т.ч. с научными учреждениями, издательствами и редакциями, библиотеками, университетами и вузами, промышленными фирмами, международными организациями и музеями.

На Западе постоянно изучаются отечественные открытые публикации, в т.ч. узкоотраслевые научно-технические журналы, справочники, специальная литература и др. издания, а также материалы международных конференций, симпозиумов, семинаров и т.п. и проводимых внутри страны.

Анализ материалов, поступающих по открытым каналам, позволяет иностранным экспертам выявлять в них сообщения о разработанных у нас в стране приоритетных достижениях науки, техники и технологии и др. военную информацию. Нередко иностранные фирмы, отказавшись по тем или иным причинам от приобретения лицензий на наши изобретения, выступают затем как инициаторы научно-технического сотрудничества по этой тематике.

Для сбора интересующей информации фирмы промышленно развитых стран используют и различные приемы.

Например, на проводимых у нас в стране или за рубежом международных выставках представители фирм пытаются путем опроса и анкетирования наших специалистов получить подробную информацию об их месте работы, тематике проводимых ими исследований и разработок.

Проведенный обзор официальных каналов передачи информации за границу поможет трансформировать их применительно к условиям предприятия, определить степень их уязвимости с точки зрения утечки сведений, составляющих коммерческую тайну, и внедрить соответствующие мероприятия по обеспечению требуемого режима их безопасности. Но этим задача защиты коммерческой тайны предприятия не исчерпывается.

Помимо рассмотренных открытых каналов утечки информации могут существовать еще агентурный и технологический, организация работы по перекрытию которых носит сугубо специфический характер.

Относительно государственных секретов эту работу выполняют специальные органы государства, режимно-секретные подразделения предприятий.

Что же касается коммерческой тайны, то организация ее защиты от утечки в комплексе по всем каналам, включая агентурный и технологический, целиком и полностью ложится на предприятие.

Как свидетельствует зарубежный опыт, для этого в зависимости от объема и сложности решаемых на данном участке задач может быть эффективным создание специального подразделения, например, службы безопасности.

Лекция 13. Мероприятия по защите коммерческой тайны предприятия

Создание надежного механизма защиты коммерческой тайны требует проведения хорошо продуманных мероприятий. План их осуществления должен преследовать три цели:

- предотвращать кражу;
- дать всем понять, что для вас коммерческая тайна очень важна и что вы приложите все усилия для защиты последней и наказания лиц, разглашающих или пытающихся разгласить ее;
- добиться, чтобы эта программа как можно больше отвечала названным целям.

Уделив достаточно времени разработке программы, и определив источник финансирования ее проведения, решите вопрос о назначении кого-нибудь ответственным за ее постоянное выполнение и своевременный пересмотр.

Этот работник будет оценивать эффективность программы и улучшать ее время от времени. Организация эффективной защиты коммерческой тайны предприятия во многом зависит от правильного установления круга носителей информации.

Анализ в этой области позволяет выделить четыре вида носителя информации в зависимости от их функционального назначения, в частности: документ, человек, изделие (предмет, материал) и процесс.

Документ, согласно ГОСТам 16487–83; 6.10.1–88, представляет собой средство закрепления различным способом на

специальном материале информации о фактах, событиях, явлениях объективной действительности и мыслительной деятельности человека. Документ отличает то, что его функциональное назначение целиком и полностью исчерпывается свойством носителя информации. В период своего существования документ проходит определенные этапы: составление и оформление, размножение, пересылка, использование, хранение, уничтожение. Конкретное наполнение этих этапов зависит от типа документа.

В настоящее время известны документы на бумажных носителях, на микроформах, на магнитных носителях. В целом система документов имеет довольно разветвленную структуру.

Известно, что всякая деятельность любого предприятия должна быть юридически оформлена. Это положение в полной мере относится и к организации защиты коммерческой тайны. Поэтому одной из первоочередных задач, которые встают перед предприятием при организации защиты своей коммерческой тайны, является разработка соответствующих нормативных документов, регламентирующих деятельность всех звеньев предприятия в этом направлении.

Если обратиться к мировой практике по данному вопросу, то речь, по сути дела, идет либо о необходимости внесения соответствующих дополнений в уже имеющиеся на предприятии документы, такие как Устав, Коллективный договор и др., либо о подготовке самостоятельных внутренних инструкций и рекомендаций.

При этом может быть рекомендован такой порядок разработки и утверждения указанных нормативных документов, при котором они согласовываются с советом (правлением) предприятия, а при необходимости проводятся в жизнь через решение общего собрания (конференции) трудового коллектива.

Исходной правовой базой для организации защиты коммерческой тайны является УСТАВ предприятия. Именно в нем, прежде всего, необходимо зарегистрировать право на коммерческую тайну, потому что предприятие может осуществлять лишь те виды деятельности, которые отвечают целям, предусмотренным в нем. Сделать это следует путем внесения дополнения к Уставу специального раздела.

Важным подспорьем среди мер по обеспечению коммерческой тайны является КОЛЛЕКТИВНЫЙ ДОГОВОР, ежегодно заключаемый на предприятии между трудовым коллективом и администрацией. В нем следует предусмотреть соответствующие

положения по защите коммерческой тайны, содержащие взаимные обязательства сторон по данному вопросу.

Наличие таких обязательств в коллективном договоре позволит повысить взаимную ответственность трудового коллектива и администрации за обеспечение мер по защите коммерческой тайны и организовать действенный контроль над выполнением этих обязательств.

Необходимым и крайне важным подспорьем является СПЕЦИАЛЬНАЯ ИНСТРУКЦИЯ ПО ОБЕСПЕЧЕНИЮ СОХРАННОСТИ КОММЕРЧЕСКОЙ ТАЙНЫ ПРЕДПРИЯТИЯ. В ней следует детализировать порядок действия исполнителей, предусмотреть четкую систему документооборота, изготовление изделий, организации работ в режимных помещениях, регламентировать условия применения средств связи, использования средств ВТ, приема представителей др. предприятий и т.п. В такой инструкции возможно определить:

- правила и процедуру присвоения и снятия грифа документам, работам и изделиям, содержащим коммерческую тайну предприятия;
- процедуру допуска работников предприятия к сведениям, составляющим коммерческую тайну предприятия;
- обязанности и ограничения, налагаемые на исполнителей, допущенных к сведениям, составляющим коммерческую тайну предприятия;
- правила обращения (делопроизводство, учет, хранение, размножение и т.д.) с документами и изделиями, содержащими коммерческую тайну предприятия; – правила приема представителей др. предприятий;
- принципы организации и проведения контроля за обеспечением сохранности сведений, составляющих коммерческую тайну предприятия;
- ответственность за разглашение сведений, составляющих коммерческую тайну, и др. нарушения установленного порядка их защиты.

Очень важным нормативным началом в деле обеспечения названного режима является СПЕЦИАЛЬНАЯ ПАМЯТКА. Она составляется для работников, которые допущены к сведениям, составляющим коммерческую тайну предприятия, и должна содержать основные положения по обеспечению сохранности этих сведений. При небольших объемах работы с документацией и изделиями, содержащими коммерческую тайну, и малом числе работников, допущенных к ним, она может заменять собой инструкцию предприятия по данному вопросу.

Прежде всего, в памятку следует включить обязанности работников по сохранению коммерческой тайны, за нарушение которых может последовать установленная ответственность. Кроме того, необходимо указать, что работник обязан:

- работать только с теми сведениями и документами, содержащими коммерческую тайну предприятия, к которым он получил доступ в силу своих служебных обязанностей;

- знать, какие конкретно сведения подлежат защите;

- знать, кому из сотрудников предприятия разрешено работать со сведениями, составляющими коммерческую тайну предприятия, к которым он сам допущен, и в каком объеме эти сведения могут быть доведены до этих сотрудников.

В памятке также устанавливается, что при участии в работе сторонних организаций работник может знакомить их представителей со сведениями, составляющими коммерческую тайну предприятия, только с письменного разрешения руководителя структурного подразделения. При этом руководитель должен определить конкретные вопросы, подлежащие рассмотрению, и указать, кому и в каком объеме может быть доведена информация, подлежащая защите.

Следует включить в памятку и положение о том, что запрещается помещать без необходимости сведения, составляющие коммерческую тайну предприятия, в документы, содержащие государственные секреты и имеющие в связи с этим соответствующий гриф секретности. Такое нарушение порядка обращения со сведениями, составляющими коммерческую тайну предприятию, может рассматриваться как их разглашение и влечет ответственность в соответствии с установленным законом порядком. В зависимости от особенностей предприятия в памятке могут содержаться и др. положения.

На предприятии наряду с названными принимается целый ряд др. документов. Хотелось бы, чтобы на практике были учтены следующие советы по обращению с ними.

Контроль за документацией должен стать самым важным делом, потому что на предприятии циркулирует огромное количество документов.

Следует быть очень внимательным к установлению системы контроля за документами и регулярно ее проверять и совершенствовать. К примеру, если вы хотите разрешить служащим брать работу на дом, желательно, чтобы выносимые материалы были классифицированы, правильно использовались, были необходимым образом защищены и возвращены.

В целях установления надлежащего контроля за хранением и использованием секретных документов необходимо выделить их из общей массы документов, находящихся в обороте на предприятии. Для этого следует ясно обозначить на лицевой обложке всех документов степень их секретности.

Начните создание вашей системы защиты коммерческой тайны с изучения процесса составления, циркуляции, хранения и уничтожения документов.

Составление документов представляет собой самую обязательную и, может быть, самую легкую область контроля.

В первую очередь следует определить порядок и стандарты идентификации документации, которую требуется защитить от раскрытия или неправильного использования.

Необходимо решить вопрос об установлении различных степеней секретности. Видимо, вам надлежит определить и объявить всем сотрудникам, какие конкретно типы документов должны быть закрыты.

Напечатайте гриф «секретно» на регулярно используемых формах (к примеру, чертежах, титульных листах и т.д.). Для других документов можно использовать штамп. При этом в надписи на документе целесообразно указать, что этот документ является вашей собственностью и определить ограничения по его использованию. Можно предложить в качестве примеров такие ограничения:

1. Этот документ содержит информацию, являющуюся собственностью предприятия. Получение и владение им не дает никаких прав на его размножение, раскрытие его содержания или на производство, использование и продажу того, что он описывает. Размножение, опубликование или использование без особого письменного разглашения данного предприятия строго запрещено.

2. Это конфиденциальный документ, распространение которого контролируется. Копирование производится только через тот отдел, который будет заниматься такой работой.

3. Секретный документ предприятия. Не копировать.

Техника контроля за циркуляцией копий строго секретных документов включает необходимость нумерации копий, составления списка лиц, получающих эти копии, фиксирования времени получения и сдачи документов.

Такая методика предусматривает и наличие формы, подписанной всеми получателями, посредством которой они обязуются никому не передавать, не копировать и возвращать документ по требованию.

При этой системе достаточно одного взгляда на формуляр с фамилиями получателей, чтобы определить, сколько и где находится копий документа в обороте.

В разряд документов, содержащих информацию, влияющую на конъюнктурные колебания, могут входить документы внутреннего маркетинга, финансовые документы, чертежи и оттиски, технические данные и планы.

Следовало бы на каждой странице перечней программного обеспечения ЭВМ обозначить, что эта информация конфиденциальная и является собственностью предприятия.

Необходимо, чтобы все тетради с проектной документацией постоянно переплетались и озаглавливались.

На них должны быть напечатаны фамилия, имя, отчество сотрудника, наименование предприятия, гриф секретности и отметка о собственности этого предприятия.

Существует объективная необходимость в организации СПЕЦИАЛЬНОГО ДЕЛОПРОИЗВОДСТВА с документальными носителями коммерческой тайны предприятия, устанавливающего порядок их подготовки, маркировки (т.е. присвоения соответствующего грифа), размножения, рассылки, приема и учета, группировки в дела, использования, хранения, уничтожения и проверки наличия, а также создания подразделения специального делопроизводства или назначения уполномоченного по данному вопросу.

Следует вести журнал учета входящих, исходящих и внутренних документов, содержащих коммерческую тайну предприятия, который будет полезен для проведения периодической инвентаризации таких документов, четкой регистрации их нахождения и уничтожения.

Передавайте конфиденциальные документы только тем, кому действительно необходимо знать содержащуюся в них информацию. Учтите, если у вас не отработана система определения такого контингента лиц, то любая система контроля за движением документов будет бессмысленной и вам не удастся сохранить вашу коммерческую тайну.

Просто установления процедуры контроля за документацией недостаточно. Необходимо создать соответствующую систему, гарантирующую правильную циркуляцию документов. Это включает различные инструкции по правилам хранения и использования документов с целью исключить доступ к содержащейся в них информации для всех, кому не нужно ее знать. Такое относится как к работающим, так и к неработающим на предприятии.

Обычная деятельность предприятия немыслима без взаимодействия с другими предприятиями. Такая взаимосвязь закрепляется в хозяйственных договорах. Помимо их основного назначения (установление взаимоотношений на выполнение работ, оказание услуг и т.п.) договоры следует использовать как средство обеспечения сохранности коммерческой тайны. В них необходимо специально оговаривать обязательства о соблюдении условий конфиденциальности и предусмотреть последствия нарушения принятых обязательств.

При заключении договора с иностранной фирмой условия конфиденциальности должны быть выражены в форме, предусмотренной законодательством страны принадлежности фирмы.

В некоторых случаях требуется присутствие в контракте определенного терминологического сочетания, напр.: «Сведения о технологии, конструкции, характере производства передаются (доверяются) исключительно для целей сооружаемого объекта и не могут быть переданы какой-либо др. фирме». Потому теперь очень необходимо изучение национальных законодательств фирм-партнеров и конкурентов.

Следует иметь в виду, что соглашение об условиях конфиденциальности может предшествовать заключению между будущими партнерами коммерческих соглашений о передаче лицензий, ноу-хау, договоров о создании совместных предприятий и т.д. Однако, являясь частью таких соглашений, условия конфиденциальности сохраняют свою автономность и могут действовать после прекращения основного договора.

Очень важным является решение вопросов, связанных с УНИЧТОЖЕНИЕМ ДОКУМЕНТОВ И ИХ РАССЕКРЕЧИВАНИЕМ. Следует разработать свою программу по ликвидации конфиденциальных документов. Она должна включать, прежде всего, обязанность администрации регулярно просматривать инвентарные списки контролируемой документации. В том случае, если информация, содержащаяся в ней, перестает быть секретной, ее необходимо рассекречивать. Постарайтесь избежать вот какой крайности.

Если вы просто будете засекречивать все документы, при этом никогда не будете отменять степени секретности, не разработаете процедуру рассекречивания, то сохранение секретности всей вашей информации станет весьма проблематичным.

После отбора документов, которые могут быть рассекречены, вам необходимо найти безопасный метод ликвидации их или др.

ненужных копий. Не следует выбрасывать их просто в мусор, а необходимо порвать или уничтожить иным способом.

Успех осуществления мероприятий по защите коммерческой тайны во многом зависит от СОЗДАНИЯ И СОБЛЮДЕНИЯ СПЕЦИАЛЬНОГО РЕЖИМА ПОЛЬЗОВАНИЯ КОМПЬЮТЕРАМИ.

Использование в современных условиях компьютеров, с одной стороны, значительно облегчило сбор и хранение необходимой информации, а с другой – весьма усложнило решение проблемы защиты коммерческой тайны предприятия. Это связано с тем, что:

- вы вынуждены иметь дело с обширным объемом информации, требуемой защиты;
- в процессе производства и хранения информации она становится доступной большому количеству людей;
- обеспечение закрытости такой информации требует новых и более сложных процедур.

Ведь если видны свидетельства физического вторжения в помещение, где хранятся секретные документы и даст основание утверждать, что совершено хищение, то такой вывод порой невозможно сделать, когда похищается информация, хранящаяся в электронной памяти.

Надо обратить внимание на то, что не существует какой-то единственной системы, которая бы способна была обеспечить сохранность информации, заложенной в ЭВМ. Решение комплекса вопросов, связанных с защитой коммерческой тайны, зависит от типа используемого компьютера и степени конфиденциальности информации, которую и обрабатывает. Необходимо предпринимать особые меры предосторожности для обеспечения контроля за доступом к информации через персональные компьютеры. Следует учитывать и тип информации, которая хранится в памяти ЭВМ.

По мере развития технологии обработки электронных данных будут разрабатываться и новые технологии для борьбы против «компьютерных преступлений». Учитывая такие особенности, следует высказать некоторые советы.

Принимая во внимание необходимость обеспечения закрытости информации, следует установить контроль за доступом ко всем терминалам. Целесообразно регулярно изменять имена пользователей и ключевые слова, особенно если на предприятии происходит частая смена операторского состава.

Вмените кому-нибудь в обязанности контролировать доступ к системе ЭВМ и процесс ее использования, а также периодически

проверять проводимые на ней операции для того, чтобы вовремя определить применение необычных программ.

Весьма эффективен порядок, когда при работе с компьютером, содержащим информацию о коммерческой тайне предприятия, каждый из допущенных работников имеет свой личный код, позволяющий ему пользоваться лишь теми программами и данными, которые его непосредственно касаются.

Наличие указанных кодов предохраняет также от доступа посторонних к хранящейся информации. На Западе создана целая индустрия защиты вычислительной техники от несанкционированного доступа и побочных излучений. Определенные шаги в этом направлении делаются и в нашей стране.

При возникновении необходимости следует рассмотреть вопрос о закупке соответствующих программных и технических средств иностранного или отечественного производства. Если имеются возможности, целесообразно создать такие средства защиты ЭВМ самостоятельно.

Как бы ни была надежна система защиты коммерческой тайны, используемая вами, периодически необходима ее проверка. К примеру, если частная информация включается в ваши документы, подготовленные для вышестоящих инстанций или правительства, вам потребуется проверить весь порядок засекречивания документов так, чтобы защитить их от раскрытия. Таким же образом, если контракты требуют возвращения документации после прекращения ваших деловых отношений, следует удостовериться в том, что у вас разработан надежный процесс возвращения документации.

Процесс проверки должен включать мероприятия как по защите информации, так и по уничтожению документации.

Чтобы избежать ненужного накопления старой информации, необходимо посвятить максимум времени рассекречиванию и удаления информации из системы. Более того, хотя некоторые документы больше не представляют для вас никакой пользы и подлежат рассекречиванию, содержащаяся в них информация может быть полезной для вашего конкурента, который может узнать, какую технологию вы отвергли и как вы принимаете деловые решения.

В ходе проверки вам надо проанализировать, насколько эффективно вы уничтожаете свои записи с целью исключить возможность использования рассекреченной информации в ущерб вашим интересам.

Конечным итогом системы проверки служит определение факта похищения или передачи конфиденциальной информации. Предусмотрите возможность доклада ваших сотрудников об обстоятельствах, вызывающих подозрение, внутри и вокруг предприятия,

Так, торговые представители регулярно обсуждают со своими коллегами и покупателями и сравнивают конкурирующую продукцию. Поэтому они первыми могут информировать вас о том, что ваш конкурент объявил о выпуске продукции, похожей на вашу. Кроме того, они часто посещают торговые выставки, ярмарки, конференции и т.п., где также могут получить интересующую вас информацию.

Лекция 14. Методика выделения сведений составляющих коммерческую тайну

Порядок выделения из всего объема собственной информации предприятия (фирмы) ее наиболее ценных частей для последующей защиты тесно связан с процессом производства товаров (услуг) и вытекает из практики конкурентной борьбы.

Факторы, определяющие конкурентоспособность предприятия, могут приносить положительные результаты только при условии их сокрытия от экономических соперников. Поэтому отнесение таких сведений к коммерческой тайне является формой защиты экономической безопасности предприятия (фирмы).

Сущность формирования методики выделения ценных сведений заключается в отыскании логики действий и признаков, характеризующих КТ.

Представим всю циркулирующую на предприятии информацию в виде круга и последовательно произведем следующие действия:

1. Выделим из него сектор сведений, являющихся государственными секретами (если они имеются на предприятии), так как порядок и организация защиты регламентируются требованиями, установленными правительством.

2. Исключим из рассмотрения сведения общеизвестные и широко применяемые другими предприятиями, а также информацию, содержащуюся в Постановлении правительства РСФСР «О перечне сведений, которые не могут составлять коммерческую тайну».

3. Оставшийся сектор информации разделим на два вида сведений: НИОКР, технология, управление и деловая информация (коммерческо-финансовая).

Часть первого вида информации с учетом выгоды и целесообразности можно защищать с помощью патентного и авторского права. После последовательного выполнения вышеназванных действий предметом анализа и оценки остается часть незащищенных с помощью патентов и авторского права сведений, а также коммерческо-финансовые данные.

Сделаем небольшое отступление. В отечественной и зарубежной литературе приводятся различные варианты перечней сведений, составляющих КТ предприятия. Но в комментариях к ним отсутствуют пояснения, почему тот или иной блок сведений (цена, себестоимость, дизайн и т.п.) включен в Перечень.

Ключ в пониманию того, какие сведения целесообразно в тот или иной период защищать как коммерческую тайну, является конкуренция (ценовая и неценовая). Именно поэтому к КТ целесообразно относить сведения, которые дают (могут дать) значимые преимущества в конкурентной борьбе. Разглашение же этой информации наносит экономический ущерб вследствие снижения конкурентоспособности товаров и услуг предприятия.

Рассмотрим один из примеров ценовой конкуренции. Ваше предприятие заканчивает разработку изделия, имеющего преимущества перед аналогичными товарами других производителей, которые в свою очередь ведут работы по созданию более совершенных изделий. По каким-либо причинам конкурентам становится известной информация о готовящемся выведении на рынок новейшего изделия и его планируемой цене. Полученные сведения позволяют экономическим соперникам заблаговременно (на стадии НИОКР, опытного производства) внести коррективы в разработку своего изделия и добиться снижения издержек производства, а следовательно, создать условия для продажи своего товара по более низкой цене по сравнению с ценой своего изделия. При схожих параметрах покупатель скорее всего отдаст предпочтение изделию конкурента.

Знание особенностей ценовой конкуренции позволяет понять, почему себестоимость разрабатываемого товара является коммерческой тайной. Таки образом, на последнем этапе оставшийся блок информации оценивается с позиций получения конкурентных преимуществ на рынке товаров и услуг. И чем значительнее могут быть выгоды от использования этих сведений

в конкурентной борьбе, тем они ценнее и требует соответствующей защиты.

Следующий этап методики выделения сведений, составляющих коммерческую тайну, – анализ и оценка сфер и циклов производства товаров. Фирма «Артур Д. Литтл» составила перечень из восьми сфер, в которых возможны нововведения: товар, сервис, маркетинг, производство, распределение, финансирование, управление, социальная сфера. На основе анализа был определен объем нововведений (%) в каждой из этих сфер, необходимый для успешной деятельности. Наибольший объем сведений, составляющих КТ (нововведений, влияющих на конкурентоспособность), приходится на сферы: товар, маркетинг, производство, сервис, управление.

Основные циклы производства товара приводятся в так называемой петле качества товара, которая включает в себя:

- маркетинг, поиск, изучение рынка;
- проектирование или разработку технических требований;
- материально-техническое снабжение;
- подготовку и разработку производственных процессов;
- производство;
- контроль, проведение испытаний и обследований;
- упаковку и хранение;
- реализацию и распределение продукции;
- монтаж и эксплуатацию;
- техническую помощь и обслуживание;
- утилизацию после использования.

Маркетинговые исследования позволяют выявить запросы потребителя, сформулировать исходные требования к новой продукции, а также определить потребность в принципиально новой продукции.

Фирмы экономически развитых стран уделяют значительное внимание оценке положения на рынке выпускаемой продукции, определению факторов, обеспечивающих конкурентоспособность.

Большинство зарубежных фирм начинает создание новой продукции с анализа данных службы маркетинга о преимуществах и недостатках уже освоенной продукции, а также продукции конкурентов.

Результаты исследований рынка и намечаемые на этой основе мероприятия являются информационной основой для эффективной производственно-коммерческой деятельности и поэтому могут быть отнесены к КТ предприятия.

Важный элемент маркетинговой деятельности предприятия – так называемый реинжиниринг, конструирование наоборот.

Так, американская фирма «Форд покупает изделия конкурентов и разбирает их. Все съемные детали откручиваются, вынимаются все блоки, удаляются даже заклепки, вскрываются отдельные точечные сварные швы. Фирма составляет подробную опись всех деталей и анализирует особенности применявшегося изготовителем производственного процесса. Затем проводят расчет издержек. Детали оценивают с точки зрения их стоимости при изготовлении или покупке, делают заключение о их разнообразии и унифицированности узлов и блоков.

Наиболее важными из получаемых сведений являются данные о количестве и разнообразии деталей и числе сборочных операций. Соотнося эти данные с количеством выпускаемых автомобилей, численностью персонала на заводе и т.д., оценивают уровень экономии.

При разборе товаров конкурентов фирма определяет, из чего именно складываются издержки конкурента. Иногда обнаруживаются детали, которые можно изготовить по более низкой цене. А это, в свою очередь, приводит к достижению ценового преимущества. Если вы сумеете определить, в какую именно сумму должно было обойтись изготовление товара, то заодно узнаете, сможет ли конкурент при желании позволить себе снизить цены. Японские фирмы используют информацию такого рода для сбивания цены, зная, что конкуренты не смогут последовать их примеру.

На имеющемся в литературе примере рассмотрим, какова технология действий японской фирмы при создании нового товара.

Группе испытаний товара передают по одному образцу всех закупленных моделей и ставят задачу произвести оценку эксплуатационных свойств каждой из них.

По два оставшихся экземпляра каждой модели передают группе дизайна, где их полностью разбирают. Один комплект – для того, чтобы подсчитать количество и разнообразие деталей, оценить стоимость каждой использованной детали и простоту сборки. Второй – чтобы испытать каждую деталь на долговечность, выявить дизайнерские усовершенствования и составить полную картину применяемого конкурентами технологического процесса.

Третья группа занимается изучением служб маркетинга и распределением у конкурентов. Она подсчитывает число торговых точек, в которых продавались товары конкурентов, изучает используемую ими систему сервиса и степень доступности каждого товара.

Группе производственников поручают изучение предприятий-кокурентов с точки зрения стоимости рабочей силы, сырья, материалов и оценке производительности.

С учетом полученной информации разрабатывают дизайн, превосходящий продукцию конкурентов. На основе макета и схемы предполагаемого процесса производства определяют расчетную стоимость предлагаемой продукции.

Исследования показывают, что среди английских и западноевропейских фирм девять из десяти в качестве отправной точки своих дизайнерских разработок используют товары конкурентов. Половине этих фирм эти товары служат источником идей. Чуть меньше половины фирм (46 %) заявили, что приспосабливают для себя товары конкурентов или пытаются усовершенствовать их, 6 % признали, что просто копируют эти товары.

Фирмы, видоизменяющие товары конкурентов, относились к группе в целом преуспевающих фирм. Действуя подобным образом, хороших результатов могут добиться даже фирмы, не имеющие возможности претендовать на роль лидеров в области техники и технологии.

Результаты маркетинговых исследований имеют важное значение и на стадии проектирования. Это обусловлено тем, что уровень затрат на эксплуатацию, являющийся одним из основных показателей конкурентоспособности товаров, более чем на 80 % определяется характеристиками, закладываемыми на стадии разработки. На стадии проектирования и изготовления опытного образца конструктор может воздействовать лишь на 15 % общих затрат, а когда изделие передается в серийное производство, эти возможности падают на 5 %.

Проектирование и разработка включают в себя определение основных технико-экономических параметров, составление смет затрат, составление структуры затрат по этапам внедрения, определение цены, расчет прибыли, формулирование условий продаж, проектирование каналов и методов сбыта, порядок техобслуживания и объем услуг послепродажного обслуживания.

Каждый из вышеназванных этапов разработки нового товара, учитывающий результаты маркетинговых исследований, включает информацию, создающую предпосылки для конкурентных преимуществ, т.е. содержит сведения, составляющие коммерческую тайну.

Разработчики новой продукции используют сведения о дефектах, поломках ранее спроектированных, но еще реализуемых на рынке изделий. Разглашение названной

информации может нанести фирме серьезный ущерб в виде снижения уровня продаж и доверия потребителей.

Материально-техническое снабжение – важнейший элемент производства товаров. Наиболее ценной информацией, требующей защиты, являются сведения, использование которых может привести к созданию узких мест в снабжении. Результатом разглашения КТ в этой области деятельности может стать повышение цен на сырье, оборудование, комплектующие; срыв поставок, расторжение контракта; снижение уровня сотрудничества предприятия с поставщиками и т.п.

Рассматривая цикл производства с позиции охраны КТ, следует учитывать, что большинству фирм удается добиться динамического роста и финансово-коммерческого успеха путем последовательных небольших усовершенствований. Как считают специалисты, это самый реалистичный путь. Следует также иметь в виду, что, хотя крупные прорывы с большой долей вероятности появляются при значительных инновациях в области высоких технологий, требующих для осуществления и солидных капиталовложений, и продолжительного времени, успех на рынке неизменно приносят непрерывные усовершенствования в сфере высокой технологии, на которые не нужно ни больших денег, ни длительных сроков.

Большинство новинок представляют собой усовершенствованные варианты существующих изделий. Иногда одна-две из ста оказывается чем-то принципиально новым.

Залогом преуспевания многих фирм являются небольшие поэтапные усовершенствования. Их применяют не сразу в момент появления. Фирма аккумулирует эти усовершенствования, а затем на их основе выпускает товары – дополнения, улучшенные по сравнению с существующими сразу по нескольким показателям.

С учетом этих особенностей рынка к коммерческой тайне должны относиться сведения об усовершенствованиях выпускаемых изделий, включая технологию, и другие вопросы (а не только значительные инновации).

Для руководителей и специалистов по защите КТ проблема дифференциации качества товаров относительно товаров конкурентов обязательно должна найти отражение в мероприятиях по защите информации. На стадии разработки товара определенную ценность как раз и будут представлять сведения (информация) о его свойствах, обеспечивающих существенное отличие от уже имеющихся на рынке изделий. Это наиболее ценные сведения предприятия (фирмы), составляющие коммерческую тайну.

При покупках руководствуются не только ценой, но и показателями дифференциации товаров, достигнутой в результате эффективного дизайна.

Усилия предприятий направляются на повышение ценностной значимости собственных товаров в глазах клиента и на углубление разницы между своими товарами и товарами конкурента. (Этого можно достичь разными путями: сделать товар меньше по размеру, легче по массе, быстроходнее, мощнее, дешевле, усилить имеющееся положительные качества).

Целесообразно сначала составить исчерпывающий перечень свойств своего товара, а затем задаваться вопросом, какое из этих свойств, будучи усовершенствованным, обеспечить ему наибольшее конкурентное отличие. Именно эти сведения с большей вероятностью могут быть отнесены к коммерческой тайне.

Чтобы не проигрывать в конкурентной борьбе, фирмы постоянно совершенствуют управление, организуют производство или услуги с более низкими затратами или более высокого качества. Для этого автоматизируют производство, упрощают структуры управления, реализуют программы по активному вовлечению работников в управление, увязывают размер оплаты с эффективностью труда.

Потребность в совершенствовании управления обусловлена также уменьшением времени жизненного цикла товара, увеличением номенклатуры, снижением объемов, усложнением технологических процессов.

Происходят изменения в традиционных взглядах людей на бизнес. Фирмы решительно отказываются от приверженности к производству тысяч, а то и миллионов совершенно одинаковых изделий, которая объясняется только тем, что это – дешевый способ изготовления. Фирмы все точнее и точнее приспосабливают товар к нуждам заказчиков.

Приведенные сравнительные анализы показывают, что инвестиции в повышение квалификации и совершенствование организационно-управленческой составляющей дают много раз более высокий экономический эффект, чем просто инвестиции в автоматизацию основного производства.

Принцип узкой специализации каждого из работников заменяется походом, при котором группа рабочих высокой квалификации несет полную ответственность за качество, экономию ресурсов, привлечение новых специалистов, подготовку персонала и т.д. Групповой подход к организации работ приносит

значительный экономический эффект, создает условия для повышения производительности труда в несколько раз.

Рациональное планирование рабочих мест, высокая организация производства и сборки резко сокращает время на транспортировку и сборочные операции. Так называемые операционные центры уменьшают время сборки более чем в 10 раз при использовании тех же самых инструментов.

Оценка роли управленческой информации в конкурентной борьбе за получение преимуществ перед экономическими соперниками позволяет включить ряд сведений из этой сферы деятельности предприятия в перечень данных, составляющих коммерческую тайну.

Ощутимый экономический ущерб может нанести разглашение КТ на этапе испытания разработанного товара рынком. Главное в процессе рыночных испытаний – оценить привлекательности товара для потребителя. Необходимо обеспечить защиту таких сведений, которые облегчили бы принятие конкурентами соответствующих контрмер. Как правило, охране на этой стадии подлежит торговая марка продукта, название фирмы, проводящей испытания, результаты испытаний, время вывода продукта в серийное производство и т.п.

Существенное значение для организации успешного сбыта продукции имеет упаковка. Она выполняет функцию защиты товара от повреждений. Эффективная конструкция упаковки обеспечивает условия для наилучшего использования транспорта, применения погрузочно-разгрузочных механизмов, доставки товара на значительные расстояния в неповрежденном виде, что способствует освоению новых рынков. Упаковка должна привлекать внимание покупателя и побуждать его приобрести данный товар. По существу упаковка является самостоятельным товаром. Поэтому к коммерческой тайне целесообразно относить сведения, описывающие характеристики разрабатываемых упаковок, технологию их изготовления, экономический показатель производства и использования.

Важным этапом исследования сбытовой деятельности является анализ издержек обращения. В качестве одного из методов оценки эффективности сбыта используется прием сопоставления определенных затрат с аналогичными затратами конкурентов. При этом выявляются необоснованные расходы, потери в сфере продвижения товара к покупателю, проверяется рентабельность системы сбыта.

Такое сопоставление показывает излишние затраты на реализацию и создает информационные предпосылки для

выработки мер по повышению конкурентоспособности данного вида товара. Эти сведения, безусловно, создают определенные преимущества в экономическом соперничестве и многими фирмами относятся к КТ.

Для удержания или завоевания позиций на рынке предприятия активно используют рекламу. При этом могут демонстрироваться промышленные образцы, определенным образом доводится информация о новейших технологиях и т.п. Важно не допустить ошибок, которые могут привести к разглашению ценной информации, так как конкуренты, получив ее в ходе рекламы, могут внести необходимые коррективы в процесс конкурентной борьбы.

Испытанный метод рекламы, обеспечивающей защиту коммерческой тайны, – так называемый метод черного ящика. При этом описывается проблема, показываются достигнутые результаты, полученные преимущества, но как это достигнуто, сообщается в урезанном виде, с крайней осторожностью.

В последние годы в промышленно развитых странах службы безопасности стали принимать меры по защите информации, которую соперничающие фирмы могут получить при анализе отходов продукции, поступающих в утилизацию или на рынок. Главной формой защиты является содержание в тайне фирмами, специализирующимися на продаже отходов производств, сведений о предприятиях-поставщиках этого сырья.

Как указывалось выше, прибыль в значительной мере зависит от производственных и рыночных факторов. Поэтому большой блок защищаемой информации отражает специфику взаимодействия изготовителя (поставщика) и потребителя (заказчика).

Рассмотрение информационного отражения процессов производства и сбыта позволяет выделить структурные элементы перечня сведений, составляющих коммерческую тайну предприятия. Перечень включается в себя следующие блоки информации: производство; управление производством; планирование; финансовое состояние; технология производства; НИОКР; рыночная политика и состояние рынка; партнеры и конкуренты; переговоры и контракты; цены; сбыт; собственная безопасность предприятия.

Для того, чтобы принять решение о включении тех или иных данных о деятельности предприятия в Перечень сведений, составляющих коммерческую тайну предприятия, целесообразно на первом этапе определить возможные отрицательные

последствия в случае их разглашения. К отрицательным последствиям относятся:

- разрыв деловых отношений с партнерами предприятия;
- срыв переговоров, утрата возможности заключения выгодного контракта;
- снижение уровня сотрудничества с деловыми партнерами;
- невыполнение договорных обязательств;
- необходимость проведения дополнительных рыночных исследований;
- отказ от решений, ставших неэффективными в результате разглашения сведений информации, и необходимость принятия дополнительных мер, связанных с финансовыми затратами;
- использование конкурентами полученных сведений для повышения эффективности экономического соперничества;
- потеря возможности патентования и продажи лицензий;
- сокращение конкурентами затрат на проведение НИОКР, совершенствование технологий;
- снижение цен на продукцию или снижение объемов продажи;
- нанесение ущерба авторитету фирмы;
- снижение уровня экономической безопасности;
- опережение конкурентом вывода аналогичного товара на рынок;
- ухудшение условий получения кредитов;
- появление трудностей в снабжении, приобретении оборудования;
- увольнение ведущих специалистов предприятия.

Чтобы избежать ошибок необоснованной классификации сведений, специалисты предприятия должны руководствоваться дополнительными критериями отнесения информации к коммерческой тайне. Наиболее общими из них являются:

- выигрыш во времени для предприятия в сравнении с конкурирующими фирмами;
- уникальность разработки;
- новизна (новая функция потребления, новая технология, применение в новых областях);
- преимущества в технико-экономических характеристиках товара перед изделиями конкурента;
- оригинальное применение материалов, технологий;
- преимущества в ценовой конкуренции;
- значительные трудозатраты в получении информации;
- монополии предприятия на информацию по данному направлению производственно-коммерческой деятельности;

- степень очевидности использования информации конкурентами в случае ее опубликования;

- перспективы самостоятельного получения сведений, закрываемых конкурентами, и в какие сроки;

- появление возможности выхода на международный рынок;

- степень влияния на формирование у потребителя положительного представления о фирме;

- возможность обеспечения сохранности на предприятии информации в случае ее отнесения к коммерческой тайне.

Структура и содержание Перечня зависят от характеристики предприятия. В Перечне при возможности указываются сроки пересмотра сведений, отнесенных к КТ, и перевода их в разряд общедоступных.

Практика организации защиты информации показывает, что в определенных случаях даже при поставках товара на рынок конкретные сведения о его производстве и сбыте могут достаточно длительное время охраняться как интеллектуальная собственность предприятия.

При отнесении сведений к коммерческой тайне руководствуются экономической целесообразностью, так как ограничение на пользование информацией может существенно мешать эффективному функционированию предприятия. Сведения сохраняются в тайне в том случае, если они являются частью основного качества изделия (например, приборы и устройства охраны, специальные замки, сейфы) или если технология приготовления товара такова, что не позволяет конкуренту в процессе реконструирования получить скрытые данные.

Джейм Н.А. Пули в совей книге «Коммерческая тайна» рекомендует выделить в производственно-коммерческой деятельности предприятия все то, что отличает вас от конкурентов и чего вам не хотелось бы им раскрывать.

Составив список вашей технологии и деловой информации по схеме, которая для вас приемлема, надо в первую очередь защищать ценную информацию, утечка которой способна принести ущерб, превышающий затраты на ее защиту. При анализе важно установить:

- какая информация нуждается в защите;

- кого она может заинтересовать, какова ее ценность для конкурентов;

- какие элементы информации являются наиболее ценными;

- каков срок жизни сведений, составляющих коммерческую тайну;

- во что обойдется защита.

В заключение приведем порядок выделения классифицированной информации, используемый фирмами и описанный в зарубежной литературе.

В самом начале необходимо изучить структуру конечного продукта (изделия, образца) и составить список сведений, в котором будет отражена ценная закрытая информация, использованная в ходе разработки.

Потом дается обоснование, каким образом и почему изделие обеспечит или может дать какое-то преимущество в результате применения разработанного образца или конечного изделия.

Далее определяется, почему и как разработанный образец обеспечит преимущество, перечисляются функции, предназначения, ТТД или возможности конечного изделия, обеспечивающие достижения, превосходство.

Указываются характеристики, имеющие очень важное значение, являющиеся уникальными или присущими только этому изделию; отражаются особенности, благодаря которым необходимо классифицировать сведения.

На формулирования содержания Перечня влияет выбранная предприятием стратегия в области конкурентной борьбы. По оценкам специалистов маркетинга, существуют четыре роли в конкурентной борьбе, определяемые долей фирмы на рынке: лидер (40 %-ная доля), претендент на лидерство (30 %), последователи (ведомые, до 20 %), окопавшиеся в рыночных нишах (до 10 % рынка). В зависимости от позиции на рынке и предъявляемых в этой связи претензий выделяют различные стратегии маркетинга.

Лидера пытаются догнать, атаковать многие, поэтому он, хотя и чувствует себя увереннее других, часто первым выступает с действиями по изменению цен, выводу на рынок новых продуктов, интенсификации стимулирования спроса.

В целом лидеры занимают активную оборону. Фирмы - претенденты на лидерство предпочитают активные наступательные действия. Третий вид фирм предпочитает следовать за лидером, экономя силы и средства за счет того, что путь первопроходцев выполняют лидеры.

Четвертый класс стратегий (обычно с него начинаю новички) – поиск рыночной ниши, которая в этом случае должна быть достаточных размеров и прибыльности, но не вызывать интерес конкурентов.

Лекция 15. Разработка системы защиты конфиденциальной информации

Под разглашением КИ понимаются умышленные или неосторожные действия допущенных к КИ лиц, приведшие к преждевременному, не вызванному служебной необходимостью распространению указанной информации среди лиц, включая работников АО, которым эта информация не была доведена в официально установленном порядке; утечка КИ - это несанкционированное распространение информации за пределы установленного физического пространства.

Комплексная защита КИ имеет целью решение двух задач: защиту права организации на КИ, в том числе относящуюся к категории интеллектуальной собственности организации (достигается на основе применения правовых норм действующего законодательства РФ); предотвращение угроз информационной безопасности организации, их выявление и существенное ослабление (достигается на основе реализации совокупности согласованных по цели, месту и времени применения правовых, организационных и технических мер защиты КИ, образующих *систему защиты конфиденциальной информации* (СЗКИ)).

СЗКИ дает возможность укрепления экономической безопасности организации, что способствует созданию условий для долгосрочного устойчивого функционирования организации.

К категории конфиденциальной информации относятся все виды информации ограниченного доступа, защищаемой законом –

- коммерческая,
- служебная,
- личная.

за исключением государственных секретов (статьи 727, 771, 1032 Гражданского кодекса РФ, ст. 16 Таможенного кодекса РФ, Указ Президента РФ от 6 марта 1997 года № 188 "Об утверждении перечня сведений конфиденциального характера").

«Коммерческая тайна – вид тайны, включающий информацию, устанавливаемую и защищаемую ее обладателем в любой сфере его коммерческой деятельности, доступ у которой ограничивается в интересах обладателя информации».

Коммерческая тайна – один из главных видов тайн, так как успешность функционирования предприятия по производству продукции или услуг определяется умением вести конкурентную борьбу, а значит, уметь увидеть, за счет чего можно добиться повышения прибыли по сравнению с конкурентами.

К сведениям, составляющим коммерческую тайну, можно отнести любую деловую информацию, кроме ограничений, накладываемых постановлением Правительства РФ “О перечне сведений, которые не могут составлять коммерческую тайну” от 05.12.91г. № 35.

Сведения, относящиеся к служебной информации, не являются обычно предметом самостоятельных сделок, однако их разглашение может причинить имущественный ущерб организации и вред ее деловой репутации.

В Федеральном законе от 20 февраля 1995 г. N 24-ФЗ "Об информации, информатизации и защите информации" информации о гражданах - персональные данные - сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность.

Создание системы защиты КИ.

Для того чтобы легально заниматься защитой конфиденциальной информации нужно получить лицензию на право осуществления деятельности по технической защите конфиденциальной информации (В соответствии с ПОЛОЖЕНИЕ О ЛИЦЕНЗИРОВАНИИ ДЕЯТЕЛЬНОСТИ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ Утвержденным Постановлением Правительства Российской Федерации от 30 апреля 2002 г. N 290). Для этого нужно выполнить следующие требования:

а) осуществление лицензируемой деятельности специалистами, имеющими высшее профессиональное образование по специальности "компьютерная безопасность", "комплексное обеспечение информационной безопасности автоматизированных систем" или "информационная безопасность телекоммуникационных систем", либо специалистами, прошедшими переподготовку по вопросам защиты информации;

б) соответствие производственных помещений, производственного, испытательного и контрольно-измерительного оборудования техническим нормам и требованиям, установленным государственными стандартами Российской Федерации и нормативно-методическими документами по технической защите информации; (пп. "б" в ред. Постановления Правительства РФ от 23.09.2002 N 689);

в) использование сертифицированных (аттестованных по требованиям безопасности информации) автоматизированных систем, обрабатывающих конфиденциальную информацию, а также средств защиты такой информации;

г) использование третьими лицами программ для электронно-вычислительных машин или баз данных на основании договора с их правообладателем.

Для получения лицензии соискатель лицензии представляет в лицензирующий орган следующие документы:

а) заявление о выдаче лицензии с указанием:

- лицензируемой деятельности;

- наименования, организационно-правовой формы и места нахождения - для юридического лица;

- фамилии, имени, отчества, места жительства, данных документа, удостоверяющего личность, - для индивидуального предпринимателя;

б) копии учредительных документов и документа, подтверждающего внесение записи о юридическом лице в Единый государственный реестр юридических лиц; (в ред. Постановления Правительства РФ от 06.02.2003 N 64);

в) копия свидетельства о государственной регистрации соискателя лицензии - индивидуального предпринимателя;

г) копия свидетельства о постановке соискателя лицензии на учет в налоговом органе с указанием идентификационного номера налогоплательщика;

д) документ, подтверждающий уплату лицензионного сбора за рассмотрение заявления о выдаче лицензии;

е) сведения о квалификации специалистов по защите информации соискателя лицензии.

Если копии документов не заверены нотариально, вместе с копиями предъявляются оригиналы.

Срок действия лицензии составляет пять лет и может быть продлен по заявлению лицензиата в порядке, предусмотренном для переоформления лицензии.

Переоформление лицензии осуществляется в течение десяти дней со дня получения лицензирующим органом соответствующего заявления.

Разработка мер и обеспечение защиты информации осуществляются подразделениями по защите информации (службами безопасности) или отдельными специалистами, назначаемыми руководством предприятия (учреждения) для проведения таких работ. Разработка мер защиты информации может осуществляться также сторонними предприятиями, имеющими соответствующие лицензии Гостехкомиссии России и/или ФАПСИ на право оказания услуг в области защиты информации.

Как Известно, право - это совокупность общеобязательных правил и норм поведения, установленных или санкционированных государством в отношении определённых сфер жизни и деятельности государственных органов, предприятий (организаций) и населения (отдельной личности).

Правовые нормы обеспечения безопасности и защиты информации на любом предприятии (фирме, организации) отражаются в совокупности учредительных, организационных и функциональных документов.

Требования обеспечения безопасности и защиты информации отражаются в Уставе :

- предприятие имеет право определять состав, объем и порядок защиты сведений конфиденциального характера, требовать от своих сотрудников обеспечения их сохранности и защиты от внутренних и внешних угроз;
- предприятие обязано обеспечить сохранность конфиденциальной информации.

Такие требования дают право администрации предприятия:

- создавать организационные структуры по защите конфиденциальной информации;
- издавать нормативные и распорядительные документы, определяющие порядок выделения сведений конфиденциального характера и механизмы их защиты;
- включать требования по защите информации в 5; договоры по всем видам хозяйственной деятельности;
- требовать защиты интересов предприятия со стороны государственных и судебных инстанций;
- распоряжаться информацией, являющейся собственностью предприятия, в целях извлечения выгоды и недопущения экономического ущерба коллективу предприятия и собственнику средств с, производства;
- разработать «Перечень сведений конфиденциальной информации». Требования правовой обеспеченности защиты информации предусматриваются в коллективном договоре.

Устав организации должен содержать следующие требования:

Раздел «Права и обязанности»:

1. Фирма имеет право:

- обеспечивать свою экономическую безопасность, определять состав, объем и порядок защиты конфиденциальной информации;
- требовать от сотрудников обеспечения экономической безопасности и защиты конфиденциальной информации;

- осуществлять контроль за соблюдением мер обеспечения экономической безопасности и защиты конфиденциальной информации.

2. Фирма обязана:

- обеспечить экономическую безопасность и сохранность конфиденциальной информации;

- осуществлять действенный контроль выполнения мер экономической безопасности и защиты конфиденциальной информации.

Раздел «Конфиденциальная информация».

Общество организует защиту своей конфиденциальной информации. Состав и объем сведений конфиденциального характера, и порядок их защиты определяются генеральным директором.

НЕСЕНИЕ ЭТИХ ДОПОЛНЕНИЙ ДАЕТ ПРАВО АДМИНИСТРАЦИИ:

- создавать организационные структуры по защите коммерческой тайны или возлагать эти функции на соответствующих должностных лиц;

- издавать нормативные и распорядительные документы, определяющие порядок выделения сведений, составляющих коммерческую тайну, и механизмы их защиты;

- включать требования по защите коммерческой тайны в договоры по всем видам хозяйственной деятельности (коллективный и совместные со смежниками);

- требовать защиты интересов фирмы перед государственными и судебными органами;

- распоряжаться информацией, являющейся собственностью фирмы, в целях извлечения выгоды и недопущения экономического ущерба коллективу и собственнику средств производства.

Коллективный договор должен содержать следующие требования:

Раздел «Предмет договора»:

- Администрация обязуется в целях недопущения нанесения экономического ущерба коллективу обеспечить разработку и осуществление мероприятий по экономической безопасности и защите конфиденциальной информации.

- Трудовой коллектив принимает на себя обязательства по соблюдению установленных на фирме требований по

экономической безопасности и защите конфиденциальной информации.

- Администрации учесть требования экономической безопасности и защиты конфиденциальной информации в правилах внутреннего трудового распорядка, в функциональных обязанностях сотрудников и положениях о структурных подразделениях.

Раздел «Кадры. Обеспечение дисциплины труда».

Администрация обязуется нарушителей требований по экономической безопасности и защите конфиденциальной информации привлекать к ответственности в соответствии с законодательством РФ.

Правила внутреннего трудового распорядка для рабочих и служащих предприятия целесообразно дополнить следующими требованиями.

Раздел «Порядок приема и увольнения рабочих и служащих» При приеме сотрудника на работу или при переводе его в установленном порядке на другую работу, связанную с конфиденциальной информацией, а также при увольнении администрация обязана:

- проинструктировать сотрудника о правилах экономической безопасности и сохранения конфиденциальной информации;

- оформить письменное обязательство о неразглашении конфиденциальной информации. Администрация вправе:

- принимать решения об отстранении от работы лиц, нарушающих требования по защите конфиденциальной информации;

- осуществлять контроль за соблюдением мер по защите и неразглашении конфиденциальной информации в пределах предприятия.

Раздел «Основные обязанности рабочих и служащих».

Рабочие и служащие обязаны:

- знать и строго соблюдать требования экономической безопасности и защиты конфиденциальной информации;

- дать добровольное письменное обязательство о неразглашении сведений конфиденциального характера;

- бережно относиться к хранению личных и служебных документов и продукции, содержащих сведения конфиденциального характера. В случае их утраты немедленно сообщить об этом администрации.

Раздел «Основные обязанности администрации».

Администрация и руководители подразделений обязаны:

- обеспечить строгое соблюдение требований экономической безопасности и защиты конфиденциальной информации;
- последовательно вести организаторскую, экономическую и воспитательную работу, направленную на защиту экономических интересов и конфиденциальной информации;
- включать в положения о подразделениях и должностные инструкции конкретные требования по экономической безопасности и защите конфиденциальной информации;
- неуклонно выполнять требования устава, коллективного договора, трудовых договоров, правил внутреннего трудового распорядка и других хозяйственных и организационных документов в части обеспечения экономической безопасности и защиты конфиденциальной информации.

Администрация и руководители подразделений несут прямую ответственность за организацию и соблюдение мер по экономической безопасности и защите конфиденциальной информации.

В договоре о проведении совместных работ должены содержаться следующие требования:

Раздел «Условия конфиденциальности».

Стороны обязуются не передавать лицензии лицам и не раскрывать публично сведения о проводимых совместно работах без взаимного согласования. За нарушение данного условия стороны несут финансовую ответственность по возмещению убытков, упущенной выгоды и морального ущерба.

Лица, нарушившие условия конфиденциальности, могут быть привлечены к ответственности в соответствии с действующим законодательством.

Обязательства конкретного сотрудника, рабочего или служащего в части защиты информации обязательно должны быть оговорены в трудовом договоре (контракте). В соответствии с КЗоТ (гл. III) при заключении трудового договора трудящийся обязуется выполнять определенные требования, действующие на данном предприятии. Независимо от формы заключения договора (устного или письменного) подпись трудящегося на приказе о приеме на работу подтверждает его согласие с условиями договора (КЗоТ РФ ст. 18).

Требования по защите конфиденциальной информации могут быть оговорены в тексте договора, если договор заключается в письменной форме. Если же договор заключается в устной форме,

то действуют требования по защите информации, вытекающие из нормативно-правовых документов предприятия. При заключении трудового договора и оформлении приказа о приеме на работу нового сотрудника делается отметка об осведомленности его с порядком защиты информации предприятия. Это создает необходимый элемент включения данного лица в механизм обеспечения информационной безопасности.

Использование договоров о неразглашении тайны — вовсе не самостоятельная мера по ее защите. Не следует думать, что после подписания такого соглашения с новым сотрудником тайна будет сохранена. Это только предупреждение сотруднику, что в дело вступает система мероприятий по защите информации, и правовая основа к тому, чтобы пресечь его неверные или противоправные действия. Дальше задача — не допустить утраты коммерческих секретов.

Реализация правовых норм и актов, ориентированных на защиту информации на организационном уровне, опирается на те или иные организационно-правовые формы, к числу которых относятся соблюдение конфиденциальности работ и действий, договоры (соглашения) и различные формы обязательного права. Конфиденциальность — это форма обращения со сведениями, составляющими конфиденциальную информацию, на основе организационных мероприятий, исключающих неправомерное овладение такими сведениями.

Договоры — это соглашения сторон (двух и более лиц) об установлении, изменении или прекращении взаимных обязательств.

Обязательство — гражданское правоотношение, в силу которого одна сторона (должник) обязана совершить в пользу другой стороны определенные действия.

Правовое регулирование необходимо для совершенствования механизма предупреждения противоправных действий по отношению к информационным ресурсам, для уточнения и закрепления задач и правомочий отдельных субъектов в сфере предупредительной деятельности, охраны прав и законных интересов граждан и организаций.

Анализ законодательства, регулирующего деятельность субъектов в сфере информационной безопасности, показывает наличие определенных недостатков. Существующие правовые нормы разбросаны по различным нормативным актам, издававшимся в разное время, в разных условиях и на разных уровнях. Действующее законодательство не систематизировано, что создает большие трудности в его использовании на практике.

Организационная защита — это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и проявление внутренних и внешних угроз.

Организационная защита обеспечивает:

- организацию охраны, режима, работу с кадрами, с документами;

- использование технических средств безопасности и информационно-аналитическую деятельность по выявлению внутренних и внешних угроз предпринимательской деятельности.

Организационные мероприятия играют существенную роль в создании надежного механизма защиты информации, так как возможности несанкционированного использования конфиденциальных сведений в значительной мере обусловливаются не техническими аспектами, а злоумышленными действиями, нерадивостью, небрежностью и халатностью пользователей или персонала защиты. Влияния этих аспектов практически невозможно избежать с помощью технических средств. Для этого необходима совокупность организационно-правовых и организационно- технических мероприятий, которые исключали бы (или, по крайней мере, сводили бы к минимуму) возможность возникновения опасности конфиденциальной информации.

К основным организационным мероприятиям можно отнести:

- организацию режима и охраны. Их цель — исключение возможности тайного проникновения на территорию и в помещения посторонних лиц; обеспечение удобства контроля прохода и перемещения сотрудников и посетителей; создание отдельных производственных зон по типу конфиденциальных работ с самостоятельными системами доступа; контроль и соблюдение временного режима труда и пребывания на территории персонала фирмы; организация и поддержание надежного пропускного режима и контроля сотрудников и посетителей и др.;

- организацию работы с сотрудниками, которая предусматривает подбор и расстановку персонала, включая ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты ин формации и др.;

- организацию использования технических средств сбора, обработки, накопления и хранения конфиденциальной информации;

- организацию работы по анализу внутренних и внешних угроз конфиденциальной информации и выработке мер по обеспечению ее защиты;

- организацию работы по проведению систематического контроля за работой персонала с конфиденциальной информацией, порядком учета, хранения и уничтожения документов и технических носителей.

- организацию работы с документами и документированной информацией, включая организацию разработки и использования документов и носителей конфиденциальной информации, их учет, и выполнение, возврат, хранение и уничтожение;

Исходя из ситуации и в целях совершенствования системы защиты информации я предлагаю объединить все службы занимающиеся защитой информации в одну службу и назвать её службой безопасности, функции которой будут следующими:

• организует и обеспечивает пропускной и внутриобъектовый режим в зданиях и помещениях, порядок несения службы охраны, контролирует соблюдение требований режима сотрудниками, арендаторами, партнерами и посетителями;

• руководит работами по технической защите, а так же по правовому и организационному регулированию отношений по защите государственной тайны и конфиденциальной информации;

• разрабатывает основополагающие документы с целью закрепления в них требований обеспечения безопасности и защиты государственной тайны и конфиденциальной информации, в частности устава, правил внутреннего трудового распорядка, положений о подразделениях, а также трудовых договоров, соглашений, подрядов, должностных инструкций и обязанностей руководства, специалистов, рабочих и служащих;

• разрабатывает и осуществляет совместно с другими подразделениями мероприятия по обеспечению работы с документами, содержащими сведения, являющиеся государственной тайны и конфиденциальной информации, при всех видах работ организует и контролирует выполнение требований инструкции по защите государственной тайны и конфиденциальной информации;

• изучает все стороны производственной, коммерческой, финансовой и другой деятельности для выявления и закрытия возможных каналов утечки государственной тайны и

конфиденциальной информации, ведет учет и анализ нарушений режима безопасности, накапливает и анализирует данные о злоумышленных устремлениях конкурентов и других организаций в отношении деятельности организации и е клиентов, партнеров, смежников;

• организует и проводит служебные расследования по фактам разглашения сведений, утрат документов и других нарушений безопасности организации;

• разрабатывает, ведет, обновляет и пополняет перечень сведений, составляющих конфиденциальную информацию и другие нормативные акты, регламентирующие порядок обеспечения безопасности и защиты информации;

• обеспечивает строгое выполнение требований нормативных документов по защите конфиденциальной информации; • осуществляет руководство службами и подразделениями безопасности предприятий организации в части оговоренных в договорах условий по защите государственной тайны и конфиденциальной информации;

• организует и регулярно проводит учебу сотрудников фирмы и службы безопасности по всем направлениям защиты государственной тайны и конфиденциальной информации, добиваясь, чтобы к охране коммерческих секретов был глубоко осознанный подход;

• ведет учет сейфов, металлических шкафов, специальных хранилищ и других помещений, в которых разрешено постоянное или временное хранение государственной тайны и конфиденциальной информации;

• ведет учет выделенных для конфиденциальной работы помещений, технических средств в них, обладающих потенциальными каналами утечки информации;

Служба безопасности должна быть самостоятельной организационной единицей, подчиняющейся непосредственно генеральному директору организации.

Возглавляет службу безопасности начальник службы в должности заместителя генерального директора по безопасности.

Организационно служба безопасности состоит из следующих структурных единиц:

• отдела охраны;

• Отдел по защите конфиденциальной информации:

• Сектор обработки документов с грифом "конфиденциальная информация";

• лаборатории контроля защищенности от НСД к информации автоматизированных систем и средств вычислительной техники.

• Лаборатория комплексного контроля эффективности противодействия иностранным техническим разведкам и технической защиты информации ;

• группа анализа возможности образования технических каналов утечки информации;

Для защиты конфиденциальной информации разрабатываются в организации должны быть разработаны следующие нормативно-правовые документы:

• Перечень сведений, составляющих конфиденциальную информацию организации; • Договорное обязательство о неразглашении КИ • Инструкция по защите конфиденциальной информации

Защита информации в компьютерах должна осуществляться в соответствии с требования РД ГостехКомиссии, и СТР-к (специальные требования и рекомендации по технической защите конфиденциальной информации).

В первую очередь следует разработать перечень сведений, составляющий конфиденциальную информацию организации. В перечень должны включаться все сведения, являющиеся собственностью организации.

Под сведениями (и их носителями) понимаются:

• Данные, полученные в результате обработки информации с помощью технических средств (оргтехники);

• Информация как часть данных, несущая в себе полезные сведения и используемая сотрудниками организации для работы в служебных целях;

• Документы (носители), образующие в результате мыслительной деятельности сотрудников организации, включающие в себя сведения любого происхождения, вида и назначения, но необходимые для нормального функционирования организации.

Сведения, включенные в Перечень, имеют ограниченный характер на использование (применение). Ограничения, вводимые на использования сведений, составляющих конфиденциальную информацию, направлены на защиту интеллектуальной, материальной, финансовой собственности и других интересов, возникающих при организации трудовой деятельности работников (персонала) её подразделений, а также при их сотрудничестве с работниками других предприятий. В совокупности под конфиденциальной информацией надо понимать сведения, не являющиеся государственными секретами, но которые связаны, прежде всего, с производственной, управленческой, финансовой или другой экономической

деятельностью организации, разглашение (передача, утечка, хищение) которой может нанести ущерб её интересам или интересам их владельцев.

Законодательной основой защиты конфиденциальной информацией является часть вторая ГК РФ.

При разработки перечня следует руководствоваться:

• Конституцией РФ, принятой 12 декабря 1993 года;

• Законом РФ “ О государственной тайне ” № 5485-1 от 21.07.93;

• Федеральным законом РФ “Об информации, информатизации и защите информации” № 24-ФЗ от 20.02.95;

• Указом Президента РФ “об утверждении Перечня сведений, отнесённых к государственной тайне” № 1203 от 30.11.95;

• Указом Президента РФ “об утверждении Перечня сведений, конфиденциального характера” № 188 от 06.03.97;

• Постановлением Правительства РФ “ о Перечне сведений, которые не могут составлять коммерческую тайну” № 35 от 05.12.91;

• Сведения, являющиеся общедоступными на законных основаниях, в том числе в соответствии с Постановлением Правительства РФ № 35 от 05.12.91;

• Учредительные документы (решение о создании предприятия или договор учредителей) и устав;

• Документы, дающие право заниматься предпринимательской деятельности (регистрационные удостоверения, лицензии, патенты);

• Сведения по установленным формам отчётности о финансово- хозяйственной деятельности и иные сведения, необходимые для проверки правильности исчисления и уплаты налогов и других обязательных платежей в государственную бюджетную систему России;

• Документы о платежеспособности; сведения о численности, составе работающих, их заработной плате и условиях труда, а так же о наличии свободных рабочих мест;

• Документы об уплате налогов и обязательных платежах;

• Сведения о загрязнении окружающей среды, нарушении антимонопольного законодательства, несоблюдении безопасных условий труда, реализации продукции, причиняющей вред здоровью населения, а так же других нарушениях законодательств РФ и размерах причиненного при этом ущерба;

• Сведения об участии должностных лиц предприятия в кооперативах, малых предприятиях, товариществах и других

организациях, занимающихся предпринимательской деятельностью;

• Анализом преимуществ и недостатков для работы открытым и закрытым (внутренним) применением таких сведений;

• Анализом характера возможного ущерба в случае несанкционированного распространения сведений конфиденциального;

После разработки проекта перечня, он обсуждается и утверждается на ЭТК и согласовывается с генеральным директором организации, начальниками основных служб и отделов Перечень вводится приказом генерального директора организации в виде приложения к нему.

Сотрудники организации, допускаемые по роду своей работы или функциональным обязанностям к сведениям, составляющим конфиденциальную информацию, должны под расписку ознакомится с этим приказом и приложением к нему.

Перечень дифференцированно должен доводиться не реже 1 раза в год до всех сотрудников организации, которые используют в своей работе частично или в полном объёме сведения, информацию, данные или работают с документами ДСП и их носителями. Все лица принимаемы на работу в организацию, должны пройти инструктаж и ознакомиться с памяткой о сохранении конфиденциальной информации.

Сотрудник, получивший доступ к конфиденциальной информации и документам, должен подписать индивидуальное письменное договорное обязательство (приложение 2) об их неразглашении. Обязательство составляется в одном экземпляре и хранится в личном деле сотрудника не менее 5 лет после его увольнения. При его увольнении из организации ему даётся подписка о неразглашении конфиденциальной информации организации.

Далее должна быть разработана инструкция, регламентирующая порядок доступа сотрудников к КИ, порядок создания, учёта, хранения и уничтожения конфиденциальной документов организации. При написании такой инструкции следует руководствовать положениями ГОСТа Р6 30-2003- “ Унифицированные системы документации.”, а так же “ Унифицированная система организационно-распорядительной документации. Требования к оформлению документов”, который был принят и введен в действие постановлением Госстандарта РФ от 3 марта 2003 г. N 65-ст.

Инструкция по защите конфиденциальной информации должна состоять из следующих частей:

1.Общие положения.

2.Конфиденциальная инфромация.

3.Ответственность за разглашиение конфиденциальной информации.

4.Система доступа сотрудников к сведениям составляющим конфиденциальную информацию.

4.1.Круг лиц, имеющих право давать разрешение на доступ к конфиденциальным документам.

4.2.Порядок оформления разрешения на доступ к конфиденциальным документам

4.3.Порядок доступа на совещания по вопросам, содержащим конфиденциальные сведения.

5.Подготовка и издание конфиденциальных документов.

6.Учёт, прохождение и отправление изданных документов.

7.Приём и учёт прохождения поступивших документов

8.Учёт конфиденциальных документов выделенного хранения

9.Учёт журналов и карточек

10.Организация хранения конфиденциальных докуметов

11.Организация и технология контроля исполнения конфиденциальных документов.

12.Размножение документов

13.Уничтожение документов

14.Составление и оформление номенклатуры дел с грифом «КОНФИДЕНЦИАЛЬНО»

15.Формирование и оформление дел

16.Проверка наличия конфиденциальных документов.

17.Подготовка конфиденциальных документов на архивное хранение

18.Порядок передачи конфиденциальных документов в архив

19.Приложения

Защита КИ является одним из важнейших факторов создания предпосылок для стабильного существования и прогрессивного развития организации.

Основными условиями обеспечения информационной безопасности организации в контексте намеченного подхода к решению задач защиты КИ являются:

• построение моделей злоумышленников и конкурентов на основе поиска и аутентификации информации о их намерениях и устремлениях;

• определение перечня сведений, составляющих объект защиты интересов концерна в конкретных областях его деятельности;

• формирование предпочтительной для концерна структуры системы защиты КИ на основе синтеза, структурной оптимизации и технико-экономической оценки альтернативных вариантов;

• управление процессом реализации избранного замысла защиты КИ и координация работ по организации защиты КИ между всеми заинтересованными структурными подразделениями организации;

• совмещение организационно-административных мер защиты КИ с активными вовлечением в указанный процесс всего персонала организации;

• введение персональной ответственности (в том числе и материальной) должностных лиц всех уровней, а также других работников концерна, допущенных к КИ, за обеспечение установленного в АО режима конфиденциальности.

Вышеперечисленные документы разработаны с учетом общих требований к содержанию и оформлению подобных документов.

Разработанные автором документы вы можете получить, для этого достаточно отправить просьбу об получении такой инструкции мне на e-mail указав название организации, область деятельности).

Лекция 16. Система доступа к сведениям, составляющим коммерческую тайну предприятия

Важно место в системе организационных, административных, правовых и других мер, позволяющих качественно решать задачи информационного обеспечения научно-производственной и коммерческой деятельности, физической сохранности материальных носителей закрытых сведений, предотвращения их утечки, сохранения коммерческой тайны занимает разрешительная система доступа исполнителей к классифицированным документам и сведениям.

С учетом Закона РСФСР «О предприятиях и предпринимательской деятельности» (Утратил силу с 1 июля 2002 года на основании Федерального закона от 21 марта 2002 года N 31-ФЗ. Следует руководствоваться Федеральным законом РФ № 98-ФЗ от 29.07.2004 «О коммерческой тайне» и частью 4 ГК РФ) руководитель предприятия (фирмы) вне зависимости от форм собственности может устанавливать специальные правила доступа к сведениям, оставляющим коммерческую тайну, и ее носителям, тем самым обеспечивая их сохранность.

В системе мер безопасности существенное значение имеет оптимальное распределение производственных, коммерческих и финансово-кредитных сведений, оставляющих тайну предприятия, между конкретными исполнителями соответствующих работ и документов. При распределении информации, с одной стороны, необходимо обеспечить предоставление конкретному сотруднику для качественного и своевременного выполнения порученных ему работ полного объема данных, а с другой стороны, исключить ознакомление исполнителя с излишними, не нужными ему для работы классифицированными сведениями.

В целях обеспечения правомерного и обоснованного доступа исполнителя к сведениям, составляющим коммерческую тайну фирмы, рекомендуется разрабатывать и внедрять на предприятиях соответствующую разрешительную систему.

Под доступом понимается получение письменного разрешения руководителя предприятия (или, с его санкции, других руководящих лиц) на выдачу тому или иному сотруднику конкретных (или в полном объеме) закрытых сведений с учетом его служебных обязанностей (должностных полномочий).

Оформление доступа к КТ может производиться в соответствии с утвержденным директором Положением о разрешительной системе доступа, где юридически закрепляются полномочия должностных лиц предприятия по распределению информации и пользовании ею. Руководитель предприятия может разрешить пользование любой охраняемой информацией любому работнику данного предприятия или лицу, прибывшему на объект из другой организации для решения каких-либо вопросов, если в отношении этих сведений не установлены ограничения на ознакомление со стороны производственно-коммерческих партнеров по совместному производству и т.п.

На небольших предприятиях с ограниченным объемом закрытых работ (документов и изделий) руководитель имеет возможность лично распределять всю закрытую информацию, поступающую извне и создаваемую внутри предприятия между работниками независимо от занимаемых ими должностей. В этом случае осуществляется так называемое прямое распределение классифицированной информации. Однако прямое распределение становится невозможным на предприятии с большим объемом закрытых работ, рассредоточенным по различным подразделениям и участкам, в которых задействованы сотрудники различных должностных категорий. В этих условиях руководитель предприятия физически не имеет возможности лично

регулировать потоки классифицированной информации и распределять ее между работниками. Возрастает вероятность ошибок в виде неправильного адресования сведений или разрешения на доступ лицам, не имеющим к ним прямого производственного отношения.

Для качественного выполнения управленческих функций в данных условиях руководитель предприятия часть своих прав распоряжаться движением классифицированных сведений передает (делегирует) руководителям нижестоящих уровней. При определении полномочий каждого из нижестоящих руководителей выполняется ряд условий. Полномочия должны соответствовать и осуществляться в рамках его должностного положения (прав и обязанностей) и распространяться только на определенные категории исполнителей закрытых работ и документов.

Важнейшее значение для сохранности коммерческой тайны имеет надежность сотрудника, которому разрешают работать с ценной информацией. Как указывалось в одной из книг, степень надежности шифра определяется прежде всего надежностью шифровальщика. В связи с этим система доступа должна быть основана на убеждении, что лица, получающие разрешение на доступ к закрытым сведениям, лояльны по отношению к предприятию (фирме). Такой вывод могут сделать в процессе совместной деятельности служба безопасности и отдел кадров предприятия. Эти подразделения утверждают у директора предприятия список сотрудников, кто по своим личным качествам может быть допущен (или не допущен) к работе со сведениями, составляющими КТ. Соответствующие выписки передаются для учета руководителям подразделений, которым директором делегировано право выдавать разрешения на доступ к конкретным сведениям, входящим в Перечень охраняемой информации.

Руководитель, как правило, оставляет за собой право распоряжаться наиболее ценными сведениями, составляющими КТ (конфиденциальные договоры с фирмами, отчеты о результатах работ по перспективным изделиям и т.п.). Перечень таких документов, утвержденный директором, должен находиться в СБ. В соответствии с этим перечнем вся классифицированная информация и изделия, поступившие извне или созданные на предприятии, докладываются руководству СБ. Остальная информация поступает из СБ непосредственно руководителям подразделений в соответствии с действующей на предприятии разрешительной системой. Они и распределяют ее между исполнителями. Количество уровней должностной иерархии и

должностных лиц, которым могут быть предоставлены полномочия на распределение классифицированной информации, зависит от структуры предприятия, количества и сложности проводимых закрытых работ.

Эффективная работа разрешительной системы возможна только при соблюдении определенных правил:

1. Разрешительная система в качестве обязательного для выполнения правила включает в себя дифференцированный подход к разрешению доступа, учитывающий важность классифицированных сведений, в отношении которых решается вопрос о доступе.

2. Необходимо документальное отражение выданного разрешения на право пользования теми или иными защищаемыми сведениями. Это означает, что руководитель, давший разрешения на право пользования, должен его в обязательном порядке зафиксировать в письменном виде на соответствующем документе или в действующей на предприятии учетной форме. Никакие устные указания и просьбы о доступе кого бы то ни было (за исключением руководителя предприятия) не имеют юридической силы и не обязательны для работников СБ. Это требование относится и к руководителям всех уровней, работающих с классифицированной информацией и ее носителями. Таким образом, только письменное разрешение руководителя (в рамках полномочий) является разрешением для выдачи тому или иному лицу охраняемых сведений.

3. Следует строго соблюдать принцип контроля со стороны СБ. Это означает, что любое разрешение (здесь возможны изъятия по согласованию с руководителем) на ознакомление с закрытыми документами, сведениями и объектами должно быть согласовано с начальником СБ. Каждое разрешение должно иметь дату его оформления и выдачи.

Широкое распространение имеет такой традиционный вид разрешения как резолюция руководителя на самом классифицированном документе. Такое разрешение должно содержать перечень фамилий сотрудников, обязанных ознакомиться с документами или их исполнить, срок исполнения, другие указания, подпись руководителя и дату. Руководитель может при необходимости предусмотреть ограничения в доступе конкретных сотрудников к определенным сведениям.

Резолюция, как вид разрешения, применяется главным образом для оперативного доведения до заинтересованных лиц закрытой информации, содержащихся в документах и изделиях, поступаемых извне и создаваемых на предприятии.

Руководитель предприятия может дать разрешение на доступ в распорядительных документах: приказах, указаниях, распоряжениях по предприятию. В них должны содержать фамилии, должности лиц, конкретные классификационные документы и изделия, к которым они могут быть допущены (ознакомлены).

Другой вид разрешений – по фамильные списки лиц, имеющих право знакомиться и производить какие-либо действия с классифицированными документами и изделиями. По фамильные списки утверждаются директором предприятия или в соответствии с действующей разрешительной системой руководителями, занимающими, как правило, должности не ниже руководителей соответствующих подразделений.

По фамильные списки лиц могут использоваться при организации доступа к классифицированным документам и изделиям, имеющим особо важное значение для предприятия, при оформлении доступа в режимные помещения, на различного рода закрытые мероприятия (конференции, совещания, выставки, заседания научно-технических советов и т.п.). В пофамильных списках могут быть определены конкретные руководители, которые допускаются руководителем ко всем закрытым документам и изделиям без соответствующих письменных разрешений. В них указывается Ф.И.О. исполнителя работ, отдел, занимаемая должность, категория документов и изделий, к которым он допущен. На практике применим и вариант должностных списков, в которых указывается: должность исполнителя, объем документов (категории документов) и типы изделий, которыми необходимо пользоваться работникам предприятий, занимающим соответствующую списку должность. Следует отметить, что для предприятий с небольшим объемом классифицированных документов и изделий может оказаться достаточным использование таких видов разрешения, как резолюция руководителя на самом документе, по фамильные списки, должностные списки.

В организационном плане по фамильные списки должны готовиться заинтересованными руководителями структурных подразделений. Перечень сотрудников, вошедших в список, визируется начальником СБ и утверждается руководителем предприятия, который может делегировать права утверждения другим лицам из числа дирекции.

Наряду со списками могут быть использованы персональные карточки-разрешения на доступ к классифицированной информации и изделиям.

Разрешительная система должна отвечать следующим требованиям:

- распространяться на все виды классифицированных документов и изделий, имеющихся на предприятии, независимо от их место нахождения и создания;

- определять порядок доступа всех категорий сотрудников, получивших право работать с КТ, а также специалистов, временно прибывших на предприятие и имеющих отношение к совместным закрытым заказам;

- устанавливать простой и надежный порядок оформления разрешений на доступ к охраняемым документам и изделиям, позволяющий незамедлительно реагировать на изменения в области информации на предприятии;

- четко разграничивать права руководителей различных должностных уровней в оформлении доступа соответствующих категорий исполнителей;

- исключать возможность бесконтрольной и несанкционированной выдачи документов и изделий кому бы то ни было;

- не разрешать лицам, работающим с классифицированной информацией и объектами, вносить изменения в четные данные, а также подменять учетные документы.

При разработке разрешительной системы особое внимание должно быть уделено выделению главных, особо ценных для предприятия сведений, что позволит обеспечить к ним строго ограниченный доступ. При наличии совместных работ с другими предприятиями (организациями), иностранными фирмами или их отдельными представителями, необходимо предусмотреть порядок доступа этих категорий к коммерческой тайне предприятия. Целесообразно определить порядок взаимодействия с представителями обслуживающих государственных организаций: технадзором, санэпидемстанцией и др.

В пределах разрешительной системы руководители среднего звена управления фирмой могут:

- давать разрешение (в рамках полномочий) на доступ к классифицированным документам и сведениям исполнителям своего подразделения, исполнителей других подразделений по ходатайству их руководителей и в пределах их функциональных обязанностей;

- знать степень важности проводимых работ, разрабатываемых и находящихся в работе документации и изделий, задачи и функциональные обязанности своих подчиненных;

- незамедлительно сообщать в СБ об изменениях функциональных обязанностей сотрудников, не допуская адресования им документов и изделий до переоформления функциональных обязанностей в специальных решениях;

- не допускать со стороны подчиненных действий, влекущих нарушение требований разрешительной системы, принимать меры к исключению неоправданного ознакомления с теми сведениями, которые не относятся к выполняемым обязанностям работника;

- осуществлять контроль над адресованием классифицированных документов и изделий, ознакомлением с ними командированных лиц.

Сотрудники СБ фирмы должны контролировать:

- правомочность выдачи охраняемой информации и изделий сотрудникам предприятия и командированным лицам;

- правомерность адресования классифицированных документов и изделий из одного подразделения в другое;

- порядок оформления на доступ к коммерческой тайне фирмы.

В Положение о разрешительной системе фирмы необходимо указать, что передача классифицированных документов и изделий от исполнителя к исполнителю возможна только в пределах структурного подразделения и с разрешения его руководителя. Передача, возврат таких документов изделий производится по установленному на фирме порядку и только в течение рабочего времени данного дня.

Вся классифицированная документация и изделия, поступившие на предприятие и разработанные на нем, принимаются и учитываются работниками СБ. После регистрации документация передается на рассмотрение руководителю предприятия под расписку. Руководители могут передавать документы и изделия на исполнение после их регистрации только через СБ.

Предварительное рассмотрение оперативной переписки, оценка степени важности изделий осуществляется начальником (либо специально выделенным референтом директора), который определяет необходимость доклада полученной информации руководителю фирмы. Документы и изделия, не требующие обязательного рассмотрения директором фирмы, докладываются другим руководителям и начальникам структурных подразделений. Рассмотренные директором входящие и внутреннего распорядка документы и изделия адресуются соответствующим руководителям и исполнителям структурных

подразделений, которые дают письменное разрешение на самих документах (сопроводительных листах к изделиям) соответствующим подчиненным им исполнителям. Контроль за правильностью адресования документов и изделий осуществляется руководством подразделения экономической безопасности.

Переадресование классифицированных документов и изделий производится руководителями фирмы, указанными в разрешительной системы, начальниками структурных подразделений в пределах своего подразделения. При несоответствии назначенного документа и изделия функциональным обязанностям исполнителя вопрос решается на соответствующем уровне с участием СБ.

Командированные лица могут быть допущены к закрытым сведениям только с разрешения руководителя фирмы или его заместителей, которым такое право передано. Разрешение на дается письменно. Письменное разрешение должно четко определять объем коммерческой тайны и круг вопросов, по которым можно предоставлять информацию. В разрешении обязательно указывается должностное лицо фирмы, ответственное за прием и работу с командированными.

В карточке о допуске командированного руководитель должен указать, какие объекты, службы, помещения имеет право посетить командированный. Командированный может присутствовать на совещаниях и советах, рассматривающих только те вопросы, которые определены для него руководителем предприятия.

В Положение о разрешительной системе фирмы необходимо указать, что закрытые совещания по служебным вопросам проводятся только с разрешения руководителя фирмы или его заместителей. Особые требования могут распространяться на заседания ученых советов, совещания по рассмотрению результатов НИОКР и финансово-коммерческой деятельности и т.п. На такие мероприятия рекомендуется в обязательном порядке оформлять разрешительные списки и включать в них лишь тех сотрудников предприятия, которые имеют непосредственное отношение к планируемым мероприятиям и участие в которых вызывается служебной необходимостью.

Как уже отмечалось выше, сотрудники других фирм могут участвовать в закрытых совещаниях только с персонального разрешения руководства фирмы. Готовит списки, как правило, ответственный за организацию совещания в контакте с заинтересованными руководителями структурных подразделений. Список является основанием для организации контроля над

допуском на данное совещание. Перед началом совещания сотрудник СБ предупреждает присутствующих, что обсуждаемая информация носит закрытый характер и не подлежит распространению за пределы установленной фирмой сферы обращения, и выдает инструкции по порядку ведения записей.

Важно подчеркнуть, что установление в фирме определенного порядка обращения с закрытой информацией и изделиями существенным образом повышает надежность защиты коммерческой тайны, снижает вероятность разглашения, утраты носителей этих сведений.

Лекция 17. Создание комплексной системы защиты конфиденциальной информации

1. Введение

При создании комплексной системы защиты конфиденциальной информации необходимо защищать информацию во всех фазах ее существования - документальной (бумажные документы, микрофильмы и т.п.), электронной, содержащейся и обрабатываемой в автоматизированных системах (АС) и отдельных средствах вычислительной техники (СВТ), включая персонал, который ее обрабатывает - всю информационную инфраструктуру. При этом защищать информацию необходимо не только от несанкционированного доступа (НСД) к ней, но и от неправомерного вмешательства в процесс ее обработки, хранения и передачи на всех фазах, нарушения работоспособности АС и СВТ, воздействия на персонал и т.п. Обобщая, можно сказать, что информационная структура должна быть защищена от любых несанкционированных действий. Защищать необходимо все компоненты информационной структуры предприятия - документы, сети связи, персонал и т.д.

Целью работы должно являться построение комплексной системы защиты конфиденциальной информации (далее по тексту КСЗИ). Это предполагает необходимость использования, создания и разработки совокупности методологических, организационных и технических элементов КСЗИ, взаимообусловленных и взаимоувязанных, и базируется на использовании методологии построения комплексной системы защиты конфиденциальной информации. Методологические, организационные и технические компоненты КСЗИ разрабатываются и создаются в рамках трех

параллельных направлений работ - методическом, организационном и техническом.

Методология есть совокупность способов и приемов рассмотрения вопросов информационной безопасности и методов их решения в целях построения комплексной системы информационной безопасности. Она дает возможность в рамках единого подхода использовать согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.

Методология построения комплексной системы защиты конфиденциальной информации описывает основные методы и принципы решения следующих вопросов:

- Обеспечение комплексной безопасности;
- Компоненты комплексной системы защиты информации;
- Направления работ по созданию комплексной системы информационной безопасности;

Основные принципы построения системы комплексной информационной безопасности:

- принцип равномощности (комплексности);
- принцип непрерывности защиты;
- разумная достаточность;
- гибкость системы защиты;
- принцип независимости стойкости СЗИ от раскрытия информации о механизмах ее использования;
- принцип простоты применения.

Основные организационно-методические мероприятия по созданию и поддержанию функционирования комплексной системы защиты:

- создание службы обеспечения конфиденциальности (СОК);
- перечень основных нормативных и организационно-распорядительных документов, необходимых для организации комплексной системы защиты информации.

Рекомендации по методологии построения матрицы конфиденциальности:

- определение объектов и субъектов информационных потоков;
- определение характеристик и признаков объектов и субъектов информационных потоков (матрицы конфиденциальности);

- построение правил разграничения доступа субъектов к объектам информационных потоков на основании матрицы конфиденциальности.

Методика оценки рисков:

- методика анализа угроз конфиденциальной информации и построения неформальной модели нарушителя;
- методика определения общих требований к защищенности автоматизированной системы:
- классификационные требования Гостехкомиссии России к защищенности от НСД средств вычислительной техники и автоматизированных систем;
- классификационные требования ФАПСИ к системам защиты информации;
- основные механизмы защиты компьютерных систем от проникновения с целью дезорганизации их работы и несанкционированного доступа к информации.

Методика определения уровня ЗИ в соответствии с РД ФАПСИ и ГТК.

2. Методическое направление работ по созданию КСЗИ

В рамках методического направления должна быть разработана концепция (политика) безопасности.

Мероприятия по созданию систем защиты конфиденциальной информации, реализуемые вне единого комплекса мер, прописанных в рамках концепции политики безопасности, бесперспективны с точки зрения ожидаемой отдачи по решению проблем безопасности. Под концепцией понимается взаимоувязанный комплекс организационно-технических мер, методологических указаний, регламентов, комплектов форм типовых документов и т.д., решающих задачи защиты конфиденциальной информации.

Концепция (Политика) безопасности - документ, в котором:

- применяется методика определения и описания информационных потоков, описанная в методологии, представляющая собой формальное и точное описание работы с информацией в подразделениях Заказчика, с учетом их изменении со временем, определены критерии, по которым принимается решение о появлении или прекращении конкретного информационного потока;
- анализируются, описываются и фиксируются информационные потоки, существующие при работе с информацией Заказчика на текущий момент;

- определяются для каждого информационного потока фазы существования информации (например, бумажный документ, электронный документ, запись в базе данных);

- определяются категории конфиденциальной информации Заказчика, разрабатывается классификация информации по категориям конфиденциальности;

- проводится категорирование информации по категориям и фазам, создана матрица конфиденциальности;

- определяются возможные пути разглашения конфиденциальной информации (модель угроз);

- для каждой угрозы и атаки определяется модель нарушителя, в которой определяется:

- профессиональный круг лиц, к которому принадлежит нарушитель;

- мотивация нарушителя (цели нарушителя);

- впредполагаемая квалификация нарушителя;

- предполагаемые ограничения на действия и характер возможных действий нарушителя.

- определяются уровни риска для всей матрицы конфиденциальности, вероятности реализации каждой атаки, стоимость ущерба при каждой атаке и усредненные вероятные величины убытков (риски);

- определяются порядок изменения Концепции безопасности и Регламента обеспечения безопасности.

3. Организационное направление работ по созданию КСЗИ

В рамках организационного направления работ создается организационная компонента КСЗИ - совокупность правил (руководящих документов) и технических средств, регламентирующих деятельность сотрудников при обращении с информацией независимо от форм ее представления.

Включает в себя разработку регламента обеспечения безопасности, применение методологии при работе с персоналом Заказчика, при создании СОК, обучение и консультации сотрудников СОК, работы по уточнению требований к характеристикам защищенности системы, анализ информационной структуры Заказчика, разнесение субъектов и объектов информационных отношений по категориям конфиденциальности, определение допустимых формы их взаимодействий и т.д.

Регламент обеспечения безопасности - комплект документов, регламентирующий правила обращения с конфиденциальной

информацией в зависимости от фазы ее обработки и категории конфиденциальности. В регламенте должен быть определен комплекс методических, административных и технических мер, включающих в себя:

- создание подразделения, ответственного за обеспечение конфиденциальности информации (СОК);
- определение порядка допуска сотрудников к конфиденциальной информации;
- определение обязанностей, ограничений и условий, накладываемых на сотрудников, допущенных к конфиденциальной информации;
- установление категории конфиденциальности информации; определение категории конфиденциальности работ, проводимых Заказчиком и информации, содержащейся в документах, связанных с работами; порядок изменения категории конфиденциальности работ и информации;
- требования к помещениям, в которых проводятся конфиденциальные работы и обрабатывается конфиденциальная информация, по категориям;
- требования к конфиденциальному делопроизводству;
- требования к учету, хранению и обращению с конфиденциальными документами;
- меры по контролю за обеспечением конфиденциальности работ и информации;
- план мероприятий по противодействию атаке на конфиденциальную информацию (действия, которые надо предпринимать в случае обнаружения разглашения информации с целью пресечения процесса разглашения/утечки информации);
- план мероприятий по восстановлению конфиденциальности информации (действия, которые надо предпринимать после пресечения процесса разглашения/утечки информации);
- определение ответственности за разглашение конфиденциальной информации.

Для Регламента обеспечения безопасности должны быть разработаны следующие документы:

- Общие документы
- Инструкция по обеспечению режима конфиденциальности на предприятии.
- Требования к пропускному и внутриобъектовому режиму.
- Общие требования к системе разграничения доступа в помещения (СРД).
- Регламент взаимодействия Службы обеспечения конфиденциальности и Службы безопасности.

- Документы по работе с кадрами
- Инструкция по работе с кадрами, подлежащими допуску к конфиденциальной информации.
- Требования к лицам, оформляемым на должность, требующую допуска к конфиденциальной информации.
- Документы по защите АС и СВТ
- Режим конфиденциальности при обработке конфиденциальной информации с применением средств вычислительной техники.
- Определение требований к защищенности Автоматизированной системы.
- Концепция безопасности Автоматизированной системы (АС).
- Анализ существующей АС.

Документы определяют работу комплексной системы защиты информации:
- в штатном режиме;
- изменения в штатном режиме работы;
- нештатный режим (аварийные ситуации).

4. Техническое направление работ по созданию КСЗИ

Техническая компонента КСЗИ - комплекс технических средств и технологий защиты информации (ЗИ) при ее обработке, хранении и передаче, включая криптографические средства. Техническая компонента создается в рамках технического направления работ. При реализации технического направления проводится сбор исходных данных для разработки технических предложений по оснащенности автоматизированной системы (АС) обработки, хранения и передачи информации средствами ЗИ, позволяющими реализовать требуемый уровень защищенности.

АС является составляющей информационной системы предприятия, поэтому подготовка технических предложений хронологически следует за разработкой общей концепции КСЗИ.

Подготовка технических решений проблемы соответствия параметров Автоматизированной Системы установленным требованиям защищенности (определяются в Концепции безопасности) возможна в двух направлениях:
- Разработка АС "с нуля" с учетом требований защищенности;
- Встраивание механизмов защиты в существующую АС посредством наложения некоторого набора аппаратно-программных средств ЗИ, имеющих сертификаты ГТК и ФАПСИ.

Выбор направления предполагает взвешенный анализ сопоставимости результата объемам инвестиций в построение

системы, проводимый в соответствии с методикой оценки рисков, описанной в Методологии построения комплексной системы защиты конфиденциальной информации.

Лекция 18. Этические проблемы ведения деловой разведки

1. *Деловая разведка* – составная часть корпоративной культуры ведения современного бизнеса. Определение основных целей и понятий деловой разведки. Для выживания предприятия в условиях современной конкурентной борьбы первоочередное значение начинает играть разведка намерений конкурентов, изучение основных тенденций бизнеса, анализ возможных рисков и т.д. Дисциплина, изучающая эти аспекты бизнеса, получила на Западе название “деловая разведка” (business intelligence). Поскольку этот термин (далее для краткости ДР) еще не устоялся, в литературе можно встретить также термины “конкурентная разведка”, "бизнес-разведка", которые эквивалентны ДР. Деловая разведка является мощным инструментом исследования рынка и конкурентной среды, и в настоящее время представляет собой бурно развивающуюся дисциплину, возникшую на стыке экономики, юриспруденции и специальных дисциплин. Деловая разведка занимается сбором и анализом информации о конкуренте (собственно разведкой), защитой своей информации (промышленная контрразведка), а также проведением специальных операций (например, защитой имиджа предприятия и руководителя, противодействию “черному” PR и т.д.).

2. *Основное отличие деловой разведки* от промышленного шпионажа – поиск и получение всей необходимой информации исключительно законными (с точки зрения норм существующего права) методами. Отличием деловой разведки от промышленного шпионажа является то, что ДР проводится в рамках действующих правовых норм, и свои результаты получает благодаря аналитической обработке огромного количества разнообразных открытых информационных материалов. Появление новых информационных технологий (сетевых структур типа Internet, коммерческих баз данных, систем поиска информации и т.д.) и относительная дешевизна доступа к информационным ресурсам позволяют аналитикам ДР готовить качественные материалы, пригодные для принятия решений руководством компаний. Методы промышленного шпионажа ориентированы на использование всех доступных средств для получения искомой

информации, включая как прямое нарушение законов (шантаж, подкуп, воровство, насилие и т.д.), так и неэтичные методы (обман, распространение компрометирующих сведений, выпытывание и т.д.). Методы деловой разведки исключают использование уголовно наказуемых средств, и в большей степени ориентированы на цивилизованные способы ведения бизнеса. Однако грань между этичными и неэтичными методами ведения деловой разведки (хотя и при соблюдении в обоих случаев действующих законов) остается очнь размытой. По мере возрастания потребностей в получении ценной деловой информации возрастает роль этических норм. При возникновении проблем с получением информации в подразделении ДР появляются стимулы "срезать углы" и нарушить этические ограничения. Иногда само руководство компании толкает на такие действия, так как для нее неважно, как получена информация, лишь бы была выполнена работа.

3. *Этика работы в Сети Internet*. Сетевое сообщество живет по своим законам, которые необходимо соблюдать. Хотя эти законы не регламентированы, “де-факто” они уже существуют. При ведении разведки в сети и проведении PR-акций (т.е. выполнении функций деловой разведки) необходимо выполнять определенные правила, в частности, при сборе деловой информации не выдавать себя за другое лицо или организацию (зарегистрировавшись под чужим, но известным именем); не заниматься сбором сведений, составляющих коммерческую тайну конкурента (участвуя в электронных конференциях); не переманивать ведущих специалистов конкурента; не “забивать” сайты конкурентов; не публиковать компромат на конкурентов в любой форме;

4. *Два подхода в методах сбора необходимой информации*: Соблюдение законов, но пренебрежение нормами морали (подглядывание, обман при найме на работу, переманивание ведущих специалистов, получение информации из “мусорных ящиков” конкурентов,…) при ведении разведки. В обоих примерах руководством фирм были наняты частные детективы, которые собирали деловую информацию из “мусорных ящиков” конкурентов. Этично ли это? На данный вопрос нет однозначного ответа у профессионалов деловой разведки. Если метод сбора информации легален, всегда ли он соответствует принятым этическим нормам? Все зависит от среды воспитания сотрудника деловой разведки. Люди, вышедшие из недр правительственных

служб, например бывшие оперативники ЦРУ, часто думают и действуют только с точки зрения "буквы закона". Если их действия не выходят за рамки действующего законодательства, то они считают их нормальными. Соблюдение норм морали присущих данному обществу при сборе деловой информации. Однако люди работающие в разведке, воспитанные в академической корпоративной среде, оценивают свои поступки исходя из других принципов, например, стремясь не попасть на страницы скандальной хроники. Большинство профессионалов, работающих в области деловой разведки, не будет восстанавливать и исследовать “мусор” других организаций и обманывать людей под видом приема на работу. Они считают такое поведение неэтичным и в их кругу не приемлемым.

5. *Этические нормы поведения в разных странах.* Этические соображения становятся также чрезвычайно важными по мере того, как компания расширяет свой бизнес и начинает деловые контакты с представителями зарубежных стран. Общепринятые стандарты делового поведения в разных странах различные. Например, в некоторых странах совершенно легальна дискриминация при приеме на работу по признакам пола. В других странах гражданские служащие ожидают вознаграждения за представляемые вам официальные документы. Эта практика также отличается от развитых европейских и североамериканских норм ведения бизнеса.

6. *Деловая разведка и коммерческая тайна.* Важно знать, что хотя противозаконно пользоваться коммерческими тайнами чужих компаний, во многих случаях эти компании потеряли право называть что-то коммерческой тайной из-за своих собственных необдуманных действий. Например, если компания выходит с новым продуктом на рынок, она должна предварительно его запатентовать и проконтролировать, не существует ли какой-то производитель, который может разобрать этот продукт на части и воспроизвести его под своим патентом.

В другом примере, один отечественный завод по производству некоторого класса железобетонных изделий потерял юридическое право, чтобы говорить о способе производства ЖБИ как о коммерческой тайне, потому что администрация завода не позаботилась об охране производственных помещений и не проинформировала служащих о необходимости соблюдения коммерческой тайны. Поэтому любой посетитель завода мог

осмотреть производственную зону и собрать необходимую информацию.

7. Какое поведение соответствует принятым *этическим нормам*? Трудно дать определение, что такое этические нормы поведения. Толковый словарь Вебстера определяет этику как дисциплину, имеющую дело с добром и злом и с нравственным долгом. Для большинства из нас практическое ежедневное применение этических правил очень помогает в жизни. Например, как бы мы почувствовали себя, увидев заметку о своих действиях на первой странице бульварной газеты? Что бы мы чувствовали, если бы активность газетчиков была бы направлена на нас? Почувствовали бы мы заблуждение или обман?

Ответы на эти вопросы и образуют принципы, которым мы должны руководствоваться в нашем поведении при сборе информации. Хотя многие компании декларируют правила этического поведения для своих сотрудников, в действительности, в ежедневной гонке за прибылью этические правила могут не соблюдаться. Говоря о своем служении высокой морали, многие менеджеры вместе с тем находятся под огромным давлением обстоятельств. Они не должны ограничивать возможности своих подразделений деловой разведки по сбору информации определенными рамками. Многие компании награждают свои подразделения ДР за проделанную ими работу, но никогда не поощряют их за то, что эта работа выполнена при соблюдении этических норм. Возможность несоблюдения этических норм поведения при сборе информации администрация аргументирует тем, что конкуренция по своей природе неэтична, поэтому зачем следовать каким-то правилам при проведении деловой разведки. Многие из менеджеров новой формации считают, что было бы неправильным совсем не заниматься мошенничеством, если этим занимаются конкуренты. Этот вопрос является одним из самых трудных, потому что этика изменяется так же, как изменяется и общество. Конечно, к сожалению, приходится согласиться, что мошенничество становится частью нашей культуры. С другой стороны, следует ли поощрять падение нравов, глядя сквозь пальцы на мошенничество, и считать это нормой? Одним из самых трудных вопросов при изучении поведения менеджера является необходимость учитывать психологию человека. Например, хотя все соглашаются, что наем на работу служащих из конкурирующей фирмы лишь для того, чтобы получить их промышленные секреты, является неэтичным, всегда можно убедить себя, что вы нанимаете этого человека только из-за его

высокой квалификации. В большинстве случаев люди переходят из компании в компанию в поисках новых возможностей внутри одной отрасли промышленности и почти невозможно доказать обратное.

8. *Преимущества следования этическим нормам поведения.* Следование этическим нормам является не только правильным с моральной точки зрения, но и экономически выгодно. Возможно, самая важная причина почему надо следовать этическим нормам поведения состоит в том, что такое поведение убережет вашу фирму от судебного разбирательства и связанных с ним затрат. Случаи с фирмами Microsoft и Oracle, Avon и Mary Kay служат хорошим примером. Другая причина, по которой целесообразно следовать этическим нормам поведения, состоит в том, что такое поведение делает жизнь служащих более спокойной и менее напряженной. Зная требования, предъявляемые к ним обществом, люди точно понимают, что им можно делать, а чего нельзя. С них снимается ответственность в выборе решений. Третья причина - доверие к компании и общественному мнению. Репутация одного из руководителей российской компании А, занимающейся гостиничным бизнесом была запятнана, когда он нанял консалтинговую фирму, которая помогала ему собирать информацию об организации гостиничного бизнеса в России. Нанятый им "охотник за головами" (The headhunter) получил несколько интервью у ряда менеджеров таких компаний. Хотя он не лгал, говоря, что сейчас для них есть работа, однако он обещал им ее в будущем. Действительно, некоторых из них впоследствии были наняты в компанию А. Однако, интервьюер в результате бесед получил много информации о гостиничном бизнесе, которую он бы не смог получить никаким другим способом. Ясно, что обещанием работы в будущем можно раскрыть многие секреты в настоящем. Еще раз отметим, что нельзя определить истинные мотивы интервьюера и его методы, но этот случай показался подозрительным для многих наблюдателей.

9. *Этический кодекс деловой разведки.* Для правильной организации своей деятельности компании нуждаются в собственном наборе этических правил - своеобразном кодексе поведения.. Ниже перечислены основные стандарты поведения, связанные со сбором информации. Большинство из них ориентируется на следующие минимальные требования, позволяющие не нарушать законы различного уровня. К ним относятся следующие нормы:

- Незаконны попытки обладания чужой коммерческой тайной.

- Незаконно получение какой-либо информации (составляющая коммерческую тайну или нет) от конкурента силой или обманом.

- Отказ от противоправных действий (например, нарушение чужого права владения или перехват телефонных сообщений) при сборе информации.

- Возврат владельцу конфиденциальной и частной информации, полученной случайно или непреднамеренно. В случае получения конфиденциальной правительственной информации, государственные органы должны быть уведомлены о нарушении государственной безопасности.

Важно отметить, что приобретение информации, о которой вы не знаете, что она "ворованная", или получение секретной информации, о конфиденциальности которой вы не знаете, не является нарушением закона. Однако, после того как вы узнали о ее противозаконном приобретении, невозвращение владельцу или использование ее в своих целях уже может рассматриваться как нарушение.

Поскольку многие менеджеры все еще полагают, что деловая разведка связана с чем-то непорядочным, абсолютно необходимо, чтобы руководитель подразделения деловой разведки представил директору компании "Этический кодекс деловой разведки", который был бы составной частью "Этического кодекса компании" (если он существует). В действительности, специфика кодекса ДР должна заключаться в том, что в нем указываются виды информации, которые можно собирать и которые нельзя собирать, и приводятся дозволенные и недозволенные методы сбора информации. Кодекс также должен включать положения о поведении сотрудников ДР при случайном получении запрещенной информации, например конфиденциальных заметок или личных писем. В течение длительного времени приверженцы этического поведения утверждают, что нарушение норм морали и снижение этических стандартов общества приведет к огромным затратам на обеспечение его безопасности. В качестве аргумента выдвигается тезис, что если повсеместно этические стандарты ухудшаются, бизнесменам придется больше платить, чтобы защитить себя от агрессивной тактики поведения конкурента, которая может стать общепринятой нормой поведения в деловом мире, и тогда превентивные меры могут оказаться очень дорогими. Подходящей аналогией может служить та цена, которую общество платит из-за того, что не дает всем детям правильного воспитания с детства. Обществу приходится

затрачивать огромные средства на содержание в тюрьме преступника и устранение последствий его преступлений, причем эти средства значительно больше, чем потребовались бы на воспитание законопослушного гражданина.

Можно сделать вывод, что если в деловом сообществе будет стремительно распространяться неэтичное поведение, то у высшего руководства не будет иного выхода, как ограничить информацию для своих сотрудников. Это может привести к недоверию среди служащих и к нежеланию работать с большей эффективностью - как утверждает адъюнкт-профессор Гарвардской школы бизнеса Лин Шарп Пейн (Lynn Sharp Paine), в журнале деловой этики Journal of Business Ethics. Ограничения пользованием служебным телефоном и ограниченный доступ к внутрифирменной информации для служащих компании, желающих расширить свои знания, налагают очевидные препятствия на внутренний обмен информацией, жизненно важной для фирмы. Когда исследователям отказывали в представлении информации о проектах, над которыми они сами работали, и в сведениях о том, как их работа связана с работой других людей, они тем самым отсекались от побудительной и творческой полезной информации. Для сбора требуемой информации нет необходимости нарушать Этический Кодекс. Даже для этой молодой дисциплины - деловой разведки - действуют старые истины. Одна из них гласит: "85% информации, которая Вам необходима, находится в общественном пользовании. Другие 15%, возможно, вам и не потребуются никогда". Некоторые аналитики говорят о 90%. Используя экспертный анализ и соблюдая этические нормы, профессионалы деловой разведки в состоянии выполнять свою работу квалифицированно и эффективно. Ниже в качестве примера приводится Этический Кодекс, составленный американским “Обществом профессионалов конкурентной разведки” (Society of Competitive Intelligence Professionals) для своих членов.

10. *Этический Кодекс* американского общества профессионалов конкурентной разведки.

Постоянно старайся увеличить уважение и признание к этой профессии на всех государственных уровнях

Выполняй свои служебные обязанности с рвением и прилежанием, поддерживай самый высокий уровень профессионального мастерства и избегай всех неэтичных поступков

Оставайся верным политике компании, ее целям и общему курсу и выполняй обещания, данные своей компании

Выполняй все действующие законы

Во время делового свидания предоставляй всю относящуюся к делу информацию, включая принадлежность к организации

Соблюдай правила работы с конфиденциальной информацией

Действуй в полном соответствии с этими этическими стандартами при работе внутри компании, при ведении переговоров и во всех ситуациях, когда придется работать по специальности.

11. *Правила поведения* компании Fuld & Company. Частные службы и самостоятельные консультанты КР должны также объявить, какие виды деятельности им разрешены, а какие запрещены и осуждаются ими. Например, ведущая американская компания в области деловой разведки Fuld & Company, опубликовала свои собственные этические правила поведения, названные "Десять заповедей легального сбора разведывательной информации". По этим заповедям сотрудники компании не должны:

Лгать, когда представляетесь.

Нарушать официальную генеральную линию вашей компании.

Записывать на диктофон разговор с собеседником без его разрешения.

Предлагать взятки.

Устанавливать подслушивающие устройства.

Умышленно вводить собеседника в заблуждение при переговорах.

Получать от конкурента и передавать ему ценную конфиденциальную информацию.

Распространять дезинформацию.

Воровать промышленные секреты.

Осознанно давить на собеседника с целью получения требуемой информации, если это может подвергнуть опасности его жизнь или репутацию.

Наконец высший управленческий персонал должен следить за тем, чтобы этические нормы соблюдались не только в конкурентной разведке, но и в самой компании в целом.

Заключение

Безопасность ценной документируемой информации определяется степенью ее защищенности от последствий

экстремальных ситуаций, в том числе стихийных бедствий, а также пассивных и активных попыток злоумышленника создать потенциальную или реальную угрозу несанкционированного доступа к документам с использованием организационных и технических каналов, в результате чего могут произойти хищение и неправомерное использование злоумышленником информации в своих целях, ее модификация, подмена, фальсификация, уничтожение.

Главным направлением защиты документированной информации от возможных опасностей является формирование защищенного документооборота, то есть использование в обработке и хранении документов специализированной технологической системы, обеспечивающей безопасность информации на любом типе носителя. Таким образом, защищенность документопотоков достигается за счет:

1) одновременного использования режимных (разрешительных, ограничительных) мер и технологических приемов, входящих в систему обработки и хранения конфиденциальных документов;

2) нанесения отличительной отметки (грифа) на чистый носитель конфиденциальной информации или документ, в том числе сопроводительный, что позволяет выделить их в общем потоке документов;

3) формирования самостоятельных, изолированных потоков конфиденциальных документов и (часто) дополнительного их разделения на подпотоки в соответствии с уровнем конфиденциальности перемещаемых документов;

4) использования автономной технологической системы обработки и хранения конфиденциальных документов, не соприкасающейся с системой обработки открытых документов.

Приложение 1
Анализ системы конфиденциального делопроизводства в организации ОАО «Газпром-нефть»

1. Общая характеристика организации.

«Газпром нефть» – одна из крупнейших и быстрорастущих нефтегазовых компаний России.

Основными видами деятельности Компании являются разведка, разработка, добыча и реализация нефти и газа, а также производство и сбыт нефтепродуктов. «Газпром нефть» осуществляет свою деятельность в крупнейших нефтегазоносных

регионах России: Ханты-Мансийском и Ямало-Ненецком автономных округах, Томской и Омской областях. Основные перерабатывающие мощности компании находятся в Омской, Московской и Ярославской областях. Собственные доказанные запасы нефти компании «Газпром нефть» превышают 4 миллиарда баррелей, что ставит ее в один ряд с двадцатью крупнейшими нефтяными компаниями мира. Ресурсная база «Газпром нефти» ежегодно увеличивается за счет приобретения новых активов в России и за рубежом.

В состав группы «Газпром нефть» входят более 40 нефтедобывающих, нефтеперерабатывающих и сбытовых предприятий из 18 регионов РФ и стран ближнего зарубежья, объединенных по принципу вертикальной интеграции. Компания перерабатывает более 60 % добываемой нефти, демонстрируя лучшее в отрасли соотношение добычи и переработки.

Продукция «Газпром нефти» экспортируется в 48 стран мира и реализуется на всей территории РФ через разветвленную сесть собственных сбытовых предприятий. В настоящее время в управлении Компании находится около 900 АЗС в России и странах СНГ.

По итогам 2008 года «Газпром нефть» вошла в пятерку ведущих российских нефтяных компаний по объемам добычи и переработки нефти, а также сбыта нефтепродуктов.

В соответствии с Уставом, структура органов управления «Газпром нефти» включает в себя: общее собрание акционеров, совет директоров, коллегиальный исполнительный орган (Правление) и единоличный исполнительный орган (Генеральный директор). Эффективная работа органов управления «Газпром нефти» обеспечивает стабильное развитие Компании, а также служит залогом доверия акционеров, инвесторов и партнеров.

2. Система делопроизводства, критерии отнесения документов к различным категориям в организации.

На предприятии ОАО «Газпром-нефть» утверждены правила документооборота, устанавливающие принятую классификацию документов, регламентирующие порядок хранения и уничтожения документов, а также устанавливающие основные правила пользования электронной почтой.

В соответствии с данными правилами документооборота документы на предприятии распределяются на четыре основные группы: для ограниченного пользования, личные и конфиденциальные, конфиденциальные и прочие.

К документам для ограниченного пользования относится особо важная информация, хранение которой должно контролироваться. Несанкционированное раскрытие данной информации может нанести непоправимый вред компании. В соответствии с этим передача такой информации осуществляется только при наличии официального разрешения на передачу, доставку или вскрытие документов. На территории компании осуществляется передача с посыльным. Внутренние и внешние рассылки упаковываются в запечатанный конверт, внутри которого наносится маркировка «для ограниченного доступа» и заметка «лично в руки». При электронной коммуникации тщательно контролируется доступ к системе и паролю. Хранение таких документов обязательно в недоступном месте.

К личным и конфиденциальным документам относится информация, которая принадлежит одному человеку. Несанционированное раскрытие ее может значительным образом изменить отношения со служащими клиентами, или компанией в целом. Ограничения на эту информацию применяются в соответствии с законодательством Российской Федерации.

К конфиденциальным документам относится информация, которая является важной для бизнеса компании и составляет собственность компании. Включает информацию о коммерческих клиентах, поставщиках, дилерах и продавцах. Несанкционированное раскрытие ее может повлечь негативные последствия для компании, деловых отношений, коммерческих клиентов, дилеров или продавцов. Доступ к такой информации осуществляется только по деловой необходимости при обязательном предупреждении об ответственности за документ. Необходимо разрешение на раскрытие информации для других лиц. Необходимо подходить с осторожностью к использованию общих принтеров.

К прочим документам относится информация, которая не требует особого хранения. Несанкционированное раскрытие практически не отражается на делах компании. Доступ к такой информации имеется у всех служащих, однако требуется наличие производственной необходимости. При передаче такой информации требуется разрешение руководства на обнародование информации в соответствии с принципами компании и авторского права.

3. Правила документооборота конфиденциальной документации, принятые в организации.

При хранении документов в компании приняты следующие правила. По степени важности документы делятся на три категории, для каждой из которых сформированы собственные требования к организации хранения.

К первой категории относятся документы, крайне необходимые для ведения дел компании или важные для ознакомления с ее прошлым. Их потеря повлияет на финансы компании, связи с общественностью, отношения со служащими, акционерами, клиентами или поставщиками; документы также могут быть запрошены по юридическому, законодательному или экологическому требованию.

Ко второй категории относятся документы, имеющие определенный период хранения и важные для совершения ежедневных операций, они могут быть конфиденциальными.

К третьей категории относятся документы, не требующие особого хранения. Их отсутствие не повлияет на работу компании. Они не являются важными для ознакомления с прошлым компании, не являются конфиденциальными, не затрагивают вопросы частного характера. Не имеют особой важности для выполнения ежедневных операций.

Наивысшие требования к организации хранения предъявляются к хранению документов первой категории, в соответствии с которыми:

- доступ к этим документам должен быть строго ограничен;
- необходимо контролировать температуру и влажность в помещении с хранящимися документами;
- система с документами должна иметь резервную копию, которая может быть необходима при восстановлении потерянной информации.

Также разработаны общие требования к хранению документов первой и второй категории, которые соответствуют общепринятым и законодательно установленным требованиям к хранению документов.

Для документов третьей категории никаких требований к хранению не установлено.

Для успешного ведения дел необходимо, чтобы документы создавались, использовались и уничтожались в соответствии с Уставом Компании. Уничтожение документов является необходимым, и должно осуществляться разумно, следуя всем нормативным указаниям. Неаккуратное уничтожение документов может повлечь за собой раскрытие конфиденциальной информации.

В соответствии с этими принципами в ОАО «Газпром-нефть» разработана политика уничтожения документов, основные принципы которой изложены ниже.

Уничтожение какого-либо документа обязательно должно сопровождаться удалением его копии. Как определено в Корпоративном Руководстве Безопасности, есть три категории документов, которые требуют особого внимания при их создании, использовании и уничтожении: с ограниченным доступом, личные и конфиденциальные и конфиденциальные. Документы такого рода удаляются так, чтобы их восстановление было невозможным.

В основе организации контроля исполнения служебных документов в ОАО «Газпром-нефть» лежат принципы:

- заблаговременности;
- объективности: важно, чтобы контроль опирался на точные, объективные и научно обоснованные нормативы;
- открытости: подчиненные должны знать, что, как, и по каким решениям контролируют; о результатах контроля надо уведомлять подчиненного;
- системности: контроль должен касаться каждого участка работы, а не только предпочтительных, по мнению начальства;
- индивидуального подхода.

Игнорирование перечисленных принципов контроля приводит к снижению результатов работы органов предприятия, его аппарата.

Основными задачами, которые решает контроль в системе управленческой деятельности, являются повышение ответственности должностных лиц и эффективности управления и эффективное использование системы делопроизводства, обеспечение отлаженности, целесообразности и точности прохождения документов по адресам.

В практической деятельности предприятия применяется два метода контроля: внутренний и внешний контроль.

Внешний контроль осуществляется со стороны вышестоящих органов. Каждую неделю в понедельник от контрольно-аналитического управления приходит информация с указанием документов, срок которых истекает через неделю. В случае неисполнения документа, стоящего на контроле в Администрации предприятия в срок, и непредставления при этом в адрес контрольно-аналитического управления обоснования со стороны предприятия данный вопрос выносится на рассмотрение губернатора области.

Внутренний контроль в ОАО «Газпром-нефть», проверку исполнения документов, а также постановлений и распоряжений

осуществляет канцелярия предприятия. Также на предприятии издан Приказ о совершенствовании организации контроля в ОАО «Газпром-нефть», в котором назначается ответственный за организацию контроля на предприятии, а также даются указания начальникам структурных подразделений о принятии мер по совершенствованию контрольной работы на предприятии ОАО «Газпром-нефть».

Внутренний контроль охватывает три группы вопросов:

- контроль исполнения документов по существу содержащихся в них заданий. Такой контроль подразумевает оценку правильности и полноты решения поставленного вопроса. В ОАО «Газпром-нефть» такую оценку дает директор либо по его поручению заместитель директора. Если директор согласен с решением данного вопроса, то документ подписывается, если же данное решение его не устраивает, то документ возвращается исполнителю на доработку;

- контроль соответствия документов требованиям ГОСТов. Данный контроль заключается в проверке правильности оформления документа, полноты реквизитов, наличия всех приложений. Такой контроль осуществляется как сотрудниками канцелярии, так и ответственными исполнителями самостоятельно;

- контроль исполнения документов в установленные сроки. Данный вид контроля осуществляет канцелярия ОАО «Газпром-нефть».

В ОАО «Газпром-нефть» обязательному контролю подлежат все распорядительные документы, особенно имеющие конкретные поручения о представлении отчетов, информации.

Директором утвержден перечень документов, подлежащих контролю.

При постановке документа на контроль на нем проставляется отметка о контроле, которую обозначают штампом «Контроль», и указывается дата истечения срока исполнения данного документа.

Каждую неделю работники канцелярии распечатывают отчет о выполнении контрольных поручений в подразделениях Учреждения, срок которых истекает через неделю, и раздают исполнителям в качестве напоминаний.

Все поручения исполняются в указанные в них сроки. Если в документе срок исполнения не указан, то ставятся типовые сроки, установленные законодательными и другими актами.

Если в тексте поручения содержится указание «Срочно», то документы исполняются в 3-дневный срок, а требующие дополнительного изучения поставленных вопросов - в течение 10

дней. Также в 10-дневный срок исполняются поручения, содержащие в тексте указание «Оперативно».

Продление сроков исполнения поручения производится на основании представления через канцелярию на имя руководителя, давшего поручение, мотивированной просьбы о продлении этого срока и о причинах отсрочки, причем не позднее чем за 5 дней до истечения ранее установленного срока.

Решение о продлении срока исполнения поручения принимается руководителем, установившим срок. Канцелярия сообщает о принятом решении исполнителю: возвращает ему для приобщения к делу рассмотренную записку о продлении срока.

Канцелярия несет полную ответственность за соблюдение исполнителями сроков ответа по документам. Если исполнитель не предоставил ответ на документ и не написал промежуточного, с просьбой о продлении срока исполнения, заведующий канцелярией пишет служебную записку на имя директора с указанием нарушения.

Поручение считается исполненным, если представленная информация о выполнении предусмотренных в ней заданий принята и по ней не даны дополнительные поручения. Поручение снимается с контроля должностным лицом, давшим поручение. Отметка об исполнении документа также проставляется в журнале и контроль снимается.

Канцелярия обеспечивает контроль, сбор, обработку, обобщение поступающей информации о ходе и результатах выполнения контролируемых документов и поручений, а также осуществляет взаимодействие по этим вопросам с контрольно-аналитическим управлением Администрации.

Таким образом, контроль представляет собой совокупность процессов и методов, обеспечивающих стабильность деятельности предприятия.

Организация эффективного внутреннего и внешнего контроля является обязательным элементом управления. Проверка качества и своевременности исполнения решений и распоряжений различных уровней управляющей системы должна проводиться постоянно. Именно тогда контроль становится эффективным.

4. Основные направления повышения эффективности конфиденциального документооборота в организации.

Основой современной организации рациональной и оперативной работы по созданию и обработке огромного потока документов в организациях стали персональные компьютеры (ПК).

Компьютерные технологии радикально изменили сам характер труда в делопроизводстве и управлении.

Перечислим основные возможности компьютерных технологий в делопроизводстве:

•помощь в создании документа (конструирование бланков для организации; подготовка документа и размещение его в памяти; использование шаблонов в создании документов; поиск, хранение и редактирование текста документов);

•передача документа на расстояние любому адресату, у которого есть факсимильная связь или ПК и модем (документ передается в электронном виде с компьютера на компьютер, в компьютерной локальной сети, а также с помощью электронной почты и сети Интернет);

•регистрация документа (заполняется регистрационная карточка на экране ПК, а регистрационный номер наносят на сам документ в штамп для отметки о получении документа);

•контроль за исполнением документа (в электронной карточке делается отметка о контроле, и это автоматически позволяет информировать руководство организации об уровне исполнительской дисциплины работающих сотрудников, а также составлять разного рода справки-отчеты по документообороту);

•перевод текста документа с одного языка на другой (осуществляется в автоматическом режиме при наличии соответствующего пакета программ и дополнительном редактировании текста);

•защита документов (от случайного доступа к информации в ПК; восстановление текста; антивирусная защита).

Внедрение электронного документооборота в организации позволяет повысить эффективность труда его сотрудников за счет сокращения времени на поиск, разработку, тиражирование и пересылку документов. В то же время следует учесть, что использование ПЭВМ в документообороте организации зачастую наталкивается на многочисленные препятствия – финансовые, программно-технические и психологические.

При внедрении подобных систем необходимо следовать некоторым общим принципам, которые позволят избежать серьезных ошибок.

К принципам внедрения электронного документооборота в организации следует отнести:

–постепенное увеличение удельного веса ПЭВМ при создании документов (особенно внутри организации);

–своевременную модернизацию технического и программного обеспечения;

–первоочередное использование ПЭВМ для сокращения рутинных операций при создании документов;

–предпочтительное использование ПЭВМ на этапах документооборота с наибольшими временными затратами (как правило, при переписке);

–ясное понимание необходимости внедрения подобных систем руководством организации.

Автоматизация и механизация работы с документами направлены на повышение оперативности управленческого труда, сокращение трудозатрат на документирование, обработку и передачу, использование документной информации, усиление контроля исполнения и упорядочение документооборота.

Автоматизированная работа с документами осуществляется путем создания и внедрения специальных программ с использованием ПЭВМ и автоматизированных рабочих мест (АРМ). При этом должна быть обеспечена информационно-техническая совместимость средств вычислительной техники между собой и с централизованными базами данных.

Автоматизированная подготовка документов осуществляется в основном на АРМ в структурных подразделениях организации. Документ, подготовленный средствами вычислительной техники, может использоваться в работе на правах подлинника.

Автоматизированная регистрация документов может производиться также децентрализованно, в местах регистрации документов на АРМ структурных подразделений и в канцелярии предприятия. Запись производится непосредственно с документа с использованием установленного единого набора обязательных реквизитов. Запись на машинном (магнитном, оптическом и т. п.) носителе должна дублироваться машинограммой контрольно-учетной карточки, которая используется в качестве справочной картотеки.

На базе данных автоматизированной регистрации документов строится автоматизированная информационнопоисковая система, обеспечивающая информационными данными обо всех документах и месте их нахождения при помощи вывода информации на экран дисплея или изготовления машинограмм. При этом должна соблюдаться совместимость традиционной и автоматизированной систем регистрации и поиска.

Автоматизированный контроль исполнения документов строится на базе данных автоматизированной регистрации и обеспечивает оперативное информирование исполнителей группы контроля о состоянии исполнения всех документов, а также

предварительный контроль сроков исполнения документов, анализ исполнительской дисциплины.

Напоминания исполнителям о сроках исполнения, сводки состояния исполнения, сведения о переносе сроков и т.д. выводятся на экран дисплея.

Руководство предприятия должно нести ответственность за эффективность использования автоматизированной технологии работы с документами, определять право доступа сотрудников к информации, хранящейся на машинных носителях.

В настоящее время на платформе Microsoft существует целый ряд систем автоматизации делопроизводства и документооборота, отвечающих современным требованиям. В качестве примера будет рассмотрена система «Дело».

Данная система автоматизации делопроизводства и документооборота (далее САДД) полностью соответствует существующей делопроизводственной практике. Она обеспечивает ведение множества электронных картотек, которые, однако, являются при этом подмножествами единой картотеки органа власти. При этом резолюции и связанные с ними документы автоматически перемещаются между картотеками в соответствии с принятой технологией прохождения документов.

Таким образом, в любой момент времени имеется полная информация о состоянии, истории движения и исполнения документов. Данный комплекс программного обеспечения (ПО) позволяет также решить проблему координации работы с документами в территориально-распределенных подразделениях или представительствах. Обеспечивается обмен документами и резолюциями с использованием современных систем связи между подразделениями.

Основные факторы эффективности автоматизации документооборота с использованием предлагаемого программного решения:

•Экономия организационно-технических затрат, связанных с размножением и перемещением документов, регистрацией работы с ними.

•Упорядочение технологии работы с документами. Внедрение единой компьютерной технологии позволяет предприятию перейти на единую систему делопроизводства и документооборота.

•Ускорение прохождения документов на предприятии за счет эффективной электронной технологии рассылки документов и резолюций.

•Полный контроль за документами и работой персонала с ними. Средства системы позволяют осуществлять как оперативный контроль за деятельностью предприятия, так и аналитическую обработку накапливаемых данных о документах и работе с ними персонала.

Основа предлагаемого решения — система автоматизации делопроизводства и документооборота — является современным масштабируемым решением.

Предлагаемое решение обладает средствами контроля за документооборотом — от непосредственного контроля руководителем за исполнением собственных резолюций до контроля статистических параметров документооборота отдельных подразделений и ОАО «Газпром-нефть» в целом.

Текущий контроль исполнения резолюций осуществляется по записям в папке «На контроле» кабинета автора резолюции. РК находятся в этой папке с момента вынесения контрольной резолюции до утверждения автором резолюции отчета ответственного исполнителя.

Общий контроль исполнения резолюций осуществляется с помощью отбора РК по различным реквизитам резолюций, который производится с помощью функции Поиск. При этом отбор может производиться:

•для каждой картотеки и для всех картотек сразу;

•за определенный период времени регистрации РК или наложения резолюции;

•по авторам и исполнителям резолюций;

•по контрольным или неконтрольным резолюциям;

•по находящимся на контроле или снятым с контроля резолюциям;

•по резолюциям, выполненным в срок или с нарушением срока.

Также контроль исполнения можно осуществлять с помощью отчетов, получаемых при работе с отчетными формами системы автоматизированного документооборота.

Еще один способ эффективного контроля за ходом процесса по исполнению резолюции — сквозное взаимное соответствие сроков на всех технологических уровнях подготовки внутреннего или исходящего документа.

Контрольные сроки исполнения документа, определенные в резолюции, автоматически доводятся до исполнителей и учитываются средством автоматизации их деятельности. При подготовке сложных документов, где несколько исполнителей отвечают за отдельные разделы, обычно применяется

программный продукт Microsoft Project. В меньших рабочих группах контрольные механизмы системы автоматизированного документооборота могут напрямую взаимодействовать со списками задач, ведущихся в почтовых системах Microsoft Outlook непосредственных исполнителей. Однако пример системы контроля интереснее рассматривать на более сложном примере, когда исполнением резолюции занято крупное подразделение.

Помимо непосредственного контроля в кабинете, система автоматизированного документооборота и делопроизводства предоставляет следующие виды контроля с использованием отчетов:

•Сведения о документообороте. Отчет содержит данные об объеме документооборота какого-либо структурного подразделения, имеющего собственную картотеку, по группам документов за указанный период времени. При формировании отчета учитываются документы, находящиеся в текущей картотеке.

•Сводка об исполнении контрольных документов. Эта сводка содержит сведения о количестве исполненных и находящихся на исполнении контрольных документов. Сводка формируется по документам текущей картотеки, т.е. в сводке учитываются документы, резолюции на которые наложены должностными лицами, приписанными к текущей картотеке. Сводка об исполнении контрольных документов может быть обобщенной или по ответственным исполнителям. При этом сводка может составляться для документов с заданным интервалом дат регистрации (в отчет попадают сведения о количестве документов, имеющих контрольные резолюции) и для резолюций с заданным интервалом плановых дат (в отчет попадают сведения о количестве контрольных резолюций).

Отдельный аспект контроля — протоколирование действий пользователя с РК. В системе предусмотрена автоматическая регистрация всех изменений, вносимых в РК. С этой целью для каждой карточки ведется протокол изменений основного и дополнительных разделов РК, а также протоколы изменений резолюций. Для каждого изменения в протоколе регистрируется дата и время, характер выполненных действий и фамилия пользователя.

Приложение 2

Пример приказа об организации работы по защите конфиденциальной информации (компания ОАО «ФСК ЕЭС»)

ПРИКАЗ
17.05.2004
№ 105

Об организации работы
по защите конфиденциальной
информации

В целях организации работы по защите конфиденциальной информации, с учетом требований Гражданского Кодекса Российской Федерации, Федеральных законов «Об акционерных обществах», «Об информации, информатизации и защите информации», «О рынке ценных бумаг», «Об электронной цифровой подписи», указов Президента Российской Федерации от 06.03.1997 № 188, от 24.01.1998 № 61, постановления Правительства Российской Федерации от 05.12.1991 № 35, специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К –2002) Государственной технической комиссии при Президенте Российской Федерации,

ПРИКАЗЫВАЮ:

1. Утвердить:

1.1. Перечень сведений, содержащих конфиденциальную информацию в ОАО «ФСК ЕЭС» (далее - Перечень) согласно приложению 1.

1.2. Положение о порядке организации и проведения работ по защите конфиденциальной информации в ОАО «ФСК ЕЭС» (далее - Положение) согласно приложению 2.

1.3. Инструкцию о порядке работы с конфиденциальной информацией в ОАО «ФСК ЕЭС» (далее - Инструкция) согласно приложению 3.

2. Возложить ответственность за выполнение требований по защите конфиденциальной информации, в соответствии с Положением и законодательством Российской Федерации, на руководителей структурных подразделений исполнительного аппарата, филиалов и других обособленных подразделений ОАО «ФСК ЕЭС».

3. Руководителям структурных подразделений исполнительного аппарата, генеральным директорам филиалов ОАО «ФСК ЕЭС»:

3.1. Организовать работу с конфиденциальной информацией в структурных подразделениях в соответствии с утвержденными Перечнем, Положением и Инструкцией.

3.2. Ознакомить под роспись с настоящим приказом, Перечнем, Положением и Инструкцией всех работников, допущенных к сведениям, содержащим конфиденциальную информацию.

3.3. При подготовке конфиденциальных документов как на бумажных носителях, так и в электронном виде, строго руководствоваться Перечнем сведений, содержащих конфиденциальную информацию в ОАО «ФСК ЕЭС».

Запрещается размещать сведения, содержащиеся в Перечне, на не предназначенных для этой цели носителях, использовать в открытых публикациях, в интервью или каким-либо иным способом предавать их огласке без письменного разрешения Председателя Правления ОАО «ФСК ЕЭС» или его заместителей.

4. Требования Положения и Инструкции в части работы с конфиденциальной информацией в электронном виде вступают в силу с момента ввода в эксплуатацию корпоративной системы электронного документооборота и утверждения соответствующей инструкции.

5. Контроль за правильностью отнесения сведений к конфиденциальной информации возложить на Специальную дирекцию (Осипов А.А.).

6. Контроль за исполнением настоящего приказа оставляю за собой.

Председатель Правления А.Н. Раппопорт

Приложение 1
к приказу ОАО «ФСК ЕЭС»
от 17.05.2004 № 105

ПЕРЕЧЕНЬ
сведений, содержащих конфиденциальную информацию
в ОАО «ФСК ЕЭС»

1. Сведения в области организационно-управленческой деятельности

1.1. Сводные сведения об исполнении программ управления издержками производства Общества.

1.2. Структура построения корпоративной локальной вычислительной сети (ЛВС) Общества.

1.3. Сведения о создании и функционировании корпоративной информационной системы управления Общества.

1.4. Сведения о планируемых изменениях в структуре управления Обществом, его филиалами и другими обособленными подразделениями.

1.5. Сведения о цели командирования Председателя Правления Общества или его заместителей.

2. Сведения о финансово-экономической деятельности

2.1. Прогнозный баланс.

2.2. Бизнес-планы Общества.

2.3. Сводные сведения, содержащие плановые и итоговые показатели по расчету тарифов за услуги по передаче электроэнергии и размеров платы за потери электроэнергии (за месяц и более).

2.4. Сведения об остатках на счетах Общества в банках.

2.5. Сведения о путях и способах получения информации из бухгалтерской автоматизированной базы данных.

2.6. Сводные сведения о поступлении денежных средств на расчетные счета Общества за квартал и более.

2.7. Сводные сведения о списании денежных средств с расчетных счетов Общества за квартал и более.

2.8. Сведения о наличии ценных бумаг.

2.9. Сведения, связанные с функционированием системы «Банк-Клиент».

2.10. Сведения о страховании оборудования подстанций и воздушных линий.

2.11. Сводные сведения (кроме тех, которые разработаны и утверждены Правительством Российской Федерации и федеральными органами исполнительной власти, регулирующими деятельность субъектов естественных монополий) о контрагентах, условиях и ценах по договорам, которые заключаются Обществом или ведутся переговоры об их заключении, в том числе по технологическому присоединению к сетям, находящимся в пользовании Общества.

2.12. Сводные сведения о результатах анализа финансово-хозяйственной деятельности за месяц, квартал, год.

3. Сведения в области науки и технологий

3.1. Сведения, содержащие прогнозные оценки научно-технического прогресса в области электроэнергетики.

3.2. Сведения, раскрывающие существо новейших достижений в области науки и техники (в том числе открытия, изобретения, промышленные образцы, полезные модели, рационализаторские предложения, научно-технические решения,

технологические разработки или другие объекты интеллектуальной собственности), которые определяют качественно новый уровень возможностей энергетики.

3.3. Сведения в области науки и техники (в том числе открытия, изобретения, промышленные образцы, полезные модели, рационализаторские предложения, научно-технические решения, технологические разработки или другие объекты интеллектуальной собственности), позволяющие повысить возможности или приводящие к усовершенствованию существующих технологических процессов в электроэнергетике.

3.4. Сведения, раскрывающие существо новейших достижений в области науки и технологий, которые могут быть использованы в создании принципиально новых изделий и технологических процессов в области электроэнергетики.

3.5. Сведения о целевых программах научных исследований в области разработки новых эффективных средств защиты от коррозии опор высоковольтных линий, оборудования, машин и сооружений.

4. Сведения в области научно-технического сотрудничества

4.1. Сведения о принципах построения управления единой энергетической системой России, применяемые только в РФ и представляющие, в связи с этим, интерес для иностранных партнеров.

4.2. Сводные сведения по анализу состояния используемой техники и перспективах применения новых технологических процессов в технике.

4.3. Сведения о планируемых закупках на сумму, превышающую 3 (три) миллиона рублей, за исключением сведений, предназначенных для проведения конкурсов (торгов) по выбору поставщиков и подрядчиков.

4.4. Сводные сведения о плане технического перевооружения сетевого хозяйства и подстанций на год.

4.5. Сведения о требованиях, предъявляемых к предполагаемым участникам конкурса (тендера) до момента его начала.

5. Сведения о международном сотрудничестве

5.1. Сведения о результатах международных встреч и переговоров, если это предусмотрено в ходе встреч (переговоров).

5.2. Сведения о планируемых международных программах совместных действий и исследований.

5.3. Сводные сведения об иностранных участниках совместных проектов.

6. Сведения о социально-бытовых отношениях

6.1. Персональные данные работников.

6.2. Сведения о содержании трудовых договоров с Председателем Правления, заместителями Председателя Правления, членами Правления, руководителями филиалов и ДЗО Общества.

6.3. Штатное расписание работников исполнительного аппарата и филиалов Общества.

6.4. Сводные сведения о действующей системе по оплате и мотивации труда, льготах, компенсациях, медицинском обслуживании, страховании работников исполнительного аппарата и филиалов Общества.

6.5. Сведения, содержащиеся в трудовых договорах работников исполнительного аппарата и филиалов Общества.

7. Сведения о поддержании надлежащего состояния сетевых объектов

7.1. Сведения о методах и способах реализации обеспечения информационной безопасности в корпоративной ЛВС Общества.

7.2. Информация и документы, в которых рассматриваются вопросы защиты информации, создаваемой, обрабатываемой и хранящейся в средствах вычислительной техники, а также циркулирующей в ЛВС Общества.

7.3. Сводные сведения о техническом состоянии воздушных линий (ВЛ) и оборудовании подстанций (ПС).

7.4. Сводные сведения по актам расследования технологических нарушений (АРТН) и охране труда (АРМСОТ).

7.5. Оперативная информация о нарушениях в работе магистральных электрических сетей, имеющих признаки аварий.

7.6. Сводные сведения о технологических нарушениях в работе МЭС, содержащих информацию о числе аварий и инцидентах, недоотпуску электроэнергии потребителю и связанным с этим экономическим ущербом.

7.7. Технические и цифровые характеристики электрических сетей, а также мощности подстанций контрагентов Общества, содержащихся в информационной базе данных по присоединенной мощности.

8. Сведения в области гражданской обороны и об аварийных ситуациях

8.1. Сведения о наличии и дислокации объектов гражданской обороны.

8.2. Сводные сведения об аварийных отключениях, повлекших за собой:

- нарушение условий поставок электроэнергии по контрактам с зарубежными странами;

- прекращение электроснабжения крупных предприятий промышленности, транспорта, связи, добычи и транспортировки газа и нефти, их переработке, городов и жилых районов;

- отключение блоков и генераторов АЭС, снижение перетоков мощности с отключением нагрузки потребителей в дефицитной части, выделение части энергосистемы на изолированную работу.

8.3. Сводные сведения о пожарах, произошедших на объектах Общества.

8.4. Отчетные данные по охране труда, травматизму, в том числе смертельному на объектах Общества.

8.5. Сводные сведения о затратах на охрану труда и на возмещение ущерба пострадавшим от несчастных случаев.

9. Сведения об обеспечении безопасности объектов электроэнергетики

9.1. Сведения об организации и состоянии выполнения работ по защите конфиденциальной информации в Обществе.

9.2. Сведения о выявленных причинах и обстоятельствах нарушения утвержденного порядка защиты конфиденциальной информации в подразделениях Общества и мероприятиях по устранению и предупреждению таких нарушений.

9.3. Сведения о факте и существе проводимых мероприятий с целью обеспечения пожарной безопасности в исполнительном аппарате и филиалах Общества.

9.4. Порядок получения доступа к защищаемым информационным ресурсам.

9.5. Сведения о принципах построения, структуре и местах размещения инженерно-технической защиты исполнительного аппарата и объектов филиалов Общества, позволяющие получить доступ в охраняемую зону или к информации.

9.6. Сведения о фактическом состоянии системы физической защиты объектов Общества.

10. Сведения в области геодезии, топографии, картографии, аэросъемок

10.1. Топографические карты масштаба 1 : 100000, карты-схемы электрических сетей, фотопланы и фотокарты, планы городов и других поселений, изготовленные в масштабах меньше 1 : 50000 и до 1 : 100000 включительно, издательские оригиналы указанных карт и планов, в том числе расчлененные по элементам содержания, и в системах координат 1942 г. и 1963 г. в графическом, цифровом (электронном) и других видах, а также планы городов и других населенных пунктов, изготовленных с грифом «ДСП» в соответствии с «Инструкцией о порядке составления и издания планов городов и других населенных

пунктов, предназначенных для открытого опубликования и с грифом «Для служебного пользования».

10.2. Сведения о местонахождении (координаты) геодезических пунктов и географических объектов, определенных с точностью грубее 30 метров и до 100 метров включительно в государственной системе координат 1942 года и в геоцентрических системах координат, а также геодезические, картографические и другие материалы, позволяющие уточнить указанные координаты с такой же точностью.

10.3. Первичные и производные материалы аэросъемок (телевизионной, инфракрасной, микроволновой, радиолокационной и др.) с разрешением на местности лучше 2 метров независимо от масштаба, покрывающие площадь в одном массиве на застроенные и малозастроенные территории не более 75 кв. км, эти же материалы с разрешением на местности от 2 до 4 метров независимо от покрываемой ими площади и масштаба съемки.

10.4. Первичные данные аэросъемок и производные материалы с них на полосы трасс аэросъемок шириной до 5 км или полосы обзора (для сканирующей телевизионной и радиолокационной аппаратуры) шириной до 20 км с разрешением на местности лучше 2 метров, эти же данные и материалы с разрешением на местности от 2 до 4 метров независимо от ширины полос трасс аэросъемок, расположенных за пределами городов, поселков городского типа и режимных объектов.

10.5. Схемы (картограммы), отображающие сводные данные геодезической, топографической, картографической, гравиметрической и аэросъемочной изученности на участке местности, превышающие по площади один номенклатурный лист топографической карты масштаба 1 : 200000.

11. Разное

11.1. Материалы мировых соглашений с контрагентами по погашению задолженности до рассмотрения дела в суде по существу вопроса.

11.2. Материалы, относящиеся к проведению конкурсов по выбору заказчика или поставщика МТР и О на объекты капитального строительства, технического перевооружения и реконструкции.

11.3. Сведения по организации и проведению конкурсов (торгов) по выбору подрядчика или поставщика МРТ и О на объекты капитального строительства, технического перевооружения и реконструкции, за исключением сведений о предмете, сроках проведения и победителях конкурсов.

11.4. Информация о финансовом состоянии контрагентов Общества, полученная в процессе осуществления производственной деятельности.

11.5. Сведения об акционерах Общества, раскрытие которых может повредить их деловой репутации или будет являться вмешательством в частную жизнь.

Примечание:

При пользовании перечнем надлежит исходить из следующих положений:

- при перечислении сведений через союз «и» конфиденциальность устанавливается всем сведениям в совокупности;
- при перечислении сведений через запятую и с союзом «и» перед последней категорией сведений конфиденциальность устанавливается всем сведениям в совокупности;
- при перечислении сведений через запятую, союзы «или» и «либо» конфиденциальность устанавливается для каждого сведения в отдельности;
- с союза «а также» начинаются новые сведения, которые отличны от предыдущих и которым устанавливается конфиденциальность, указанная в данном пункте.

Приложение 2
к приказу ОАО «ФСК ЕЭС»
от 17.05.2004 № 105 10

ПОЛОЖЕНИЕ

о порядке организации и проведения работ по защите конфиденциальной информации в Открытом акционерном обществе «Федеральная сетевая компания Единой энергетической системы» (ОАО «ФСК ЕЭС»)

1. Общие положения

1.1. Настоящее Положение определяет общие требования по защите конфиденциальной информации, циркулирующей в исполнительном аппарате и филиалах ОАО «ФСК ЕЭС» и порядок организации работы по обеспечению ее защиты.

1.2. К конфиденциальной информации в Обществе относятся:

- коммерческая тайна;
- служебная тайна;
- персональные данные работников Общества;

- сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них;

- научно-техническая, технологическая, организационная или иная информация, используемая в деятельности Общества, которая обладает действительной или потенциальной коммерческой ценностью в силу ее неизвестности третьим лицам, к которой нет свободного доступа на законном основании и по отношению к которой Общество принимает правовые, организационные, технические и иные меры защиты.

1.3. Конфиденциальная информация фиксируется на бумажных (документы, издания, книги, брошюры, буклеты и т.п.), магнитных (дискеты, аудио, - видео пленки и др.), оптических (лазерные диски) и других носителях (далее - документы). Таким документам присваивается ограничительный гриф «Конфиденциально».

2. Термины, сокращения и определения

2.1. Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

2.2. Документированная информация (документ) – зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

2.3. Конфиденциальная информация – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

2.4. Конфиденциальный документ – документ на материальном носителе, имеющий гриф ограничения доступа.

2.5. Коммерческая тайна – сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами.

2.6. Служебная тайна – служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами.

2.7. Персональные данные – сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность, за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

2.8. АС – автоматизированная система.

2.9. СВТ – средства вычислительной техники.

2.10. ОТСС – основные технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации (АС различного уровня и назначения на базе СВТ, средства и системы связи и передачи данных, включая коммуникационное оборудование, используемое для обработки и передачи конфиденциальной информации).

2.11. Технический канал утечки информации – совокупность источника информации, физической среды распространения информативного сигнала и технических средств, которыми добывается защищаемая информация.

3. Порядок работы со сведениями, отнесенными к конфиденциальной

информации

3.1. К работе со сведениями, содержащими конфиденциальную информацию, допускаются работники Общества, заключившие трудовой договор, содержащий соответствующее условие о неразглашении конфиденциальной информации.

3.2. Отнесение сведений к категории конфиденциальной информации осуществляется в соответствии с Перечнем сведений, содержащих конфиденциальную информацию в ОАО «ФСК ЕЭС» (далее – Перечень).

3.3. Внутри Общества особый порядок обращения с этой категорией информации, как правило, не предусматривается, т.е. он может оставаться таким же, как и для открытой информации.

3.4. При возникновении необходимости направления конфиденциальной информации за пределы Общества, либо в случае установления исполнителем документа особого порядка его обращения внутри Общества, на документе (его электронном аналоге) проставляется гриф «Конфиденциально».

Дальнейшая работа с такого рода документами осуществляется в соответствии с требованиями Инструкции «О порядке работы с конфиденциальной информацией в ОАО «ФСК ЕЭС».

3.5. Решение о проставлении грифа «Конфиденциально» принимает работник – исполнитель документа или руководитель, подписывающий документ.

При этом помимо Перечня необходимо также учитывать следующее:

- не составляют ли отправляемые сведения государственную тайну;

- не входят ли они в перечень сведений, которые в соответствии с законодательством Российской Федерации не могут составлять конфиденциальную информацию;

- не являются ли они общеизвестными или общедоступными;

- составляют ли они действительную или потенциальную коммерческую ценность, а также имеются ли преимущества открытого использования рассматриваемых сведений по сравнению с закрытым.

3.6. В том случае, если сведения, помещаемые в документ, по мнению исполнителя носят конфиденциальный характер, но их невозможно идентифицировать со сведениями, содержащимися в Перечне, руководитель структурного подразделения исполнительного аппарата и руководитель филиала Общества, в котором подготавливался данный документ, обязан проставить на нем гриф «Конфиденциально» и в недельный срок представить в Специальную дирекцию обоснованные предложения по соответствующему дополнению (изменению) Перечня.

3.7. Прием поступающей и отправка исходящей корреспонденции, имеющей ограничительные грифы («конфиденциально», «коммерческая тайна», «для служебного пользования» и т. п.), осуществляется:

- в исполнительном аппарате Общества – Канцелярией Департамента административного управления и делопроизводства;

- в филиалах – соответствующими структурными подразделениями (службы, отделы, группы).

Конфиденциальная информация в электронном виде может приниматься и передаваться структурными подразделениями исполнительного аппарата и филиалов Общества только с использованием защищенных каналов связи.

3.8. Отправка документов, содержащих конфиденциальную информацию, средствами факсимильной связи допускается только после получения на это разрешения руководства Общества.

4. Передача конфиденциальной информации третьим лицам.

4.1. Передача сведений, содержащих конфиденциальную информацию Общества, третьим лицам (юридическим лицам и физическим лицам, не являющимся работниками Общества) запрещается, за исключением случаев, когда они предоставляются:

- органам законодательной и исполнительной власти, контролирующим органам, имеющим право получать такую информацию в соответствии с законодательством Российской Федерации – на основании письменного запроса;

- сторонним организациям – при условии наличия в договоре (соглашении) с ними требований о соблюдении конфиденциальности.

4.2. Использование сведений с грифом «Конфиденциально» в открытых выступлениях, публикациях, интервью, на конференциях, презентациях и т.п. без разрешения Председателя Правления Общества или его заместителей запрещается.

4.3. В случае наличия разрешения руководства Общества на передачу сведений, содержащих конфиденциальную информацию, для публикации (оглашения) в открытых источниках, гриф конфиденциальности снимается, а о факте их передачи ставится в известность Специальная дирекция с последующим уведомлением об этом заинтересованных структурных подразделений и контрагентов (при необходимости).

5. Контроль соблюдения установленного порядка обращения со сведениями и документами, содержащими конфиденциальную информацию

5.1. Осуществление систематического контроля соблюдения в Обществе установленного порядка обращения со сведениями и документами, содержащими конфиденциальную информацию, возлагается:

5.1.1. В исполнительном аппарате на:

- Департамент административного управления и делопроизводства – в части получения, отправки, учета и хранения конфиденциальных документов;

- Департамент информатизации – в части обработки, передачи и хранения конфиденциальной информации средствами корпоративной информационной системы управления (КИСУ);

- Специальную дирекцию – в части правильности отнесения сведений к категории конфиденциальной информации и использования их у контрагентов.

5.1.2. В филиалах – на соответствующие структурные подразделения (службы, отделы, группы).

5.2. По результатам осуществляемого контроля составляется отчет, в котором отражаются состояние дел в области выполнения установленного порядка обращения со сведениями, содержащими конфиденциальную информацию, выявленные недостатки и нарушения, а также вносятся предложения по их устранению.

5.3. Руководителям структурных подразделений и филиалов предоставляется право вносить руководству Общества обоснованные предложения о запрете на работу с конфиденциальной информацией или с техническими средствами обработки данной информации в отношении тех или иных

работников Общества, нарушивших установленный порядок и правила сохранности сведений, содержащих конфиденциальную информацию.

5.4. В случае утраты документа или установленного факта утечки сведений, содержащих конфиденциальную информацию, об этом ставятся в известность руководитель структурного подразделения исполнительного аппарата Общества, Специальная дирекция и Департамент информатизации.

5.5. Для расследования обстоятельств утраты (утечки) сведений, содержащих конфиденциальную информацию, и определения возможного ущерба руководством Общества назначается специальная комиссия, результаты работы которой докладываются руководителю, назначившему комиссию.

Комиссия, проводящая расследование, может обратиться к руководству Общества с предложением о снятии грифа «Конфиденциально» с информации, содержавшейся в утраченном документе, и в случае принятия положительного решения обязана проинформировать об этом все структурные подразделения Общества, использующие соответствующую информацию, а также контрагентов, с которыми имеется соответствующее соглашение (договор).

6. Ответственность

6.1. Требования настоящего Положения обязательны для исполнения всеми работниками Общества, которые несут персональную ответственность за сохранность сведений, содержащих конфиденциальную информацию Общества.

6.2 Руководители структурных подразделений исполнительного аппарата и филиалов Общества несут ответственность за организацию работы с документами, содержащими конфиденциальную информацию, в подчиненных им подразделениях, в том числе за обоснованность проставления (не проставления) исполнителями-разработчиками документов грифа «Конфиденциально».

6.3. Работники Общества, допустившие утечку сведений, содержащих конфиденциальную информацию, либо нарушившие требования настоящего Положения и других распорядительных документов, устанавливающих порядок обращения со сведениями, содержащими конфиденциальную информацию, а также работники, по вине которых произошла утрата носителей конфиденциальной информации, несут ответственность, предусмотренную законодательством Российской Федерации, внутренними документами Общества и условиями трудового договора.

6.4. Ответственность лиц, не являющихся работниками Общества, за утечку или утрату сведений, содержащих конфиденциальную информацию, доверенных им в связи с участием в деятельности Общества, устанавливается соглашениями о взятии ими на себя таких обязательств и законодательством Российской Федерации.

Приложение 3
к приказу ОАО «ФСК ЕЭС»
от 17.05.2004 № 105

Приложение 3
ИНСТРУКЦИЯ
о порядке работы с конфиденциальной информацией в Открытом акционерном обществе «Федеральная сетевая компания Единой энергетической системы» (ОАО «ФСК ЕЭС»)

1. Общие положения

1.1. Настоящая Инструкция устанавливает особый порядок работы с документами – носителями конфиденциальной информации в ОАО «ФСК ЕЭС» (далее - Общество), предназначенными для направления за пределы Общества, либо используемыми внутри Общества при условии установления исполнителями таких документов особого порядка их обращения.

1.2. Регистрация, оформление, обработка, пересылка, передача, хранение, уничтожение конфиденциальных документов осуществляется с учетом требований законодательных, иных нормативных документов РФ по организации открытого делопроизводства, а также Инструкции по делопроизводству в исполнительном аппарате ОАО «ФСК ЕЭС», утвержденной приказом Общества от 18.11.2002 г. № 71.

1.3. Понятия терминов, сокращений и определений, применяемых в Инструкции, даны в «Положении о порядке организации и проведения работ по защите конфиденциальной информации в ОАО «ФСК ЕЭС».

1.4. Ответственность за конфиденциальные документы, поступившие в структурные подразделения исполнительного аппарата Общества, возлагается на руководителя и уполномоченного работника структурного подразделения Общества.

1.5. Ответственность за конфиденциальные документы, поступившие в адрес филиалов Общества, возлагается на их руководителей и руководителей (работников) соответствующих служб, отделов, групп.

1.6. Создание, обработка, пересылка, хранение и уничтожение конфиденциальных документов на технических средствах обработки информации разрешается только при наличии установленных на них специальных средств защиты.

2. Учет и обработка конфиденциальных документов

2.1. Все конфиденциальные документы подлежат однократной регистрации.

2.2. Отличительной особенностью входящих конфиденциальных документов является наличие пометки (ограничительного грифа) в верхней части документа – «конфиденциально», «конфиденциальная информация», «коммерческая тайна», «для служебного пользования» и соответствующего буквенного индекса в порядковом номере документа, указывающего на вид документа: «К», «КИ», «КТ», «ДСП».

Прием конфиденциальных документов в электронном виде осуществляется только с использованием ОТСС, специально предназначенных для этой цели.

При приеме конфиденциального документа на электронном носителе проверяется наличие и подлинность электронной цифровой подписи (далее ЭЦП) корреспондента.

При отсутствии ЭЦП на входящем конфиденциальном документе на электронном носителе, уполномоченный работник обязан проставить в нем свою ЭЦП для гарантии неизменности документа.

При обнаружении недостачи вложения составляется акт, в котором перечисляются все вложения, оказавшиеся в наличии, а также недостающие, их тематика, наличие или отсутствие повреждений на конверте, другие необходимые, по мнению составителей акта, сведения, а для конфиденциальных документов в электронном виде – объем и тематика полученного документа, факт нарушения ЭЦП.

2.3. На каждом регистрируемом входящем конфиденциальном документе после присвоения ему порядкового (входящего) номера проставляется буквенный индекс конфиденциальности («К», «КИ», «КТ», «ДСП), соответствующий наименованию ограничительного грифа на документе, и дата его поступления.

После присвоения порядкового (входящего) номера электронному документу, уполномоченный работник скрепляет его своей ЭЦП.

2.4. Конфиденциальный документ, поступивший в структурное подразделение, минуя уполномоченного работника,

должен быть передан ему для регистрации и оформления в соответствии с требованиями настоящей Инструкции.

2.5. На исходящих, а также внутренних конфиденциальных документах проставляется гриф «Конфиденциально», регистрационный номер с буквенным индексом «К» и дата регистрации.

Гриф «Конфиденциально» размещается в правом верхнем углу документа.

Исходящая конфиденциальная документация в электронном виде скрепляется ЭЦП исполнителя и помещается в электронное письмо.

Уполномоченный работник проставляет в электронном письме гриф «Конфиденциально», под ним - исходящий регистрационный номер с буквенным индексом «К» электронного документа, соответствующий его порядковому номеру, дату регистрации и скрепляет электронное письмо своей ЭЦП.

2.6. Работник, получивший конфиденциальный документ, обязан принимать меры для обеспечения его сохранности и не разглашать содержащиеся в нем сведения в беседах с посторонними лицами, а также с сотрудниками Общества, если этого не требуется для исполнения им своих служебных обязанностей.

В нерабочее время конфиденциальные документы и электронные носители, содержащие конфиденциальную информацию, должны находиться в запирающихся на ключ секциях рабочих столов или в металлических шкафах.

2.7. Выдача конфиденциальных документов или их копий работникам, которым они предназначены, а также передача их в другие структурные подразделения исполнительного аппарата Общества осуществляется под роспись в журнале учета выдачи-приема конфиденциальных документов согласно приложению к настоящей Инструкции.

2.8. Работник, получивший для работы конфиденциальный документ на бумажном носителе, обязан располагать его так, чтобы исключить возможность ознакомления с ним других лиц.

При обработке конфиденциальных документов на СВТ, они должны располагаться таким образом, чтобы исключить возможность ознакомления с электронными документами посторонних лиц. При отлучении с рабочего места работник обязан закрывать все электронные документы, содержащие конфиденциальную информацию.

2.9. При внесении изменений в электронный документ работник обязан проставить на нем свою ЭЦП.

2.10. При увольнении, переводе в другое подразделение работник обязан сдать все числящиеся за ним конфиденциальные документы. Работник также обязан сдать либо уничтожить электронную документацию, содержащую конфиденциальную информацию, находящуюся в его распоряжении.

3. Распечатывание, копирование, размножение конфиденциальных документов

3.1. Распечатывание конфиденциальных документов в электронном виде, сканирование (печатание) конфиденциальных документов на бумажных носителях производится самим исполнителем. На обороте или внизу последнего листа каждого экземпляра документа, либо в электронном документе, указывается фамилия исполнителя, его контактный телефон, дата распечатывания или сканирования (печатания).

После распечатывания (сканирования) конфиденциального документа исполнитель должен убедиться в невозможности получения повторных несанкционированных копий.

Распечатанные (отсканированные, отпечатанные) документы регистрируются в установленном порядке в соответствующих журналах учета.

3.2. Копирование (размножение) конфиденциальных документов осуществляется уполномоченным работником с разрешения руководителя структурного подразделения с указанием количества экземпляров (копий).

Новые экземпляры (копии) документов регистрируются в установленном порядке с присвоением копиям очередных номеров экземпляров основного документа.

3.3. Для копирования, размножения конфиденциальных документов уполномоченный работник обязан использовать технику, исключающую возможность получения повторных несанкционированных копий документов (электронных документов), либо убедиться в невозможности дальнейшего получения таких копий.

3.4. Представители сторонних организаций имеют право делать выписки и снимать копии с конфиденциальных документов только с разрешения руководителя структурного подразделения Общества (с указанием конкретного материала, количества копий) и на основании письменных запросов руководителей сторонних организаций, при условии совместной работы с использованием конфиденциальной информации, а также при условии подписания с ними соглашения о конфиденциальности или заключения договора, содержащего условие о конфиденциальности.

Учет конфиденциальных документов в этих случаях производится на общих основаниях, а предоставление выписок, копий - под роспись, с указанием организации и основания для передачи информации.

4. Пересылка, передача документированной конфиденциальной информации

4.1. Передача конфиденциальной информации с использованием средств факсимильной связи допускается в исключительных случаях с письменного разрешения Председателя Правления Общества или его заместителей.

4.2. Рассылка, отправка и передача конфиденциальных документов осуществляется только уполномоченным работником на основании перечней списков для рассылки приказов, распоряжений и иной документации или указаний Председателя Правления Общества или его заместителей.

4.3. При необходимости направления документации нескольким адресатам, составляется указатель рассылки, в котором поадресно проставляются номера экземпляров. Указатель рассылки подписывается исполнителем и руководителем структурного подразделения и подшивается в дело вместе с основным документом.

4.4. Пересылка конфиденциальных документов может осуществляться заказными почтовыми отправлениями, спецсвязью, фельдсвязью, или с нарочным.

4.5. Разрешается передача конфиденциальных документов посредством электронной почты, иных средств передачи электронной информации только при наличии специальных средств защиты каналов передачи.

Передача конфиденциальных документов в электронном виде в другие организации осуществляется только при заключении с ними договора о признании средств электронно-цифровой защиты (ЭЦЗ), наличия абонентского пункта и юридической значимости ЭЦП.

При отсутствии указанных условий конфиденциальная информация подлежит передаче только на бумажных носителях в установленном настоящей Инструкцией порядке.

5. Хранение, уничтожение конфиденциальных документов

5.1. Конфиденциальные документы должны храниться в сейфах, или запираемых на ключ металлических шкафах.

Конфиденциальные документы в электронном виде должны храниться только на СВТ, оснащенных специальными средствами защиты, на специальных шифруемых локальных дисках.

5.2. Конфиденциальные документы группируются для хранения согласно номенклатуре дел по функциональному направлению.

На обложке каждого дела (тома), в котором подшит хотя бы один документ, содержащий конфиденциальную информацию, проставляется гриф «Конфиденциально».

5.3. Уничтожение конфиденциальных документов, утративших практическую ценность, производится уполномоченным работником структурного подразделения в присутствии двух других работников Общества по акту. При этом в регистрационных документах делается соответствующая ссылка на акт уничтожения, который хранится как документ с грифом «Конфиденциально». Письменное разрешение на уничтожение по представляемому списку документов дает руководитель структурного подразделения.

Уничтожение копий электронных документов, находящихся у работника Общества, может производиться самим работником, в том числе по указанию уполномоченного работника, только с использованием специальных технических средств.

Уничтожение конфиденциальных документов на бумажных носителях производится путем их резки на бумагорезательной машине.

Уничтожение электронной документации производится путем ее стирания с использованием специальных средств.

Литература

1. Федеральный закон Российской Федерации от 21.11.1996 № 129-ФЗ «О бухгалтерском учете» (в ред. Федерального закона от 03.11.2006 №183-ФЗ) // Собрание законодательства РФ, 25.11.1996, №48, ст. 5369.

2. Постановление Правительства Российской Федерации от 08.07.1997 №835 «О первичных учетных документах» // Собрание законодательства РФ, 14.07.1997, №28, ст. 3448.

3. Алексенцев А.И. Конфиденциальное делопроизводство. – М.: «Управление персоналом», - 2003. – 200 с.

4. Андреева. В.И. Делопроизводство. - М., - 2004. – 564 с.

5. Замыцкова О.И. Делопроизводство (Документационное обеспечение управления): Учебник. – Ростов-на-Дону: Феникс, - 2008. – 375 с.

6. Кирсанова М.В., Аксенов Ю.М. Курс делопроизводства: Документальное обеспечение управления: Учебное пособие – 2 изд. – М.: Инфра – М. – 2004. – 321с.

7. Кугушева Т.В. Делопроизводство: Учебное пособие. – Ростов-на-Дону: Феникс, 2007. – 256 с.

8. Кудряев В.А. Организация работы с документами. – М.: Инфра-М. - 2008. – 432с.

9. Кузнецова Т.В. Делопроизводство (документационное обеспечение управления) 3-е изд. испр. и дополн. М. - 2002. – 384 с.

10. Рогожин М.Ю. Делопроизводство и документооборот в бухгалтерии. М.: Гросс-Медиа: РОСБУХ, - 2007. – 212 с.

11. Санкина Л.В. Порядок оформления документов. Требования нового стандарта // Справочник кадровика .- 2004.- № 8-9.

12. Экономика предприятия: Учебник. Под ред. О.И. Иванова и др. – М.: Экономика. - 2006. – 238 с.

13. Захаркина О.И. Кадровая служба предприятия: делопроизводство, документооборот и нормативная база. – М.: Омега–Л. – 2007. – 116 с.

Нормативно-правовые акты

1. Гражданский кодекс Российской Федерации.

2. Федеральный закон «Об информации, информатизации и защите информации».

3. Федеральный закон «Об акционерных обществах».

4. Закон «О предприятиях в СССР».

5. Закон РСФСР «О предприятиях и предпринимательской деятельности».

6. Закон РСФСР «О конкуренции и ограничении монополистической деятельности на товарных рынках».

7. Закон РФ "О товарных знаках, знаках обслуживания и наименованиях мест происхождения товаров».

8. Основы законодательства Российской Федерации об Архивном фонде Российской Федерации и архивах.

9. Проект Федерального закона «О коммерческой тайне».

10. Положение об Архивном фонде Российской Федерации, утвержденное Указом Президента РФ от 17 марта 1994 г. № 552.

11. Постановление Правительства РСФСР от 5 декабря 1991 г. № 35 «О перечне сведений, которые не могут составлять коммерческую тайну».

12. Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, утвержденное постановлением Правительства РФ от 3 ноября 1994 г. № 1233.

13. ГОСТ Р5114198. Делопроизводство и архивное дело. Термины и определения.

14. Государственная система документационного обеспечения управлений. Основные положения. Общие требования к документам и службам документационного обеспечения. М., 1991.

15. Типовая инструкция по делопроизводству в федеральных органах исполнительной власти. М., 2001.

16. Общероссийский классификатор управленческой документации. М., 1994.

17. Общероссийский классификатор профессий рабочих, должностей служащих и тарифных разрядов. М., 1994.

18. Квалификационный справочник должностей руководителей, специалистов и других служащих. М., 1998.

19. Укрупненные нормативы времени на работы по делопроизводственному обслуживанию. М., 1988.

20. Межотраслевые укрупненные нормативы времени на работы по документационному обеспечению управления. М., 1995.

21. Перечень типовых управленческих документов, образующихся в деятельности организаций, с указанием сроков хранения. М., 2001.

22. Перечень научно-технической документации, подлежащей приему в государственные архивы России. М., 1998.

23. Управленческие документы постоянного срока хранения, образующиеся в деятельности негосударственных коммерческих организаций (хозяйственных товариществ, производственных кооперативов). Справочное пособие. М., 1996.

24. Отбор на государственное хранение управленческих документов, образующихся в деятельности негосударственных организаций (новых экономических хозяйственных структур). Методические рекомендации. М., 1998.

Дополнительное профессиональное образование с применением информационных технологий в сфере физической культуры и спорта

С.Ю. Махов, к.п.н., доцент кафедры ТРиС
ФГБОУ ВПО «Госуниверситет-УНПК»

Актуальность. Развитие и широкое внедрение информационных технологий оказывает трансформирующее воздействие на все области современной жизни, включая сферы политики, экономики, науки, образования. Главной ценностью современного мира являются информация и знание. Информация и знание становятся определяющим экономическим фактором, а также важнейшим национальным ресурсом, который в значительной степени определяет благосостояние государства.

Всю свою жизнь мы приобретаем знания и повышаем свой образовательный уровень. При этом знания – это не только то, что дают нам книги, телевидение, школа, вуз, но и то, что мы получаем и используем в процессе работы и общения с людьми, накапливая жизненный опыт. Знания – это нечто большее, чем и данные, и информация. К знаниям также относятся: убеждения и моральные ценности; идеи и изобретения; суждения; навыки и профессиональные познания; теория и практика; правила; отношения; мнения; понятия; прошлый опыт. Все вышеперечисленное мы используем для того, чтобы превратить информацию в знания.

Сегодня все большее распространение получает идея «бизнес-образования». Для абсолютного большинства категорий специалистов получение дополнительного профессионального образования становится актуальным и востребованным явлением. Желающим повысить свой профессиональный и образовательный уровень или вообще сменить сферу деятельности, предлагается множество курсов, тренингов и семинаров, которые охватывают достаточно много специализаций в различных областях. Выбирая ту или иную программу повышения квалификации или профессиональной переподготовки, кто-то хочет закрепить с помощью практических тренировок полученные академические знания, другие, пытаются посмотреть на накопленные навыки и компетенции немного под другим углом, третьи желают сменить вид своей деятельности.

Большинство компаний стараются привлечь в свои ряды специалистов с опытом работы в аналогичной должности, чтобы потерять как можно меньше драгоценного времени на их обучение. Однако не всем удается заполучить требуемое количество таких работников, а постоянно повышать зарплаты сотрудникам, чтобы не потерять их, работодатели позволить себе не могут. Вариантом выхода из сложившейся ситуации является обучение и развитие собственных работников для повышения их мотивации и лояльности к компании. Именно поэтому очень многие работодатели сегодня

организовывают свои образовательные и учебные центры для обучения всем нюансам как стажеров, так и специалистов.

Прохождение качественных краткосрочных образовательных программ, как правило, свидетельствует о стремлении специалиста повышать свой профессиональный уровень. Многие специалисты по тем или иным причинам решают кардинально сменить сферу деятельности. Для освоения новой профессии им нужно получить некоторые теоретические знания и отработать их на практике. Этого можно достичь с помощью различных курсов и семинаров. Считается, что краткосрочное образование быстрее дает ощутимые результаты.

Дополнительное профессиональное образование также просто необходимо для новых специальностей и специальностей, где происходят постоянные изменения или стремительное развитие технологий. Многие профессии требуют от специалистов постоянного повышения квалификации, они должны быть в курсе всех изменений, современных тенденций и нововведений. Нередко наличие аттестата является обязательным при приеме на работу. Многие крупные компании самостоятельно отправляют новоиспеченных сотрудников на получение дополнительного профессионального образования за корпоративный счет.

На сегодняшний день сфера дополнительного профессионального образования и сектор платных бизнес-образовательных услуг уже достаточно широко развиты, хотя спрос, даже платежеспособный, как показывают исследования, далеко не насыщен. И в то же время потребитель (организация или индивид, обладающий определенными средствами) достаточно осмотрителен и хочет получить образовательный проект, полноценный с точки зрения критерия «затраты – эффективность».

В свою очередь, образовательное учреждение, начиная те или иные программы, хочет получить реальный эффект, как экономический, так и социальный. Следует сознавать, что, принимая решение о начале образовательной деятельности по той или иной модели, необходимо осознанно учитывать наличие факторов, способных создать благоприятные условия и конкурентные преимущества образовательному учреждению.

В 2013 г стоимостный объем рынка дополнительного профессионального образования в России вырос на 18,5%, до 231,4 млрд. руб. Рост выручки обеспечивался увеличением натурального объема рынка и повышением цен на услуги.

В 2013 г натуральный объем рынка дополнительного профессионального образования в России вырос на 4,8%, до 50,9 млн. академических часов. По оценкам BusinesStat, в 2013-2017 г.г. натуральный объем рынка дополнительного профессионального образования вырастет на 36% и достигнет 74 млн. академических часов. Увеличение рынка будет обеспечиваться за счет роста активности граждан в удовлетворении профессиональных образовательных потребностей, развитию государственно-частного партнерства в отрасли, увеличению объема инвестиций в отрасль.

В 2013 г средняя цена услуг дополнительного профессионального образования выросла на 9,3% и составила 194,2 руб. с чел за академический час. Основной причиной увеличения цен является активное развитие частного сектора дополнительного профессионального образования. Кроме того, растут затраты на заработную плату персонала и аренду помещений.

Рынок спортивно-оздоровительных (фитнес) услуг еще далек от насыщения. Спрос удовлетворен всего на 60–70%. Острый дефицит квалифицированных тренеров сдерживает развитие рынка. Тренеров, готовых немедленно приступить к работе, на рынке труда просто нет.

Вузы предоставляют работников близких специальностей. Но, выпускники профильных факультетов – это либо профессиональные спортсмены, либо преподаватели физкультуры, ориентированные на работу в образовательных учреждениях, где подход к подопечным принципиально отличается от того, который принят в фитнес-центрах.

Проблему повышения квалификации тренеров отчасти решают многие государственные и негосударственные учебные центры дополнительного образования, в частности, устраивают семинары и тренинги для сотрудников фитнес-центров. В основном это бывают краткосрочные (несколько дней) тренинги для молодых специалистов, где опытные столичные и местные тренеры дают мастер-классы. Но сами игроки рынка считают подобные мероприятия неэффективными.

Качественное обучение тренера занимает как минимум год, а краткосрочные тренинги, организованные учебными центрами, не приносят отдачи. Подобные мероприятия нельзя называть обучающими. Эти семинары – демонстрация достижений опытных тренеров, а не подготовка начинающих специалистов.

В настоящее время многие фитнес-центры начинают решать кадровые проблемы самостоятельно. Начали готовить специалистов для себя внутри компании. Подходы к обучению персонала различаются. Сетевые игроки держат в штате преподавателей. К примеру, в управляющей компании «СитиФитнес» есть сотрудники-методисты по разным направлениям тренинга. Они выезжают в регионы, учат тренеров на местах. Последние по окончании курсов проходят тесты. И только после этого приступают к работе. Фитнес-клуб «Верх-Исетский» отправляет своих тренеров на московские долгосрочные курсы. При этом клуб оплачивает 50% стоимости обучения. Оставшуюся часть вносит сам сотрудник. Чтобы будущий тренер получил базовые знания и навыки, необходимые для работы, потребуется один год.

Пока затраты на подготовку тренеров себя оправдывают – лучше оплатить обучение работника, чем потерять потенциальных клиентов, говорят специалисты. Тем не менее, операторы рынка надеются, что со временем в регионах появятся специализированные организации, занимающиеся подготовкой кадров для фитнес-клубов, либо колледжи и вузы введут соответствующие программы.

Основные выводы:

– В последние годы рынок образовательных услуг претерпевает качественные изменения, главную роль в которых играет Болонский процесс.

– Лидирующее место на рынке образовательных услуг занимает Москва. В настоящее время в Москве 112 государственных вузов и более 250 негосударственных.

– Повышению качественного уровня образовательных услуг способствует демографическая ситуация в стране, особенно ее прогнозирование на ближайшие несколько лет. Как следствие следует ожидать повышения конкурентной борьбы между вузами. Это коснется двух показателей: качества образования и востребованности на рынке труда выпускников.

– Одной из самых актуальных проблем для негосударственного сегмента рынка образовательных услуг остается отсутствие четкой нормативной базы и барьеры со стороны государства при лицензировании учебных заведений.

– Одной из самых перспективных форм развития образовательных услуг является не так давно появившееся направление – дистанционное обучение, которое позволяет сделать услуги качественного образования более доступным и открывает новые перспективы как для потребителей, так и для продавцов, получить желаемое образование, не выходя из дома.

В целом, взгляд на систему образования как на рынок образовательных услуг, где встречаются продавец и покупатель, еще находится в стадии формирования. Потребитель пока не может в полной мере воспользоваться предоставленными правами. Продавец же пока не готов в полной мере мобильно и адекватно реагировать на образовательный запрос общества.

Дистанционное электронное обучение (e-learning).

Электронное обучение (e-learning) – новый для российской системы образования термин, который активно входит в нашу жизнь. Прежде чем оценить объемы и перспективы развития рынка e-learning необходимо разобраться, что же что входит в это понятие. Известно, что для определения рынка используются два наиболее часто встречающихся определения: дистанционное обучение (или образование) и e-learning.

Участники рынка оперируют такими понятиями как «дистанционное обучение», «дистанционное образование», «e-learning», «система дистанционного обучения». Все эти понятия являются взаимопересекающимися и используются на российском рынке как синонимы. Но ни одно из них полностью не входит в другое и каждое из них несет свою смысловую нагрузку. Например, существует дистанционное обучение, не являющееся электронным, и также существует электронное обучение, не являющееся дистанционным. Понятие дистанционного обучения подразумевает, в первую очередь, что преподаватель и учащийся находятся на расстоянии, а доставка учебных материалов происходит с помощью каких то средств связи (почта, курьер, интернет-технологии, телевидение). При этом для дистанционного обучения нет разницы, каким именно способом будут

доставлены учебные материалы, с помощью компьютера и интернет-технологий или нет. В то время как электронное обучение подразумевает тот же самый процесс доставки учебных материалов от преподавателя к ученику, но уже исключительно в электронном виде. Таким образом, e-learning может быть использовано в дистанционном обучении, а дистанционное обучение может использовать e-learning, а может и не использовать. Дистанционное образование – это образование, полученное с помощью дистанционного обучения. Данные словосочетания также используются как синонимы.

На данный момент на российском рынке не достигнуто единое мнение по поводу терминологии и обозначений на рынке дистанционного обучения. И отсутствуют механизмы, способные обеспечить создание нормативной базы. Наиболее точное, на наш взгляд, определение термину дали специалисты ЮНЕСКО: «E-learning – это обучение с помощью Интернет и мультимедиа».

Развитию электронного обучения способствовало формирование рынка бизнес-образования. Организации, предоставляющие услуги в области бизнес-обучения, оценив эффективность нового способа, стали постепенно переходить на электронный вариант. На сегодняшний день в мире электронное образование используется повсеместно. Например, в США уже более 90% ВУЗов и школ, а также компаний, имеющих численность более тысячи – полутора тысяч человек, используют эту форму обучения. По сравнению с ситуацией в мире, развитие рынка электронного обучения в России, по оценкам специалистов, отстает на 5–7 лет.

На сегодняшний день в России рынок дистанционного образования развивается бессистемно, без централизованного планирования, отсутствует четкое понимание целей и задач развития отрасли. Что существенно отличается от ситуации, например, в Европе. Комиссией Европейского сообщества была определена стратегия развития дистанционного образования, которая определяет e-learning, прежде всего, как планирование завтрашнего образования. Стратегия подразумевает объединение всех участников рынка для оптимального взаимодействия с целью наиболее эффективного развития e-learning. Такой системный подход обеспечивает эффективное развитие отрасли, чего на данный момент не хватает рынку в РФ. И, в особенности, четко прописанного законодательного регулирования.

Потребители электронного обучения проекта.

Потребителей электронного обучения можно разделить на корпоративный, образовательный сектор и потребителей индивидуального обучения.

В *корпоративном секторе* заинтересованными компаниями являются те, которым необходимо проводить регулярное обучение сотрудников, особенно если компания имеет филиалы.

Образовательный сектор можно разделить на государственный, к которому относятся государственные учебные заведения, и частный, к которому относятся компании, предоставляющие образовательные услуги. Значительно распространено дистанционное бизнес-образование.

Индивидуальные пользователи e-learning используют все возможности, которые предоставляет интернет, а также бесплатные сайты по обучению. Это сайты, предоставляющие лекции, видеоматериалы, вебинары и тесты практически во всех областях, доступных для изучения через интернет.

Преимущества и недостатки электронного обучения e-learning.

К основным *преимуществам* e-learning относится:

– Одно из основных преимуществ электронного обучения – это экономия времени. У обучающихся и преподавателя отсутствует необходимость присутствовать очно на лекциях и тестах, добираясь до места их проведения. По данным Cedar Group, время обучения с помощью e-learning меньше на 35–45%.

– Для корпоративного и частного образовательных секторов огромное преимущество электронного обучения – сокращение затрат. Происходит оптимизация затрат на переезде сотрудников, проживании, аренде залов и оплате расходов бизнес-тренеров. По данным Cedar Group, стоимость услуги электронного обучения дешевле прочих форм образования на 32–45%.

– Электронное обучение предоставляет возможность обучения в своем темпе и в любое удобное время вне независимости от преподавателя;

– По сравнению с очными формами обучения, скорость запоминания учебного материала выше на 20–25%;

– Лёгкость актуализации учебного материала, прозрачность процесса обучения, быстрая доступность статистики для анализа и возможность просмотра видеолекций неограниченное количество раз.

Недостатки e-learning:

– Основной недостаток e-learning – это проблема идентификации личности обучаемого. Отсутствует 100% гарантия, что именно этот студент отвечает на вопросы теста. Для устранения этой проблемы существует несколько вариантов решений, которые необходимо использовать в комплексе:

- ✓ ввод уникального логина и пароля в систему, статический ip адрес;
- ✓ использование идентификации отпечатков пальцев или сетчатки глаза;
- ✓ настройка системы тестирования на мониторинг временных интервалов на ответ, т.е. если студент отвечает слишком быстро на сложнейшие вопросы, система подаст сигнал о возможных нарушениях;
- ✓ тестирование обучающегося под видеоконтролем преподавателя.

– Другой недостаток электронного обучения – отсутствие мотивации извне и недостаток контроля, характерного для очного обучения. Наибольший эффект от обучения с помощью e-learning способны извлечь те обучающиеся, кто имеет высокую внутреннюю мотивацию. Кроме того, грамотное построение электронного курса по системе Джона Келлера подразумевает создание у обучаемого мотивации на дальнейшее прохождение курса. Однако чем длиннее во времени учебный курс, тем сложнее удерживать внимание обучающегося.

– При электронном обучении фактически отсутствует обратная связь между преподавателем и студентами (если не используется вариант

интерактивного вебинара), нет живого общения, поэтому электронное обучение имеет определенные ограничения в применении. Например, оно не подходит для развития навыков работы в команде, уверенности и коммуникабельности.

Зарубежный опыт говорит о том, что при наличии качественного учебного контента и грамотного построения учебного курса, во многих отраслях эффективность электронной формы обучения не уступает эффективности очной формы обучения. На сегодняшний день, это официально признано на уровне ООН и ЮНЕСКО. В мире технологии e-learning в равной мере востребованы как в сегменте индивидуального образования, так и в сфере корпоративного обучения. Например, в Германии, по данным социологов, работодатели ценят дистанционное обучение даже выше очного. И причиной этого является то, что качество этой формы обучения не уступает очным формам, что достигается хорошим информационным обеспечением и качеством экзаменов при отсутствии коррупции.

Развитие рынка электронного обучения в России отстает от мирового рынка, в том числе на уровне государственной поддержки и централизованной организации процесса развития отрасли. В то время как рынок e-learning Европы и США можно назвать зрелым, в России и странах СНГ только начинается его становление.

Российский рынок электронного обучения e-learning.

Поскольку рынок e-learning в России не выделен пока в самостоятельную отрасль, статистические данные отсутствуют, и информация об объемах рынка носит оценочный характер. Авторы исследования «Электронное образование и развитие инновационной экономики России» считают, что объем рынка e-learning в России в 2010 году составил около 4,7 млн. долл., а в 2013 году произошло увеличение до $10 млн. в связи с реализацией государственных образовательных программ и растущим спросом.

На сегодняшний день рынок e-learning в России находится в стадии развития и является пока «незрелым». Потенциальный объем рынка оценивается очень высоко. Например, согласно данным «The Economist Intelligence Unit», граждане России тратят около $10 млрд. в год на получение дистанционного образования в иностранных университетах.

На сегодняшний день потенциальный спрос и реальное предложение российского рынка e-learning отличаются друг от друга в десятки раз. Рынок будет расти и развиваться как за счет новых потребителей, так и за счет поиска опытными потребителями улучшений существующих систем.

По данным CNews Analytics, в России корпоративный сегмент развивается более быстрыми темпами, в то время как росту государственного сектора препятствуют консервативность представителей ВУЗов, отсутствие четко прописанного законодательства в этой области и финансовые затруднения.

Согласно прогнозам участников рынка, рост рынка электронного образования в России составит 20–25% ежегодно.

Тенденции и прогнозы развития рынка e-learning.

Основными тенденциями развития рынка e-learning первого порядка в мире в настоящее время являются следующие:

– использования социальных сетей для электронного обучения;

– рост популярности SaaS решений;

– распространение мобильного обучения.

Хотя эти тенденции нельзя назвать новыми, но можно сказать, что сейчас глубже раскрывается потенциал уже известных решений. Например, социальные медиа уже используются в целях обучения, но теперь пришло осознание того, что для людей социальные сети стали неотъемлемой частью мышления и обучения. И в скором времени ожидается расцвет приложений для обучения с помощью социальных сетей.

Возрос интерес к SaaS-продуктам (***SaaS*** *(Software-as-a-Service, программное обеспечение как услуга) – это новая модель использования программного обеспечения (ПО), когда пользователь не устанавливает ПО на свой компьютер, а использует его через Интернет)*. Некоторые крупные компании переходят на модели SaaS, и, по мнению экспертов, эти системы в скором времени могут потеснить лидеров рынка, таких как, например, Blackboard. Согласно исследованию «The 2012 IT Budget Benchmarking», в 2013 году расходы компаний на SaaS решения возрастут на 20%.

По данным компании Corporate Executive Board, в корпоративном секторе в 2013 году одним из важнейших приоритетов компаний станет мобильное обучение и следует ожидать роста вложений в мобильные приложения для обучения на 60%.

Основными тенденциями развития рынка e-learning в **России** схожи с мировыми трендами, это:

– мобильное обучение;

– интеграция с социальными сервисами;

– развитие SaaS решений.

Стремительное развитие рынка смартфонов, коммуникаторов и планшетных компьютеров приносит новые веяния в индустрию e-learning, подталкивая развитие мобильного обучения. Сегодня практически любой контент систем e-learning можно просмотреть на мобильном устройстве и необходимости в разработке чего-то специального уже нет. Очевидно, что мобильное обучение в любом случае требует специального подхода, и существуют свои особенности разработки, поэтому говорить о разработке одной версии для всех устройств пока нельзя. Но движение в этом направлении вполне очевидно. В корпоративном секторе в 2013 году одним из важнейших приоритетов компаний станет мобильное обучение и следует ожидать роста вложений в мобильные приложения для обучения на 60%. По данным РАЭК сегодня в России уже около 5 миллионов пользователей мобильного интернета, и большинство из них в возрасте 16–19 лет.

В ближайшем будущем также начнут появляться различные приложения для внедрения в социальные сети, что обусловлено огромной интеграцией

жизни большинства людей молодого поколения с социальными сетями. Например, социальные медиа уже используются в целях обучения, но теперь пришло осознание того, что для людей социальные сети стали неотъемлемой частью мышления и обучения. И в скором времени ожидается расцвет приложений для обучения с помощью социальных сетей.

На сегодняшний день рыночные предложения рынка e-learning в России расширились за счет предложений модели SaaS *(Software-as-a-Service, программное обеспечение как услуга) – это новая модель использования программного обеспечения (ПО), когда пользователь не устанавливает ПО на свой компьютер, а использует его через Интернет).* Появились услуги аренды системы дистанционного обучения, аренды контента и аутсорсинг бизнес-процессов. SaaS направление постепенно набирает обороты на российском рынке. За последние два года в СНГ количество решений e-learning, предоставляемых с помощью SaaS, выросло почти на 50%.

В ближайшее время следует ожидать активизацию работы зарубежных учебных заведений в России, предоставляющих услуги бизнес-обучения. Уже сейчас в России обучением с помощью электронных технологий занимаются более 100 зарубежных компаний, которые охватывают более 350 тыс. российских граждан. На сегодняшний день около 90% учебных заведений в мире способно предложить обучение в электронном варианте. Россия в этом смысле отстает от мирового рынка на 5–7 лет.

В ближайшем будущем рынок электронного обучения в России будет характеризоваться следующими тенденциями:

– появление новых игроков на рынке e-learning;

– рост числа участников профессиональных сообществ по электронному обучению;

– рост рынка вебинаров и вебконференций;

– логичным шагом должно стать развитие адекватного государственного регулирования и создания нормативной базы быстро развивающейся отрасли с определением четких целей и задач развития электронного обучения;

– в долгосрочной перспективе рынок электронного обучения, по примеру мировых тенденций, начнет смещаться в сторону TMS *(Talent Management System – система управления талантами. Представляет собой интегрированный пакет программного обеспечения, основанный на 4 столпах управления талантами: прием на работу, служебная деятельность, обучение и развитие).*

Говоря о будущем электронного обучения в России, хотелось бы обратиться к исследованию корпоративного университета компании Caterpillar. Он сравнил затраты на очные и e-learning программы. Основной вывод – электронное обучение менее затратно вне зависимости от числа обучающихся. Даже если число учеников менее 100 человек и курс длиться менее 1 часа, e-learning все равно остается более чем на 40% выгоднее обучения с преподавателем из-за скрытых издержек на обучающегося ($9,500 против $17,062). При моделировании более длительных программ и покрытии

большего количества персонала, ценовое преимущество электронного обучения становилось еще более заметным, экономия достигала 78%.

Поскольку рынок все равно развивается, вне зависимости от отсутствия должного государственного регулирования, спрос на электронное обучение будет возрастать не только в корпоративном, но и в государственном секторе. На сегодняшний день многие учебные заведения в России стоят перед выбором сокращения невостребованных специальностей или внедрения электронного обучения. По традиции, Россия догоняет мировые рынки, на которых сейчас электронное обучение получило практически повсеместное распространение.

Таким образом, в среднесрочной перспективе следует ожидать дальнейшего распространения электронного дистанционного обучения одновременно с постепенным снижением объемов очного обучения, в большей степени это касается корпоративного сектора.

Определение эффективности штурмового боя

С.Ю. Махов, к.п.н., доцент кафедры ТРиС
ФГБОУ ВПО «Госуниверситет-УНПК»

1. Методика и организация опытно-экспериментальной работы

Не поддающиеся сегодня никакому учету множество спортивных единоборств и боевых искусств, претендующих на самую широкую универсальность и боеспособность, практически таковыми не являются. Почти все они имеют ту или иную степень условности и ограниченности, вызванную созданием различных версий правил соревнований. Боеспособным можно считать только такое боевое искусство, которое допускает применение любых способов и методов воздействия на человека.

Искусство штурмового боя состоит в том, чтобы выжить в любой ситуации и любой ценой. Учитывая непредсказуемость схватки, нужно не соревноваться с нападающим, а активно подавлять его волю и уничтожать боеспособность, используя гибкую программу действий.

Штурмовой бой – это не спорт и не искусство, а жизненная необходимость. Цель штурмового боя – сохранение чести, здоровья и жизни всеми доступными средствами в условиях реальных нападений. Педагогические технологии освоения штурмового боя позволяют повысить уровень боеспособности субъекта, и предназначены для обеспечения личной безопасности в любой критической ситуации.

Актуальность проблемы и ее практическая значимость обосновывается на невозможности противостоять преступным посягательствам посредством спортивных технологий.

На основании анализа современных спортивных единоборств и прикладных систем рукопашного боя была сформулирована **проблема исследования**. Она определяется важными противоречиями между необходимостью и потребностью граждан по овладению эффективной системой боевого выживания в обеспечении

собственной безопасности с одной стороны, а с другой – невозможностью спортивных технологий обеспечения гарантированной безопасности человека от преступных посягательств.

Решение данной проблемы определяет основную **цель исследования** – выявить наиболее эффективную методику преподавания в обеспечении личной безопасности в реальных условиях нападения.

Объект исследования – процесс организации и подготовки в штурмовом бою.

Предмет исследования – формирование устойчивых навыков активной безопасности.

В основу исследования положена следующая **гипотеза.** Традиционный подход обеспечения личной безопасности граждан, базирующийся на изучении спортивных единоборств демонстрирует свою несостоятельность. Спортивный рукопашный бой не может решать проблемы личной безопасности человека в реальном уличном столкновении.

Можно сколь угодно заниматься штурмовым боем, оттачивая любимые приемы и способы боя, и не знать истинный уровень своей подготовки в настоящий момент, что может привести к неадекватному реагированию на опасность – или переоценить свои возможности, или недооценить их, что в любом случае является факторами риска собственной безопасности. Необходимо осуществлять систематический контроль уровня собственной боеспособности, то есть постоянной готовности к бою. Знать свой уровень боеспособности – это половина победы, поскольку можно адекватно реагировать на любое нападение, используя те боевые ресурсы, которыми в значительной мере владеет защищающийся.

Боеспособность – способность к бою, интегральный показатель постоянной психофизической готовности человека к любому бою. Определение уровня боеспособности бойца даст точную оценку его боевых возможностей и позволит скорректировать тренинговую программу в подтягивании к достаточному уровню отстающих знаний и умений.

Организация исследования проводилось в три этапа, и заключалась в определении:

1. Характеристик двигательной реакции в защите и нападении.
2. Уровня боеспособности бойцов различной подготовленности.

3. Эффективности боевых действий в соревновательном стандарте штурмового боя.

Экспериментальной базой исследования являлись: Орловский государственный технический университет, Орловский государственный университет, Межрегиональная Академия безопасности и выживания. В исследовании приняли участие студенты в возрасте 17-21 лет, проходящих обучение в вузах г. Орла (всего 112 человек), что позволило выделить три контрольные и экспериментальные группы различного года обучения:

- Группа начальной подготовки первого года обучения (НП-1) численностью 44 человека. Практические занятия проводятся в количестве 4,5 часов в неделю.
- Учебно-тренировочная группа второго года обучения (УТ-2) численностью 36 человек. Практические занятия проводятся в количестве 6 часов в неделю.
- Учебно-тренировочная группа третьего года обучения (УТ-3) численностью 32 человека. Практические занятия проводятся в количестве 9 часов в неделю.

Каждую группу образуют учащиеся одной возрастной группы и одного уровня подготовки, что является важным условием в проведении чистоты исследования.

К контрольным группам относятся студенты различного уровня подготовки и занимающиеся спортивным рукопашным боем в спортивных секциях клубах г. Орла. Контрольная группа первого года обучения (НП-1) рукопашным боем РБ-1 составляет 22 человека, не имеющих разрядов по спортивным единоборствам (новички). Контрольная группа второго года обучения (УТ-2) рукопашным боем РБ-2 составляет 18 человек, имеющих начальный опыт занятий спортивными единоборствами. Контрольная группа третьего года обучения (УТ-3) рукопашным боем РБ-3 составляет 16 человек, имеющих опыт занятий спортивными единоборствами не менее 2 лет или спортивный разряд не ниже второго.

В экспериментальные группы входят студенты различного уровня подготовки и занимающиеся штурмовым боем в Межрегиональной Академии безопасности и выживания. Экспериментальная группа первого года обучения (НП-1) штурмовым боем ШБ-1 составляет 22 человека (новички). Экспериментальная группа второго года обучения (УТ-2) штурмовым боем ШБ-2 составляет 18 человек, имеющие начальный опыт занятий

штурмовым боем. Экспериментальная группа третьего года обучения (УТ-3) штурмовым боем ШБ-3 составляет 16 человек, имеющих опыт занятий штурмовым боем не менее 2 лет.

Целью первого этапа исследования является определение времени реакции защиты и нападения. Исследование проводили в тренировочных условиях на бойцах различного года обучения. Определяли возможности двигательной реакции (ДР) в атаке-защите и плотность атакующих действий (ПАД).

При определении двигательной реакции, исследуемый и его партнер находились друг перед другом на средней дистанции в разговорной (руки опущены вдоль туловища) или боевой стойке (руки на уровне головы). Исследуемый сначала выполнял 20 атак быстрым касанием пальцами лба (верхний уровень) или живота (нижний уровень) партнера. Фиксируется четкое попадание в указанные зоны, указывающее на результативность выполненной атаки. Затем исследуемый защищался отбивами, уклонами, нырками и другими защитными техническими действиями не разрывая дистанцию. Оценивается эффективность защиты от наносимых ударов-касаний в верхний и нижний уровни.

Плотность атакующих действий определяли в боевой стойке на боксёрском мешке. По звуковому сигналу исследуемый на средней дистанции из боевой стойки максимально быстро наносил удары двумя руками и (или) ногами по боксёрскому мешку за заданное количество времени. Регистрация ПАД осуществлялась снятием всего процесса на видеокамеру. Далее весь видеоматериал обрабатывался на компьютере, и покадровый просмотр позволяет точно подсчитать количества ударов руками и (или) ногами по боксерскому мешку за заданное количество времени.

Второй этап исследования проводился в начале каждого учебного года в октябре-месяце. Поскольку в учебно-тренировочном процессе по штурмовому бою отсутствуют специализированные этапы подготовки к соревнованиям, поэтому готовность к бою у бойцов должна быть постоянной, а не зависеть от тренировочных циклов. Уровень боеспособности начинал тестироваться с определения физической подготовки. Вначале выполнялись упражнения скоростной и скоростно-силовой направленности, затем – координационные, и заканчивались упражнениями на выносливость. На втором этапе определялась техническая подготовка бойцов. Третий этап заканчивал тест на психическую подготовку.

Время на определение уровня боеспособности занимал не более двух недель. Если замеры показателей между первым исследуемым и последним будут составлять более двух недель, то возможна некоторая неточность определения уровня боеспособности, поскольку степень тренированности занимающихся будет разной на момент тестирования.

Третий этап исследования для определения боевого рейтинга проводился в течение всего года после состязательных боев по штурмовому бою. Итог подводился в конце года в мае-месяце после рейтинг-турнира. Итоговый боевой рейтинг выставляется по результатам всех проведенных поединков.

2. Первый этап исследования

Характеристики двигательной реакции в защите и нападении. В спортивной практике скоростные способности атлета проявляются в виде различных форм проявления быстроты, обусловленными различными пусковыми механизмами и относительно независимы друг от друга. (Н.В. Зимкин, 1956; В.С. Фарфель, 1960; В.М. Зациорский, 1966; И.Л. Дегтярев, 1970; Л.П. Матвеев, 1977). С учетом этого выделяют два типа быстроты: быстроту как способность к экстренным двигательным реакциям и быстроту как способность, определяющую скоростные характеристики движений (Л.П. Матвеев, 1991). Таким образом, процесс реакции является важнейшей частью общей структуры психомоторного акта, во многом обуславливая успех его выполнения (Г.М. Гагаева, 1935). По данным психологических исследований, проводимых со спортсменами-боксерами, известно, что время атакующих действий боксеров находится в среднем 140 – 200 мс. Тогда как время простой защитной реакции составляет 400 – 450 мс (В.И. Филимонов, 2000; В. Н. Остьянов, И. И. Гайдамак, 2001). Обращает внимание тот факт, что время даже простой защитной реакции минимум в два раза больше времени атаки, или быстроты удара. На самом деле атакующее движение может быть неожиданным не только по времени (начало атаки), но и по траектории, и по используемой части тела. В этом случае время ответной реакции увеличивается уже в 3 – 4 раза, и таким образом, шансы на защиту у противника становятся ничтожными. Следовательно, любой человек, независимо от уровня своего физического развития и предварительной подготовки не успевает среагировать на реальную атаку при определенных условиях. Эти условия можно легко обеспечить в реальной ситуации путем контроля дистанции до противника. Для гарантированного нанесения поражающего удара в выбранную цель необходимо обеспечить лишь дистанцию вытянутой руки (в любом направлении).

Ключом к выполнению результативной атаки является дистанция поражения (дистанция поражения – дистанция при которой возможно поражение противника рукой или ногой без движения вперед), в пределах которой очень сложно защититься от неожиданного удара. Дистанция поражения ограничена пределами досягаемости вытянутых рук и ног человека в зависимости от возраста, уровня его развития и психофизического состояния. В противном случае,

контроль зоны пространства за границами вытянутых рук или ног требует участия всего тела, которое должно вытянуться в направлении атакуемой цели. Это движение в несколько раз продолжительнее, чем быстрота удара рукой или ногой, и поэтому противник успеет среагировать на атаку и нейтрализовать ее. В пределах дистанции поражения достаточно сложно защититься от быстрого и неожиданного удара. Однако на указанной дистанции, все быстрые атаки поражения становятся неотразимыми, при условии выполнения их на опережение противника. Это означает, что любой человек (независимо от уровня своей подготовки) абсолютно беззащитен, если удар против него выполняется на дистанции поражения.

Нами обнаружены и зафиксированы данные о неспособности человека адекватно реагировать на неожиданную атаку в пределах дистанции поражения. Результаты показателей двигательной реакции представлены в таблице 1.

Показатели двигательной реакции

Таблица 1.

№ п/п	Показатели	Уровень подготовки		
		1 год обучения (n=44)	2 год обучения (n=36)	3 год обучения (n=32)
1	Результативные атаки в нижний уровень из разговорной стойки	75	85	90
2	Нейтрализующие защиты из разговорной стойки (руки опущены вниз) от атак в нижний уровень	20	30	25
3	Результативные атаки в верхний уровень из разговорной стойки	65	65	75
4	Нейтрализующие защиты из боевой стойки от атак в верхний уровень	25	30	35
5	Результативные атаки в верхний или нижний уровень по выбору из боевой стойки	85	80	90
6	Нейтрализующие защиты из боевой стойки от атак в верхний или нижний уровень по выбору	10	10	15
		P<0,02, t=1,64		

Показатели результативных атак в нижний уровень из разговорной стойки для новичков достаточно высоки и составляют 75 %. Это обусловлено тем, что атаки проводились на дистанции поражения, где возможность защиты сводится к минимуму. Занимающиеся третьего года обучения свои показатели улучшили до 90 % результативных атак. Результаты нейтрализующих защит из разговорной стойки от атак в нижний уровень достаточно низки. У новичков эти показатели составляют не более 20 %, и даже квалифицированные бойцы второго и третьего года обучения показывали результаты не выше 30 % эффективных защит. Данные показатели еще больше ухудшаются при условии выполнении атак в разные уровни. Здесь играет очень важную роль фактор непредвиденности поражения цели. Защищающийся не успевает среагировать на проведенную против него атаку. Для новичков эти показатели составляют не более 10%, а для опытных бойцов – не более 15 %.

Анализ данных показывает, что необходимо контролировать расстояние до противника и не подпускать его на дистанцию поражения. Если это произошло, то атаковать следует первым и не ждать, когда противник нанесет удар. Выжидание чрезвычайно опасно. Это подтверждает один из главных принципов, что в бою лучше действовать самому, чем реагировать на действия противника. На дистанции поражения любая неожиданная и быстрая атака достигнет цели. В штурмовом бою первый удар, проводимый за пределами поля поражения, скорее всего, не достигнет цели. Однако если он будет выполняться в связке из двух и более ударов, то все последующие удары станут неотбиваемыми, даже если противник легко парирует первый удар, все остальные удары окажутся для него поражающими.

В последние годы на различных соревнованиях по спортивным единоборствам существенно возросла плотность боевых действий на ринге, то есть количество выполняемых в поединке передвижений, защит, обманных действий и ударов. В этой связи повышенные требования предъявляются к уровню развития у рукопашников моторных качеств (В.И. Филимонов, 2000).

Плотность атакующих действий (табл. 2) характеризует высокий уровень развития психомоторных качеств бойца.

Показатели плотности атакующих действий

Таблица 2.

№ п/п	Показатели	Уровень подготовки		
		1 год обучения (n=44)	2 год обучения (n=36)	3 год обучения (n=32)
1	Плотность атаки ударов руками за 3 с. (Кол-во ударов за 3 с (n)	15,3	19,5	23,1
2	Плотность атаки ударов руками за 10 с. (Кол-во ударов за 10 с (N)	51,2	64,6	80,3
3	Коэффициент сохранения энергии атаки руками: (N / 10) / (n / 3) × 100%	0,94	0,99	1,04
4	Плотность атаки ударов ногами за 3 с. (Кол-во ударов за 3 с)	12,5	12,8	14,9
5	Плотность атаки ударов руками и ногами за 10 с. (Кол-во ударов за 10 с)	14,3	17,1	20,2
6	Коэффициент согласованности атаки руками и ногами (п.4 / п.1 × 100%)	0,76	0,67	0,64
		P<0,02, t=2,16		

В исследованиях, проводимых ранее (Ф.А. Лейбович, В.И. Филимонов, 1979) были зафиксированы показатели плотности атакующих действий у членов сборной команды СССР по боксу. Среднее значение количества ударов руками нанесенных за 15 с составляет для различных весовых категорий 95,9 – 98,8 ударов, что составляет 6,3 – 6,5 ударов за 1 с. В нашем случае, высокие показатели плотности атаки руками имеют бойцы третьего года обучения и составляет 80,3 ударов за 10 с, что соответствует 8,0 ударам за 1 с. Такой высокий показатель занимающихся штурмовым боем характеризуется, прежде всего, непрерывностью и скоростью круговых и спиралевидных траекторий нанесения ударов руками, а также различной ударной формой. Следует отметить важную особенность ударов боксеров или рукопашников: величина ударов руками в значительной степени зависит от вложения в них массы тела, что снижает скорость, а значит и плотность атакующих действий.

Коэффициент согласованности атаки руками и ногами (табл. 2) показывает взаимодействие рук и ног в создании единой ударной динамики. С повышением квалификации занимающихся плотность ударов руками увеличивается (коэффициент 0,64) по отношению к действиям ног. У бойцов низкой квалификации наблюдается повышенное участие ударов ногами (коэффициент 0,76) по отношению к действиям рук. Это объясняется тем, что новички, участвующие в состязательных боях, стараются держать дальнюю дистанции, поэтому предпочитают больше наносить беспорядочные удары ногами, не вкладывая в них скорость и силу, и не выполняя их технически правильно, поэтому многие удары ногами имеют чисто формальный характер. Бойцы более высоких квалификаций выполняют удары ногами технически правильно и согласовывают движения отдельных участков тела в единое и мощное ударное движение.

Одним из важных показателей атакующих действий бойца является коэффициент сохранения энергии атаки руками (табл. 2). Данный коэффициент определяет длительность агрессивных атакующих действий, направленных на противника. Практически у всех бойцов независимо от квалификации данный показатель находится достаточно на высоком уровне. Это объясняется овладением занимающихся на начальном этапе пластичной манеры ведения боя, предусматривающей экономию энергии и уменьшением времени возвратов руки. Хотелось бы отметить такой факт. Квалифицированные бойцы третьего года обучения имеют коэффициент сохранения энергии больше единицы (1,04), что свидетельствует об увеличении ударов за единицу времени без потери качества. По-видимому, это может быть обусловлено высокой технической подготовленностью и развитием двигательных функций.

На основе данных исследований строится вся концепция штурмового боя, как агрессивно-атакующего стиля ведения боя. Любой бой должен начинаться и заканчиваться быстро. Чем дольше длится бой, тем меньше шансов победить. Нет времени на раскачку, разработку плана боя, разведку и другие подобные действия, применяемые в спортивных единоборствах. Атака должна начинаться и заканчиваться мощно и мгновенно, как взрыв, не наращивая постепенно скорость и силу. В атаке нельзя проявлять нерешительность и пассивность. Необходимо стремиться к тому, чтобы каждая атака достигала цели, подавляя дух противника.

Мы показали, что обычный человек, далекий от боевых искусств, способен уверенно побеждать любого противника независимо от уровня его подготовки, физических возможностей и антропометрических данных.

3. Второй этап исследования

Уровень боеспособности бойца в настоящее время условно представляет собой индивидуальный числовой показатель. Цель определения уровня боеспособности состоит в том, чтобы тренер мог иметь наглядное представление о готовности учеников противостоять агрессивному нападению. Уровень боеспособности дает возможность отслеживать динамику развития каждого бойца и своевременно реагировать на коррекцию в тренировочной программе. Что немаловажно, мы получаем не общее, а детальное, всестороннее представление о тенденциях роста мастерства учеников. Это позволяет принимать конкретные, точные решения, реально повышающие эффективность тренировок. Определение уровня боеспособности проходит по следующим показателям:

- физическая подготовка;
- техническая подготовка;
- психическая подготовка.

Боец должен всегда быть готовым к бою физически, технически и психически. Если хотя бы одного из этих видов готовности недостает, страдает боевая эффективность. Так, без физической подготовки боец не может действовать с надлежащей быстротой, силой, ловкостью, выносливостью; без технической подготовки он не обладает умениями и навыками ведения схватки; без психической подготовки бойцу не хватает уверенности в себе и стремления к победе.

Оценка уровня боеспособности бойца строится присуждением по каждому из перечисленных положений определенного количества баллов, от одного до десяти, и суммируются в общий числовой показатель. Максимальная суммарная оценка каждого критерия не превышает 100 баллов. Суммарная оценка по трем показателям равна числовой форме 100+100+100, следовательно, максимальный уровень боеспособности бойца равен числу 300. Боец с максимальным уровнем боеспособности, имеющий числовой показатель равный 300 баллов, является идеальным уровнем готовности к реальному бою. Любой другой уровень определяет боеспособность ниже идеального. Графическая диаграмма (рис. 1) дает первоначальное представление о сущности расчета боеспособности бойца.

Например, уровень боеспособности (БСП) бойца определяется шесть раз за один учебный год (9 месяцев, сентябрь-июнь) (табл. 1).

Показатели уровня БСП

Таблица 1.

Дата регистрации уровня БСП	Физический	Технический	Психический	**Уровень БСП**
15.09.2011	50	20	30	**100**
17.11.2011	60	40	45	**145**
24.12.2011	65	70	50	**185**
25.02.2012	70	80	50	**200**
10.04.2012	70	85	60	**215**
27.05.2012	85	90	65	**240**

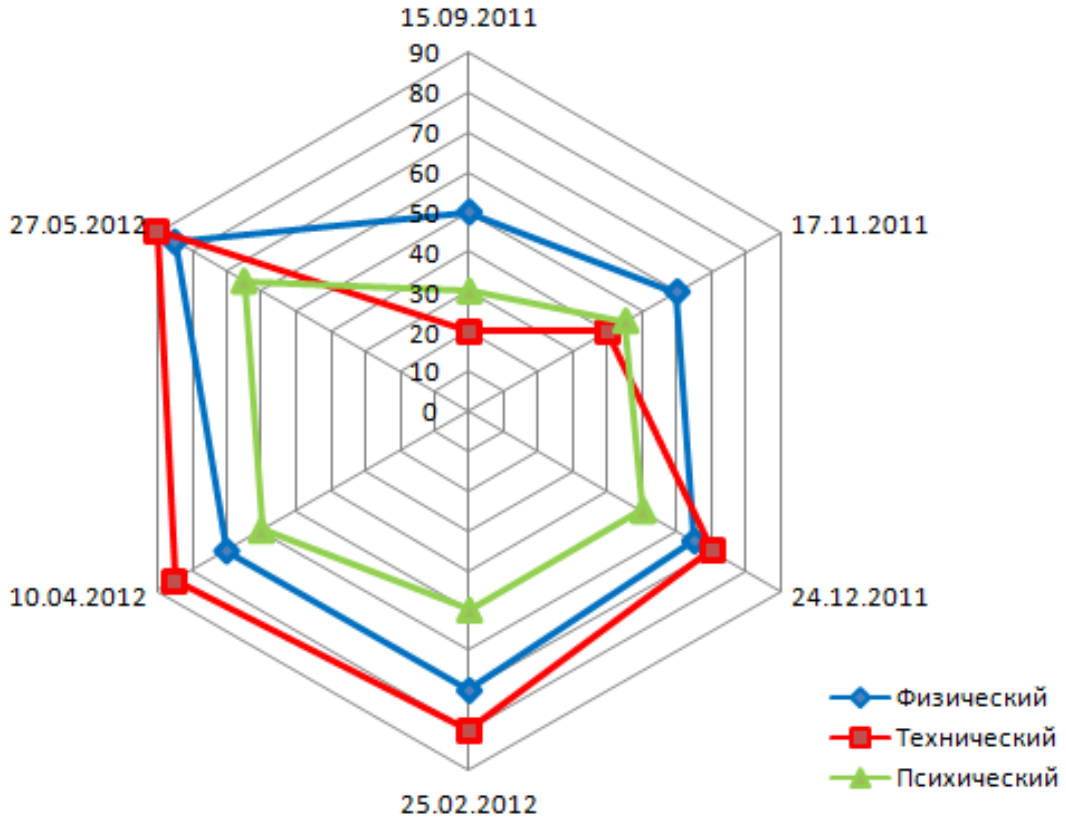


Рис. 1. Графическая диаграмма показателей уровня БСП

Критерии оценки физической подготовки. В штурмовом бою непременным условием эффективности боевых действий является физическая подготовка, и занятия самообороной не могут заменить общефизический тренинг. Следовательно, для того, чтобы иметь возможность сочетать разностороннюю боевую подготовку с

обширной программой физической подготовки, необходимо уделять достаточное время физической подготовки.

Определение физической подготовки занимающихся осуществляется выполнением десяти видов упражнений, по итогам которых ставится оценка от одного до десяти баллов (табл. 2).

Оценка физической подготовки (в баллах)

Таблица 2.

Оценка в баллах	**Виды упражнений**									
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1 балл	20	10	29	100	28	195	1	9	3	6
2 балла	25	11	30	110	27	200	2	10	4	7
3 балла	30	12	31	120	26	205	3	11	5	8
4 балла	35	13	32	130	25	210	4	12	6	9
5 баллов	40	14	33	140	24	215	5	13	7	10
6 баллов	45	15	34	150	23	220	6	14	8	11
7 баллов	50	16	35	160	22	225	7	15	9	12
8 баллов	55	17	36	170	21	230	8	16	10	13
9 баллов	60	18	37	180	20	235	9	17	11	14
10 баллов	65	20	38	190	19	240	10	18	12	15

Показатели всех видов упражнений складываются и дают итоговое значение уровня физической подготовки занимающихся в настоящее время.

Виды упражнений для оценки физической подготовки занимающихся:

1. *Отжимания*. Упор лежа, руки на ширине плеч. Отжимания от пола на кулаках, (кол-во раз).

2. *Подтягивания*. Свободный вис на горизонтальной перекладине, руки на ширине плеч, хват ладонями от себя. Подтягивания на перекладине до касания ее подбородком, (кол-во раз).

3. *Пресс*. Лежа на спине, ноги согнуты в коленях, стопы на полу. Поднимание туловища из положения лежа в положение сидя за 40 с, (кол-во раз).

4. *Скакалка*. Прыжки через скакалку за 60 с, (кол-во раз).

5. *Челнок*. Используя размеры волейбольной площадки, выполнять челночный бег по схеме (0+6+6+9+9+12+12+18+18 = 90

м): от линии начала площадки бег до линии 6 м, затем возврат назад, далее до линии 9 м и назад, далее до линии 12 м и назад, далее до конца площадки 18 м и назад до стартовой линии. Всего – 90 м. Оценивается время (в секундах) всего бега.

6. *Прыжок*. Прыжок в длину с места, (см).

7. *Уклоны*. С дистанции 3-х метров выполнить 10 бросков в голову теннисным мячом. Уклоны от летящего в голову теннисного мяча, (кол-во раз).

8. *Толчок*. Из боевой стойки толчок на дальность сильнейшей рукой набивного мяча весом 3 кг, (м).

9. *КСУ*. Контрольно-силовое упражнение (КСУ). Без перерыва выполнить пять серий по десять повторений, следующих друг за другом упражнений:

- Исходное положение: сидя, ноги на ширине плеч, руки за головой, спина прямая. Выпрыгивания вверх из глубокого приседания.

- Исходное положение: лежа, упор руками в пол, ладони находятся на расстоянии не более ширины плеч, корпус прямой. Касаясь грудью, отжимания от пола на полностью выпрямленные руки.

- Исходное положение: лежа, упор руками в пол, ладони находятся на расстоянии не более ширины плеч, корпус прямой. На один счет выполнить «упор сев – упор лежа» быстрым отталкиванием ног от пола поставить их на линии груди и сразу без остановки вернуться в исходное положение.

- Исходное положение: лежа на спине, ноги поджаты под себя и всей стопой стоят на полу, руки за головой. Поднимание туловища из положения лежа в положение сидя, касаясь грудью коленей ног.

10. *Борьба*. Вольная борьба (схватка по правилам самбо или вольной борьбы) без потери концентрации (отсутствует явно выраженная одышка или усталость, боец способен бороться дальше на равных с равным соперником), (мин).

Критерии оценки технической подготовки. Для достижения победы в настоящем бою первостепенное значение имеет овладение надежной и простой техникой, и закрепление ее в двигательных навыках. Техническая подготовка представляет собой комплекс специальных приемов и способов боя, необходимых для успешного и эффективного ведения боя против любого противника. Она дает бойцу возможность решать сложные двигательные задачи в

различных боевых ситуациях. Чтобы достичь необходимых результатов в этих условиях, боец должен владеть значительным набором приемов и способов техники.

Для определения уровня технической подготовки бойцов моделируется десять разнообразных атак с реальной скоростью и силой бойцами различного уровня подготовки. В каждой атаке по 10-бальной шкале оценивается умение защищаться любыми способами в рамках изученной технической базы системы. Показатели всех атак суммируются и дают значение технической подготовки.

1 балл = Первый уровень защиты – применение техники в схеме «защита – без контратаки». Применение примитивных защит от атак противника в виде подставок, отбивов, уходов с линии атаки.

2 балла = Второй уровень защиты – применение техники в схеме «защита – контратака». На любую атаку противника боец реагирует защитой и контратакой. Защита и контратака должны быть проведены уверенно, пусть даже и с небольшими ошибками, без надлежащей концентрации и импульса.

3 балла = Третий уровень защиты – применение техники в схеме «защита – реальная контратака». Боец адекватно реагирует на любую атаку противника, и после защиты выполняет мощную, быструю, убедительную контратаку. Скорость, мощность, концентрация должны соответствовать требованиям реального боя.

4 балла = Четвертый уровень защиты – применение техники в схеме «защита с контратакой». Контратакующие действия выполняются не после защиты, а одновременно с ней. Защита данного уровня требует максимальной реакции реагирования и взрывной быстроты. Боец выполняет быструю защиту с одновременной безусловной контратакой без концентрации на силе и скорости, возможно допущение незначительных ошибок в технике.

5 баллов = Пятый уровень защиты – применение техники в схеме «защита с реальной контратакой при любой атаке». Боец отвечает на любую одиночную, но в полную мощность реальную атаку противника защитой с одновременным поражающим действием, не оставляющей возможностей для новой атаки. Контратака должна быть убедительной и эффективной.

6 баллов = Шестой уровень защиты – применение техники в схеме «защита с реальной контратакой – добивание». На любую атаку противника боец реагирует защитой с контратакой с обязательным добиванием, по возможным схемам:

- блок, подставка – удар – бросок, сваливание, выведение из равновесия – добивание;

- уклон (нырок) – удар – бросок, сваливание, выведение из равновесия – добивание;

- проваливание – удар – бросок, сваливание, выведение из равновесия – контролирование.

7 баллов = Седьмой уровень защиты – применение техники в схеме «опережение начавшейся атаки». Защищающийся здесь уже не совсем «защищающийся», скорее нападающий в момент начала атаки противника. Этап требует совершенного чувства дистанции, мгновенной реакции, прекрасной координации и быстроты действий. Никакой защиты кроме опережения. Боец проводит поражающую атаку в наиболее благоприятные моменты боя – дистанция, инерция, отвлечение, начало атаки противника.

8 баллов = Восьмой уровень защиты – применение техники в схеме «пресечение штурмовой атакой». Лучшая защита – это нападение. Совершенно не учитываются действия и реакции противника, так как они замкнуты в гипотетическом временном континууме, стремящемся начаться уже после окончания атаки защищающегося. Остаются только принципы движений. Боец проводит штурмовую поражающую атаку на пресечение атакующих действий противника.

9 баллов = Девятый уровень защиты – применение техники в схеме «защита от управлением». Действия бойца строятся на проваливании атак противника в скольжение, управлении его действиями и вхождение в ближний бой с целью жесткого удара или захвата с последующим сбиванием и добиванием. Стратегия управления характеризуется мягкой защитой на действия противника, но жесткой и мгновенной атакой.

10 баллов = Десятый уровень защиты – применение техники в схеме «бесконтактная защита». Боец способен пропускать мимо себя мощные атаки противника без непосредственного контакта с ним. Работа строится на принципах и законах выведения из физического равновесия, создавая «пустоту» перед противником.

Критерии оценки психической подготовки. Психическая подготовка в боевой самообороне от преступных посягательствах важнее всякой другой, поскольку ее главная цель – преодоление страха и воспитание веры в собственные силы. Самые эффективные

техники и физическая сила не помогут тому, кто боится преступника. Страх ограничивает, мешает, сковывает действия бойца. Поэтому в критической ситуации, боясь потерять здоровье или жизнь, человек совершает одну ошибку за другой. Необходимо сконцентрироваться не на последствиях и исходе боя, а на его текущем моменте. Нужно драться изо всех сил и бороться за свою жизнь всеми доступными способами.

Одним из способов оценки психической подготовки является апостольский круг. Апостольский круг предусматривает проведение свободных штурмовых боев с реальным натиском без защитного снаряжения по 20 секунд с каждым из 10 бойцов, находящихся в кругу, без перерыва на отдых. Необходимо выстоять весь круг, не проиграв противнику и не отказавшись от боя (один бой = 10 баллов). Бои проводятся с бойцами равными по уровню испытуемого. Показатели всех боев складываются и дают значение психической подготовки.

Под термином «боеспособность» подразумевается совокупность различных параметров, обусловливающих достижение определенного уровня готовности к бою. В настоящее время невозможно управлять процессом подготовки бойцов, не зная величины ведущих признаков их боеспособности, определяющих стабильные достижения в самообороне. С учетом этого нами проведено исследование, в котором у каждого из 112 обследованных были зафиксированы показатели уровня боеспособности (табл. 3) учащихся контрольных групп рукопашного боя (РБ) и экспериментальных групп штурмового боя (ШБ) различного года обучения.

Показатели уровня боеспособности БСП

Таблица 3.

№ п/п	Показатели	Группы различного года обучения					
		1 год обучения (n=44)		2 год обучения (n=36)		3 год обучения (n=32)	
		РБ-1	ШБ-1	РБ-2	ШБ -2	РБ-3	ШБ -3
1	Возраст (средний показатель)	17,8	17,6	18,7	18,5	20,3	20,1
2	Физический уровень	26,3	25,5	48,2	38,9	69,4	56,4
3	Технический уровень	12,6	12,1	32,7	32,8	55,4	69,6
4	Психический уровень	20,0	20,9	34,4	42,2	55,6	72,5
5	Уровень боеспособности	58,9	58,5	115,3	113,9	180,4	198,5
6	**(%) от максимального уровня боеспособности**	**19,6**	**19,5**	**38,4**	**38,0**	**60,1**	**66,2**

Обобщенные результаты уровня боеспособности бойцов контрольных групп рукопашного боя и экспериментальных групп штурмового боя различного года обучения представлены на рис. 2.

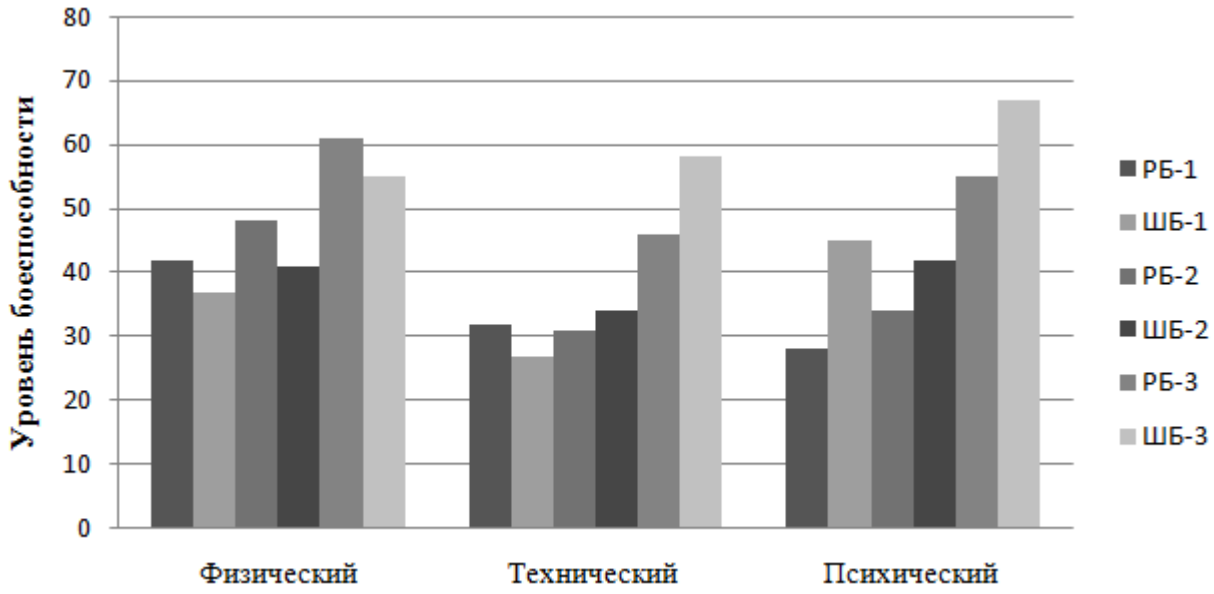


Рис. 2. Показатели уровня боеспособности

Следует отметить, что в исследуемой выборке средний уровень боеспособности в контрольной группе РБ-1 несколько выше на 0,2%, чем в экспериментальной группе ШБ-1. Такое незначительное преимущество свидетельствует о практически равных психофизических способностей занимающихся обеих групп. Однако показатель психической подготовки в экспериментальной группе ШБ-1 выше на 4,3%, чем в контрольной группе РБ-1. Это объясняется тем, что процесс обучения штурмовому бою начинается с жестких психологических установок на реальное столкновение, затем переходит на формирование двигательных способностей занимающихся. Примечательно, что этот показатель уже со второго года обучения у занимающихся штурмовым боем выше уже на 18,5%, на третьем году обучения данный показатель увеличивается уже на 23,3% и уровень психической подготовки практически составляет 2/3 общего уровня боеспособности.

Технический уровень во всех группах изменяется пропорционально по годам обучения и носит закономерный характер. Однако учащиеся третьего года обучения экспериментальной группы ШБ-3 показывают более высокий уровень технической подготовки. Данный факт объясняется тем, что техническая база штурмового боя проста и доступна в изучении и эффективна в условиях

максимального стресса. Все действия направлены исключительно на практическую составляющую и индивидуально адаптируются к любому уровню подготовки ученика.

Физический уровень в экспериментальной группе первого года обучения ШБ-1 ниже на 3,0%, чем в контрольной группе РБ-1, что свидетельствует о разности начальной физической подготовленности учащихся и недостаточном опыте занятий физическими упражнениями. Однако уже на втором году обучения и далее на третьем году в группах рукопашного боя этот показатель изменятся в сторону увеличения на 19,2% и 18,7% соответственно, подтверждающий смещение акцента в сторону физической подготовки. Представляет интерес такой факт. В группах рукопашного боя второго и третьего года обучения наблюдается большая разница показателей уровня боеспособности у занимающихся в одной группе. Напротив, в группах штурмового боя эта разница менее заметна. На наш взгляд в группах рукопашного боя одной из причин данного факта может являться неучитывание индивидуальных особенностей занимающихся и отсутствие смещения акцента тренировочного процесса в сторону отстающих показателей.

В целом уровень боеспособности всех групп рукопашного боя и штурмового боя изменяется закономерно в результате тренировочных занятий. В экспериментальной группе третьего года обучения ШБ-2 уровень боеспособности занимающихся значительно выше, чем в контрольной группе РБ-3, что доказывает эффективность треннинговой технологии штурмового боя в увеличении уровня боеспособности занимающихся.

Оценка психологической готовности к обеспечению личной безопасности. Волевые качества играют важную роль в обеспечении личной безопасности. Поэтому основная задача волевой подготовки — научить студента максимально мобилизовать свою волю, необходимую для достижения цели в реальном уличном столкновении. К волевым качествам, которые необходимо воспитать в процессе занятий, относятся: целеустремленность, настойчивость, инициативность, смелость, решительность, уверенность, само-обладание.

В оценке психологической готовности мы использовали методику «Психологический анализ развития волевых качеств спортсменов» разработанную Б. Н. Смирновым для оценки развития

волевых качеств. Мы оценивали следующие психические качества бойцов по степени сформированности волевых умений: целеустремленность, настойчивость и упорство, решительность и смелость, выдержка и самообладание, самостоятельность и инициативность.

Целеустремленность. Целеустремленность может быть сформирована только на почве интереса студента к обеспечению личной безопасности и его личной заинтересованности в достижении высокой боевой готовности. Студент должен четко знать цели и задачи каждого тренировочного занятия и периода, представлять конкретно, к чему он должен стремиться в своей подготовке в течение нескольких ближайших лет, в противном случае, у него снижается интерес к занятиям и пропадает инициативность.

Настойчивость. Настойчивость совершенствуется постепенным преодолением возрастающей нагрузки во время выполнения различных упражнений общеразвивающих и специально-подготовительных, по овладению техники и тактики, со снарядами и тренажерами. Во время штурмовых боев с максимально приближенными боевыми условиями студент должен стремиться навязывать противнику свою манеру ведения боя, поддерживать высокий темп действий и вырывать победу у более сильного противника, не нарушая принципа ведения штурмового боя. Следует также выработать умение переносить болевые ощущения, преодолевать неприятные чувства, возникающие при максимальных нагрузках и утомлении.

Инициативность. Инициативность – это умение активно и самостоятельно стремиться как на занятиях, так и в рукопашных боях к поставленной цели без принуждения преподавателя. На занятиях боец не должен воспринимать задание лишь как обязанность, которую должен выполнить. Для развития инициативности в условном рукопашном бою следует давать различные задания. Полезно использовать также вольные бои с различными по манере ведения боя партнерами. Боец должен активно вести бой, применяя разнообразные тактические действия, не переходя к грубому обмену ударами, бросками, сваливаниями и т.д.

Уверенность в своих силах. От веры в свои силы часто зависит победа или поражение в столкновении с агрессивной силой. Уверенность обычно проявляется вместе с осознанием своих возможностей, с пониманием того, что, встречаясь с сильным

вооруженным или безоружным противником, студент сможет успешно противодействовать ему с наименьшей потерей для себя. Уверенность в своих силах появляется как результат совершенствования технической, тактической и физической подготовленности. Научившись вести рукопашный бой с противниками, различными по манере, весу, с одним или группой партнеров, с оружием и без него, студент начинает осознавать, что он может действительно победить сильного, хорошо подготовленного технически, тактически и физически противника, как одного, так и несколько, как вооруженных, так и без оружия. Очень важно не путать уверенность в своих силах с самоуверенностью, где студент недооценивает противника и теряет осторожность, которая может привести к трагическим последствиям.

Смелость и решительность. Смелость и решительность основываются на уверенности в своих силах, знании своих положительных сторон и достоинств, умении хорошо и быстро разбираться в боевой обстановке. Для развития смелости и решительности необходимо учить студента преодолеть боязнь и инертность, в тренировочных боях с соответствующими партнерами, а в боях с максимально приближенными боевыми условиями воздействовать на его самолюбие и чувство собственного достоинства. В условных рукопашных боев, студент должен получать задания на неожиданные и стремительные атаки, используя встречные удары, броски, сваливания, развивать атакующие боевые схемы, активно вести бой на любых дистанциях, а в штурмовых боях избегать пассивной тактики отхода и излишней осторожности. Следует широко использовать упражнения с партнерами для отработки мягких защит и жестких контратак, во всех упражнениях развивать быстроту реакции и быстроту движений.

Постановка диагноза и оценка волевых умений. Пользуясь описанием трех признаков проявления волевых умений, мы оценили степень развития волевых качеств у бойцов по шкале оценок: отчетливое проявление – 2 балла, неотчетливое проявление – 1 балл, не проявляется – 0 баллов, и зафиксировали соответствующие результаты в протоколе (рис. 3, табл. 4).

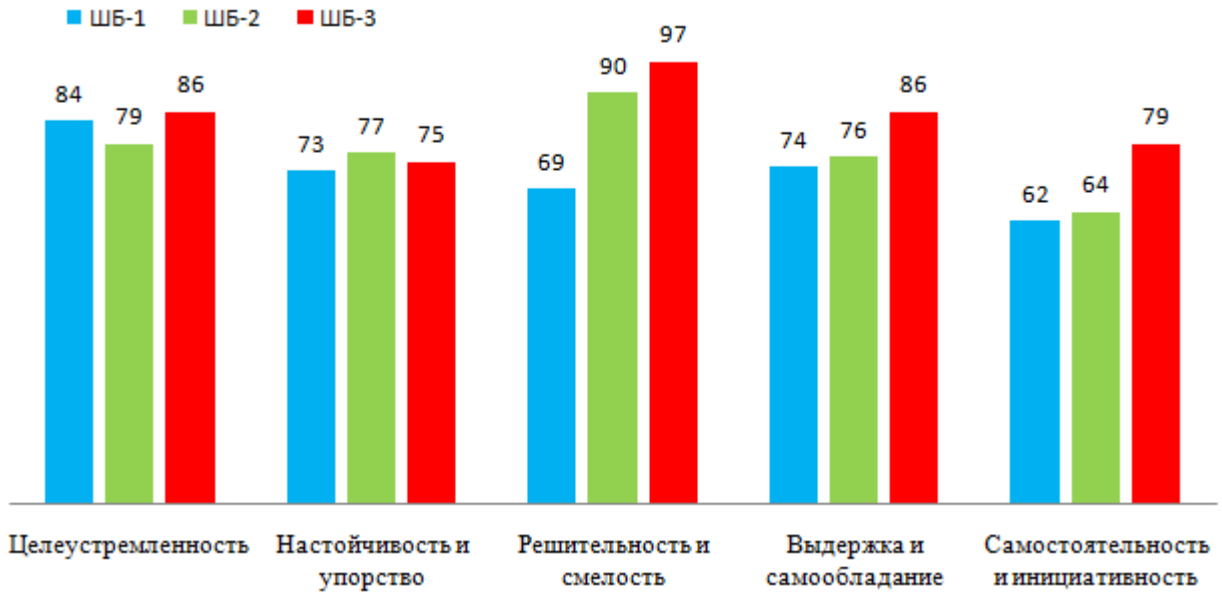


Рис. 3. Степень развития волевых качеств у бойцов

Следует отметить, что в исследуемой выборке волевые качества: самостоятельность и инициативность экспериментальной группы штурмового боя первого года обучения ШБ-1 низки на 22 % по сравнению с другими волевыми качествами, как целеустремленность, настойчивость и упорство. Такое преимущество свидетельствует о том, что на начальном этапе обучения штурмовому бою, бойцы еще не могут проявлять самостоятельность и инициативность в спарринговых сессиях. Однако данные показатели увеличиваются с годом обучения, и их прирост составляет 17%.

Примечательно, что решительность и смелость составляет наибольшую степень развития у бойцов второго и третьего года обучения ШБ-2, ШБ-3 и составляет 90% и 97% соответственно. Это объясняется тем, что штурмовой бой характеризуется активным наступательным стилем ведения боя, в котором от бойца требуется, прежде всего, смелость в проявлении атакующих возможностей и решительность в подавлении боеспособности противника.

Выдержка и самообладание во всех группах изменяется пропорционально по годам обучения и носит закономерный характер. Степень настойчивости и упорства в группах третьего года обучения ШБ-3 практически осталась неизменной по сравнению с исходными данными, что говорит о стабильности результатов.

Показатели оценки развития волевых качеств у бойцов

Таблица 4

№ п/п	Группы штурмового боя	Критерии					Оценка волевых качеств	Критерий Фишера F	Критерий Стьюдента	Коэффициент корреляции
		Целеустремленность	Настойчивость и упорство	Решительность и смелость	Выдержка и самообладание	Самостоятельность и инициативность				
1	ШБ-1, (n=22)	84	73	69	74	62	362	**2,12**	**0,35**	
2	ШБ-2, (n=18)	79	77	90	76	64	386	**1,34**	**0,44**	**0,76**
3	ШБ-3, (n=16)	86	75	97	86	79	423	**1,14**	**0,21**	

В целом степень развития волевых качеств у бойцов изменяется закономерно в результате тренировочных занятий по штурмовому бою.

Приложение 1

Показатели уровня боеспособности (БСП) контрольной группы рукопашного боя первого года обучения РБ-1

Таблица 1-1

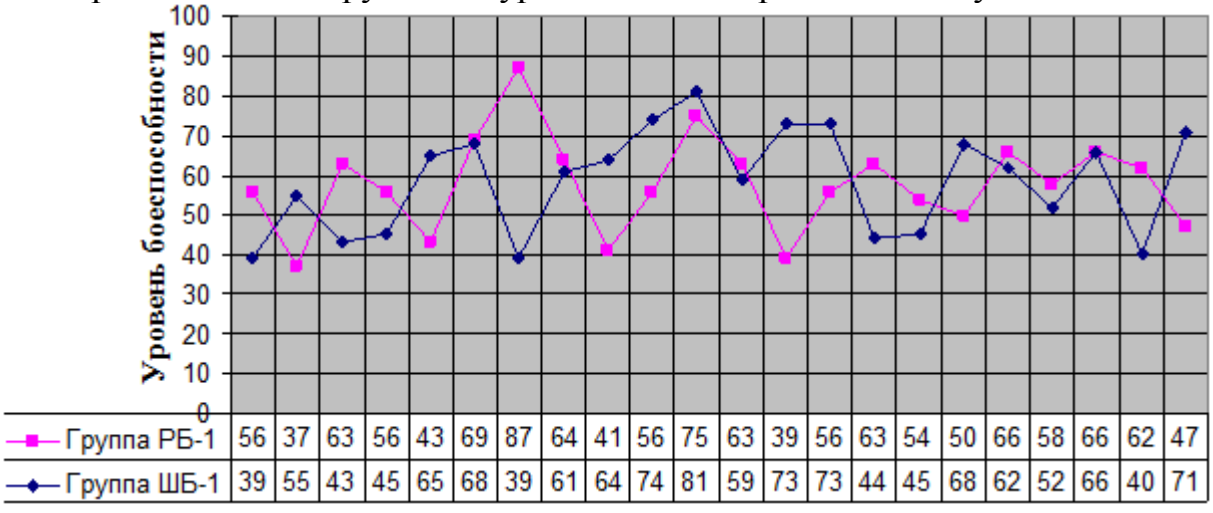
Фамилия	Критерии показателей			Уровень БСП	(%) от max	Суммарный уровень БСП	Размах БСП	Среднее значение	Отклонение от среднего значения	Дисперсия	Среднеквадратическое отклонение	Среднеквадратическое отклонение среднего	Доля уровня боеспособности в суммарном уровне (%)
	Физический	Технический	Психический										
Кочетков Н.	24	12	20	56	18,7				52				4,87
Артемов О.	16	11	10	37	12,3				37				2,73
Агафонов А.	32	11	20	63	21,0				63				4,64
Андреев М.	25	11	20	56	18,7				56				4,13
Батурин А.	20	13	10	43	14,3				43				3,17
Извеков С.	27	12	30	69	23,0				69				5,08
Басов В.	33	14	40	87	29,0				87				6,41
Глушков В.	32	12	20	64	21,3				64				4,72
Плетнев В.	19	12	10	41	13,7				41				3,02
Спицын Л.	26	10	20	56	18,7				56				4,13
Болонкин А.	31	14	30	75	25,0	**1357**	**50**	**59**	75	**176**	**13,6**	**0,27**	5,53
Герасимов Н.	22	11	30	63	21,0				63				4,64
Виноградов А.	18	11	10	39	13,0				39				2,87
Коблев А.	24	12	20	56	18,7				56				4,12
Бабарыкин А.	30	13	20	63	21,0				63				4,63
Баринов А.	37	16	20	54	24,3				54				3,98
Зимин В.	28	14	10	50	17,3				50				3,68
Гольцов С.	24	13	30	66	22,3				66				4,86
Антипов А.	27	15	20	58	20,7				58				4,27
Пономарев Г.	32	14	20	66	22,0				86				6,34
Шевцов Е.	29	13	20	62	20,7				62				4,57
Роньжин А.	23	14	10	47	15,7				44				3,24
ИТОГО	**26,3**	**12,6**	**20,0**	**59,0**	**19,7**				**59**				**4,35**

Показатели уровня боеспособности (БСП)
экспериментальной группы штурмового боя первого года обучения ШБ -1

Таблица 1-2

Фамилия	Критерии показателей			Уровень БСП	(%) от max	Суммарный уровень БСП	Размах БСП	Среднее значение	Отклонение от среднего значения	Дисперсия	Среднеквадратическое отклонение	Среднеквадратическое отклонение среднего	Доля уровня боеспособности в суммарном уровне (%)
	Физический	Технический	Психический										
Буров А.	17	12	10	39	13,0				39				2,91
Сигарев В.	24	11	20	55	18,3				58				4,33
Новицкий А.	19	14	10	43	14,3				40				2,99
Бондин С.	22	13	10	45	15,0				45				3,36
Воронков Е.	34	11	20	65	21,7				69				5,15
Притыкин В.	26	12	30	68	22,7				68				5,07
Бусурин Н.	18	11	10	39	13,0				39				2,91
Гололобов А.	27	14	20	61	20,3				61				4,55
Карпов Ю.	30	14	20	64	21,3				64				4,78
Левашов А.	31	13	30	74	24,7				64				4,77
Лисицкий А.	29	12	40	81	27,0	**1340**	**42**	**58,3**	81	**163**	**12,8**	**0,28**	6,04
Николаев Д.	28	11	20	59	19,7				59				4,40
Сафронов М.	31	12	30	73	24,3				77				5,74
Козаков В.	29	14	30	73	24,3				73				5,45
Иванов Р.	22	12	10	44	14,7				44				3,28
Ершов И.	23	12	10	45	15,0				45				3,36
Семененко Е.	25	13	30	68	22,7				58				4,33
Абросимов Р.	30	12	20	62	20,7				62				4,63
Должиков Р.	21	11	20	52	17,3				52				3,88
Осипов В.	26	10	30	66	22,0				70				5,22
Власихин П.	20	10	10	40	13,3				43				3,21
Демехин Е.	29	12	30	71	27,3				71				5,29
ИТОГО	**25,5**	**12,1**	**20,9**	**58,5**	**19,5**				**58**				**4,35**

Показатели уровня боеспособности (БСП)
контрольной группы рукопашного боя первого года обучения РБ-1 и
экспериментальной группы штурмового боя первого года обучения ШБ-1



Показатели уровня боеспособности (БСП)
контрольной группы рукопашного боя второго года обучения РБ-2

Таблица 1-3

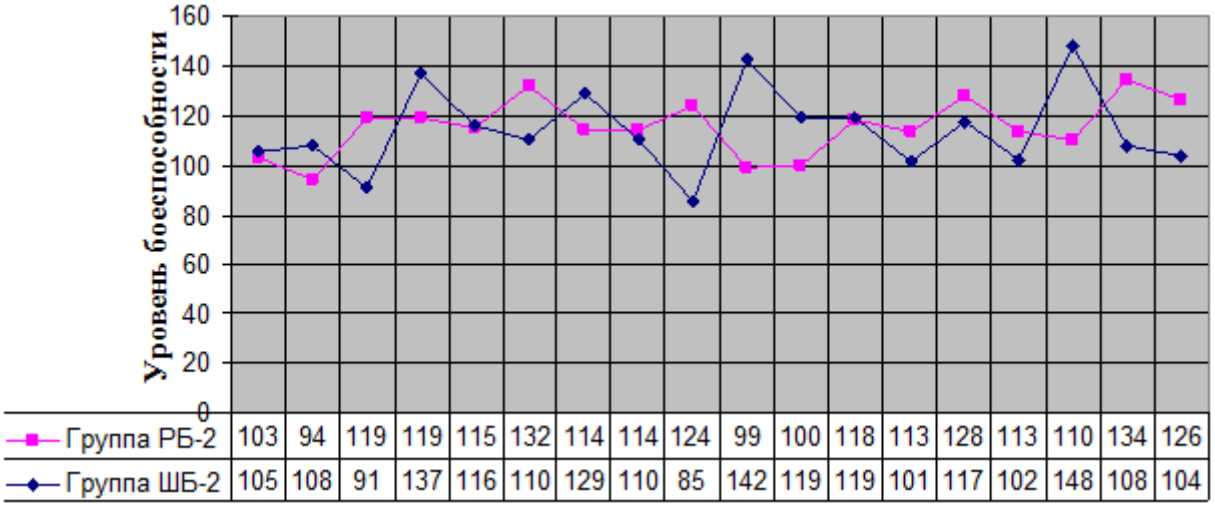
Фамилия	Критерии показателей			Уровень БСП	(%) от max	Суммарный уровень БСП	Размах БСП	Среднее значение	Отклонение от среднего значения	Дисперсия	Среднеквадратическое отклонение	Среднеквадратическое отклонение среднего	Доля уровня боеспособности в суммарном уровне (%)
	Физический	Технический	Психический										
Кочнев А.	50	33	20	103	34,3				91				4,27
Рябинин С.	45	29	20	94	31,3				93				4,41
Панин Н.	38	41	40	119	39,7				119				5,66
Кармазин Б.	51	38	30	118	39,6				118				5,65
Качалов Ю.	49	36	30	115	38,3				115				5,46
Коржевский И.	48	34	50	132	44,0				120				5,69
Фролов А.	46	28	40	114	38,0				110				5,22
Нефедов Н.	53	41	20	114	38,0				107				5,08
Попов Р.	57	37	30	124	41,3				119				5,65
Степанов В.	39	30	30	99	33,0				96				4,55
Баурин А.	41	19	40	100	33,3	**2105**	**39**	**110**	100	**137**	**11,7**	**0,29**	4,74
Мацнев О.	54	24	40	118	39,3				95				4,51
Муравлев С.	45	38	30	113	37,7				123				5,84
Тихомиров Д.	47	31	50	128	42,7				128				6,07
Щапов К.	58	25	30	113	37,7				113				5,36
Петров А.	44	36	30	110	36,7				106				5,03
Луговой С.	56	28	50	134	44,7				129				6,12
Архипов М.	46	40	40	126	42,0				113				5,36
ИТОГО	**48,2**	**32,7**	**34,4**	**115,3**	**38,4**				**111**				**5,26**

Показатели уровня боеспособности (БСП)
экспериментальной группы штурмового боя второго года обучения ШБ-2

Таблица 1-4

Фамилия	Критерии показателей			Уровень БСП	(%) от max	Суммарный уровень БСП	Размах БСП	Среднее значение	Отклонение от среднего значения	Дисперсия	Среднеквадратическое отклонение	Среднеквадратическое отклонение среднего	Доля уровня боеспособности в суммарном уровне (%)
	Физический	Технический	Психический										
Афанасьев И.	41	24	40	**105**	**35,0**				102				4,31
Иванов С.	32	26	50	**108**	**36,0**				118				5,14
Королев Е.	31	20	40	**91**	**30,3**				99				4,32
Леонов А.	43	34	60	**137**	**45,7**				140				6,09
Барыкин В.	37	29	50	**116**	**38,7**				128				5,57
Буджерин И.	50	30	30	**110**	**36,7**				115				5,00
Рогалев А.	51	38	40	**129**	**43,0**				129				5,61
Картаев Ф.	42	28	40	**110**	**36,7**				116				5,01
Никондров А.	32	33	20	**85**	**28,3**				91				3,96
Ломакин В.	45	37	60	**142**	**47,3**				149				6,48
Молчанов Н.	38	31	50	**119**	**39,7**	**2298**	**63**	**120**	119	**241**	**15,5**	**0,25**	5,18
Шемякин А.	42	27	50	**119**	**39,7**				123				5,35
Фуржиев С.	33	38	30	**101**	**33,7**				117				5,09
Турушев Р.	37	40	40	**117**	**39,0**				117				5,08
Сопов А.	40	32	30	**102**	**34,0**				124				5,34
Рябцев А.	44	44	60	**148**	**49,3**				154				6,70
Звягин А.	31	37	40	**108**	**36,3**				121				5,27
Алексеев Н.	32	42	30	**104**	**34,7**				120				5,22
ИТОГО	**38,9**	**32,8**	**42,2**	**113,9**	**38,0**				**122**				**5,26**

Показатели уровня боеспособности (БСП)
контрольной группы рукопашного боя второго года обучения РБ-2 и
экспериментальной группы штурмового боя второго года обучения ШБ-2



Показатели уровня боеспособности (БСП)
контрольной группы рукопашного боя третьего года обучения РБ-3

Таблица 1-5

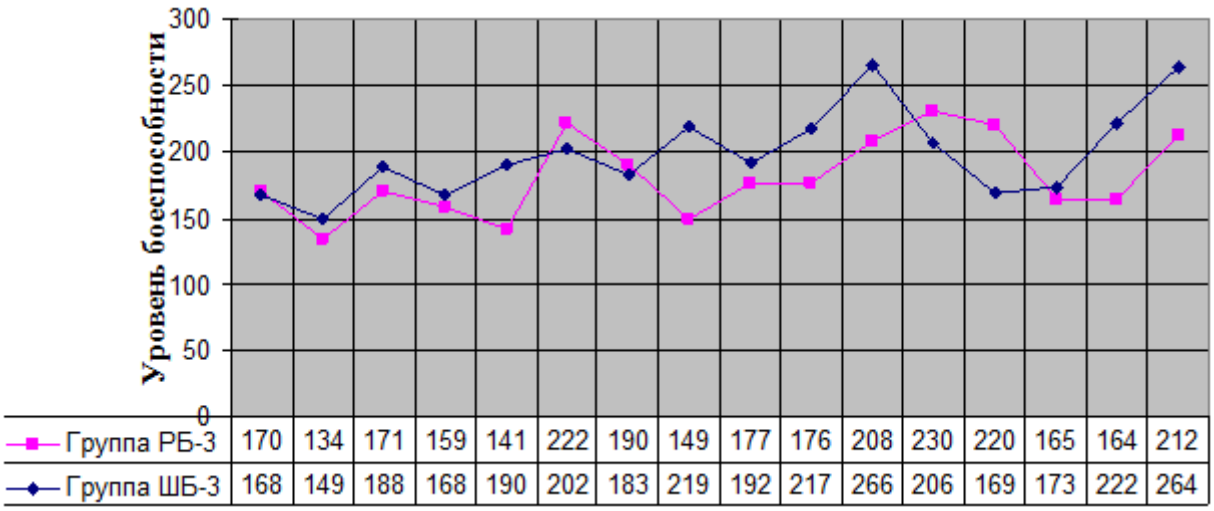
Фамилия	Критерии показателей			Уровень БСП	(%) от max	Суммарный уровень БСП	Размах БСП	Среднее значение	Отклонение от среднего значения	Дисперсия	Среднеквадратическое отклонение	Среднеквадратическое отклонение среднего	Доля уровня боеспособности в суммарном уровне (%)
	Физический	Технический	Психический										
Ливенцев Ю.	62	58	50	170	56,7				182				4,99
Мусихин Д.	55	39	40	134	44,7				134				4,11
Чемборисов С.	72	59	40	171	57,0				199				6,10
Мухаметов Н.	68	41	50	159	53,0				163				4,99
Кураков А.	59	42	40	141	47,0				153				4,69
Сотников С.	81	71	70	222	74,0				229				7,02
Аверкин Н.	67	63	60	190	63,3				190				5,82
Сайфулин А.	59	40	50	149	49,7				158				4,84
Турбанов Ю.	83	54	40	177	59,0				217				6,65
Грищенко С.	64	52	60	176	58,7				192				5,88
Волынский А.	73	65	70	208	69,3	**3264**	**119**	**192**	253	**1196**	**34,5**	**0,17**	7,75
Мышкин В.	82	68	80	230	76,7				224				6,86
Журавлев С.	90	70	60	220	73,3				233				7,14
Терский Ю.	60	55	50	165	55,0				165				5,06
Усков А.	58	46	60	164	54,7				167				5,12
Макушин И.	78	64	70	212	70,7				232				7,11
ИТОГО	**69,4**	**55,4**	**55,6**	**180,5**	**60,2**				**192**				**5,88**

Показатели уровня боеспособности (БСП)
экспериментальной группы штурмового боя третьего года обучения ШБ-3

Таблица 1-6

Фамилия	Критерии показателей			Уровень БСП	(%) от max	Суммарный уровень БСП	Размах БСП	Среднее значение	Отклонение от среднего значения	Дисперсия	Среднеквадратическое отклонение	Среднеквадратическое отклонение среднего	Доля уровня боеспособности в суммарном уровне (%)
	Физический	Технический	Психический										
Перелыгин А.	42	56	70	168	56,0				169				4,64
Журов А.	49	50	50	149	49,7				144				4,21
Парников В.	56	62	70	188	62,7				180				5,26
Родин М.	52	56	60	168	56,0				168				4,91
Елисеев Д.	66	64	60	190	63,3				194				5,67
Кузнецов И.	54	68	80	202	67,3				147				4,29
Павлов Э.	49	74	60	183	61,0				192				5,61
Жумабаев А.	51	68	100	219	73,0				256				7,48
Новиков С.	57	65	70	192	64,0				193				5,64
Дмитриев В.	61	76	80	217	72,3				241				7,04
Гаврилов В.	77	89	100	266	88,7	**3423**	**134**	**201**	278	**1906**	**43,7**	**0,15**	8,12
Лунин А.	58	78	70	206	68,7				222				6,48
Туинов А.	45	64	60	169	56,3				170				4,97
Фатеев С.	54	69	50	173	57,7				161				4,70
Бердников П.	56	86	80	222	74,0				240				7,01
Гнездилов А.	76	88	100	264	88,0				277				8,09
ИТОГО	**56,4**	**69,6**	**72,5**	**198,5**	**66,2**				**201**				**5,88**

Показатели уровня боеспособности (БСП)
контрольной группы рукопашного боя третьего года обучения РБ-3 и
экспериментальной группы штурмового боя третьего года обучения ШБ-3



14.3. Третий этап исследования

Определение боевого рейтинга. Без ограничений невозможно тренироваться, без повышенной физической нагрузки никогда не испытать параметры настоящего боя, без спаррингов, с различными противниками, которые имеют отличные друг от друга двигательные схемы и психологические параметры, никогда не обрести уверенности в своих силах. Состязательный бой – это способность решать обучающие задачи с полным сопротивлением противника. Единственное, что требует обязательный «до-боевой» опыт – механическая правильность выполнения технической базы. Все остальное – тактику, стратегию, постановочные задачи, оперативное мышление, физическую выносливость и т.п. – способен решать только свободный поединок.

В конце учебного года (май-месяц) поводятся рейтинговые поединки по правилам штурмового боя, утвержденные Правлением Межрегиональной Федерации штурмового рукопашного боя «ГРОМ» 11 января 2010 года. Соревновательный стандарт по штурмовому бою, представляет собой состязательную модель уличного столкновения с минимальными ограничениями по применению техники и тактики в поединке, и наиболее объективно отражает эффективность боевых действий бойца в реальных столкновениях с превосходящей агрессивной силой.

Суть состязательных боев по штурмовому бою заключается в решительных действиях по уничтожению боеспособности и подавлению противника за короткое время всеми доступными средствами. Основная идея проведения штурмовых боев состоит в выявлении победы объективной и очевидной для всех окружающих, свидетельствующей о безусловном подавлении противника (победа нокаутом, болевым приемом, удушением, отказ от боя в виду подавления атакой противника). Основными задачами проведения боев по штурмовому бою являются: приобретение бойцовского опыта, увеличение внутренней психической силы, способом психологического и тактического тренинга.

Боевой рейтинг представляет собой интегральный показатель боевого опыта бойца, приобретенного в свободных соревновательных боях. Боевой рейтинг определяется с целью способности бойца

участвовать в боях любого уровня с любым противником, в любом месте, по любым правилам и без них.

По итогам проведенных боев боевой рейтинг определяется *эффективностью боевых действий* бойца в виде *коэффициента боевых действий*, представляющего собой результат проведенных поединков в виде индивидуального числового показателя.

Эффективность атакующих действий бойца можно определить с помощью коэффициента атаки – соотношения количество результативных атак, дошедших до цели К(рат), к общему количеству всех проведенных атак за время всего поединка К(а):

$$\mathbf{К(атк) = К(рат) / К(а) \times 100\%}$$

Для более точного определения эффективности атакующих действий бойца нами было введено дифференцирование проведенных результативных атак по категориям:

Первой категории (Iкта) атак присваивается коэффициент ×1:

- акцентированные удары руками и ногами в любую зону поражения;
- сбивание ударом с ног;
- бросок на землю, при условии, что противник оказывается внизу на земле;
- сбивание или выведение из равновесия.

Второй категории (IIкта) атак присваивается коэффициент ×2:

- временная потеря сознания в результате нанесенного удара (нокдаун).

Третьей категории (IIIкта) атак присваивается коэффициент ×4:

- потеря контроля над ситуацией (боец не может защищаться от наносимых ударов);
- потеря сознания в результате нанесенного удара (нокаут);
- болевой прием, при котором противник сдался;
- удушение, при котором противник сдался.

Итоговый показатель проведенных результативных атак вычисляется как сумма атак всех категорий, помноженных на соответствующий коэффициент:

$$\mathbf{К(рат) = (Iкта \times 1) + (IIкта \times 2) + (IIIкта \times 4)}$$

Итоговый коэффициент атаки определяется по формуле:

К(атаки) = (Iкта×1) + (IIкта×2) + (IIIкта×4) / К(а) × 100%

Эффективность защитных действий бойца можно определить с помощью коэффициента защиты – соотношения количества нейтрализованных атак противника К(нап) к общему количеству атак проведенных противником за время всего поединка К(апп):

К(защ) = К(нап) / К(апп) × 100%

Для более точного определения эффективности защитных действий бойца нами было введено дифференцирование нейтрализации атак противника по категориям:

Первой категории (Iктз) защит присваивается коэффициент ×1:

- нейтрализация любых атак противника с преимуществом для защищающегося.

Второй категории (IIктз) защит присваивается коэффициент ×(-2):

- временная потеря сознания в результате нанесенного удара (нокдаун).

Третьей категории (IIIктз) защит присваивается коэффициент ×(-4):

- полная потеря контроля над ситуацией и невозможность защищаться: нокаут, удушение, болевой прием.

Итоговый показатель нейтрализации атак противника вычисляется как разница между количеством нейтрализованных атак противника первой категории и суммы количества защит второй и третьей категории, умноженных на соответствующие коэффициенты:

К(нап) = (Iктз×1) - ((IIкта×(-2)) + (IIIкта×(-4))

Итоговый коэффициент защиты определяется по формуле:

К(защ) = (Iктз×1) - ((IIкта×(-2)) + (IIIкта×(-4)) / К(апп) × 100%

Эффективность боевых действий бойца определяется коэффициентом боевых действий:

К(бод) = К(атк) + К(защ) / 2

Повышение коэффициента боевых действий определяет высокий уровень боеспособности бойца, достаточно быстро и качественно увеличивающегося при обучении штурмовым боем.

Анализ данных результатов показывает, что в экспериментальной группе первого года обучения ШБ-1 ярко выражен коэффициент атаки К(а) = 0,51 по сравнению с контрольной группой РБ-1, где К(а) = 0,40. Общее количество атак в экспериментальной группе первого года обучения на 8,3% выше, чем в контрольной группе. Причем количество атак второй и третьей категории в два раза выше, чем в контрольной группе. Все это свидетельствует об остроатакующей манере ведения боя занимающихся штурмовым боем. Однако хотелось бы отметить такой факт. В контрольной группе рукопашного боя первого года обучения количество нейтрализованных атак противника выше на 34,6%. Это подтверждает, что бойцы экспериментальной группы штурмового боя первого года обучения ШБ-1 не достаточно заботятся о собственной защите. Однако, коэффициент боевых действий группы ШБ-1 немного выше группы РБ-1, что еще раз подтверждает один из главных принципов штурмового боя – лучше действовать самому, чем реагировать на действия противника.

Установлено, что в экспериментальных группах штурмового боя второго ШБ-2 и третьего года обучения ШБ-3 значительно увеличивается результативность атакующих действий. Данный результат для контрольных групп рукопашного боя РБ-2 и РБ-3 практически остается неизменным. Это обусловлено методической направленностью развития взрывного атакующего технико-тактического инструментария штурмового боя. Интересен тот факт, что бойцы штурмового боя второго и третьего года обучения часто заканчивают поединки нокаутом или подавлением атакой. Рукопашники того же уровня подготовки, в поединках побеждают за счет технического мастерства. Это подтверждает атакующий жесткий напор штурмового боя.

Анализ результатов эффективности боевых действий по штурмовому бою контрольных и экспериментальных групп представлен в таблице 5.

Результаты эффективности боевых действий по штурмовому бою

Таблица 5.

№ п/п	Показатели	Время обучения					
		1 год обучения		2 год обучения		3 год обучения	
		РБ-1	ШБ-1	РБ-2	ШБ-2	РБ-3	ШБ-3
1	К(а) – общее количество проведенных атак	290	316	207	254	167	236
2	К(рат) - количество результативных атак	117	162	101	140	106	172
3	К(атк) - коэффициент атаки	0,40	0,51	0,49	0,55	0,63	0,73
4	К(апп) - общее кол-во атак проведенных противником	326	275	222	261	179	212
5	К(нап) - количество нейтрализ. атак противника	124	81	81	132	75	106
6	К(защ) - коэффициент защиты	0,38	0,29	0,36	0,51	0,42	0,5
7	К(бод) - коэффициент боевых действий	0,39	0,40	0,43	0,53	0,53	0,61
8	Критерий Фишера F	**2,35**		**1,45**		**1,2**	
9	Критерий Стьюдента t		**0,35**		**0,17**		**0,13**
10	Коэффициент корреляции r	**0,8**					

Проверим гипотезу Стьюдента о равенстве генеральных средних для коэффициента боевых действий по формуле (рис. 4).

$$t = \frac{(\bar{x} - \bar{y}) - M(\bar{x} - \bar{y})}{\sigma_{\bar{x}-\bar{y}}} = \frac{\bar{x} - \bar{y}}{\sqrt{\frac{\sigma_x^2}{n_1} + \frac{\sigma_y^2}{n_2}}}$$

Рис. 4. Проверка на прогрессивность

Для контрольной и экспериментальной групп первого года обучения tэ=0,35, табличное значение коэффициента для степеней свободы m=21, tт=0,26, соответственно можно сделать вывод, что на первом году обучения различий между обучающимися в обеих группах нет.

Для контрольной и экспериментальной групп второго года обучения tэ=0,17, табличное значение коэффициента для степеней свободы m=17, tт=0,26, соответственно можно сделать вывод, что на

втором году обучения есть качественные различия между обучающимися рукопашным боем и штурмовым боем.

Для контрольной и экспериментальной групп третьего года обучения tэ=0,13, табличное значение коэффициента для степеней свободы m=15, tт=0,26, соответственно можно сделать вывод, что на третьем году обучения есть качественные различия между обучающимися рукопашным боем и штурмовым боем.

Проверим гипотезу о равенстве средних, вычислив значение статистики F (критерий Фишера) (рис. 5).

$$F = \frac{\frac{1}{n_1 - 1}\left[(n_1 - 1)\hat{s}_1^2/\sigma^2\right]}{\frac{1}{n_2 - 1}\left[(n_2 - 1)\hat{s}_2^2/\sigma^2\right]} = \frac{\hat{s}_1^2}{\hat{s}_2^2}$$

Рис. 5. Проверка на равнорассеяность
(данные принадлежат одной выборке)

Для первого года обучения для рукопашного боя и штурмового боя Fэ=2,35, табличное значение коэффициента для степеней свободы m=21, Fт =2,4; для второго года обучения - Fэ=1,45, табличное значение коэффициента для степеней свободы m=17, Fт=0,8; для третьего года обучения - Fэ=1,2 табличное значение коэффициента для степеней свободы m=17, Fт=0,9, в соответствии с этим можно сделать вывод о принадлежности данных к разным выборкам генеральной совокупности.

Определим корреляционную взаимосвязь между годами обучения самообороной в экспериментальных группах, вычислив коэффициент линейной корреляции r по формуле (рис. 6).

$$r = \frac{\overline{xy} - \bar{x}\,\bar{y}}{s_x s_y}.$$

Рис. 6. Взаимосвязь между годами

В результате вычислений коэффициент r=0,8, что говорит об изменении общего коэффициента боевых действий, носящем закономерный характер в результате тренировочных занятий (табл. 6).

Обобщенные результаты эффективности боевых действий

Таблица 6.

Статистика критерия	1 год	2 год	3 год
Стьюдента t	0,35	0,17	0,13
Фишера F	2,35	1,45	1,2
Коэффициент линейной корреляции r	0,8		

Вывод. В ходе опытно-экспериментальной работы полученные результаты подтвердили рабочую гипотезу настоящего исследования. Повышение коэффициента боевых действий определяет высокий уровень боеспособности бойца, достаточно быстро и качественно увеличивающегося при обучении штурмовому бою. Таким образом, можно сделать вывод об эффективности штурмового боя для обеспечения личной безопасности от агрессивного нападения.

Данное исследование не исчерпывает всех аспектов обеспечения личной безопасности человека от преступных нападений. Дальнейшую разработку проблемы представляется возможным осуществлять в других направлениях, позволяющих создать целостную систему формирования личной стратегии безопасности.

Приложение 2

Результаты эффективности боевых действий по штурмовому бою контрольной группы рукопашного боя первого года обучения РБ-1

Таблица 2-1

Номера испытуемых	Количество результативных атак				Общее кол-во атак К (а)	Коэффициент атаки К (атк)	Количество нейтрализованных атак				Общее кол-во атак прот. К (апп)	Коэффициент защиты К(защ)	**Коэффициент боеспособности К (бсп)**
	I кта	II кта	III кта	К(рат)			I ктз	II ктз	III ктз	К(нап)			
1	3			3	9	0,33	5	2		3	16	0,19	**0,26**
2	4			4	11	0,36	4			4	15	0,27	**0,32**
3	6			6	13	0,46	6		4	2	17	0,12	**0,29**
4	5			5	12	0,42	3			3	11	0,27	**0,34**
5	8			8	12	0,67	2			2	12	0,17	**0,42**
6	5			5	13	0,38	4			4	15	0,27	**0,33**
7	4			4	9	0,44	3			3	13	0,23	**0,34**
8	4			4	10	0,40	5			5	14	0,36	**0,38**
9	8	2		10	15	0,67	4			4	12	0,33	**0,50**
10	7		4	11	16	0,69	3	2		1	11	0,09	**0,39**
11	6			6	14	0,43	5			5	12	0,42	**0,42**
12	8			8	15	0,53	4			4	14	0,29	**0,41**
13	6			6	13	0,46	3			3	10	0,30	**0,38**
14	4			4	13	0,31	5			5	12	0,42	**0,36**
15	5			5	16	0,31	3			3	9	0,33	**0,32**
16	7			7	14	0,50	5			5	10	0,50	**0,50**
17	5			5	14	0,36	4			4	9	0,44	**0,40**
18	7			7	16	0,44	3			3	10	0,30	**0,37**
19	4			4	10	0,40	7		4	3	13	0,23	**0,32**
20	9			9	14	0,64	5			5	12	0,42	**0,53**
21	7	2		9	15	0,60	6			6	15	0,40	**0,50**
22	8			8	16	0,50	4			4	13	0,31	**0,40**
ИТОГО	**130**	**4**	**4**	**138**	**290**	**0,48**	**93**	**4**	**8**	**81**	**275**	**0,29**	**0,39**
P<0,02, t=0,35, F=2,35													

Результаты эффективности боевых действий по штурмовому бою экспериментальной группы штурмового боя первого года обучения ШБ-1

Таблица 2-2

Номера испытуемых	Количество результативных атак				Общее кол-во атак К (а)	Коэффициент атаки К (атк)	Количество нейтрализованных атак				Общее кол-во атак прот. К (апп)	Коэффициент защиты К(защ)	**Коэффициент боеспособности К (бсп)**
	I кта	II кта	III кта	К(рат)			I ктз	II ктз	III ктз	К(нап)			
1	4			4	10	0,40	6			6	14	0,43	**0,41**
2	7			7	14	0,50	5			5	11	0,45	**0,48**
3	5			5	9	0,56	5			5	12	0,42	**0,49**
4	8			8	15	0,53	7			7	16	0,44	**0,49**
5	7			7	15	0,47	6	2		4	14	0,29	**0,38**
6	9		4	13	16	0,81	10			10	17	0,59	**0,70**
7	7	2		9	14	0,64	8			8	14	0,57	**0,61**
8	5			5	12	0,42	4			4	13	0,31	**0,36**
9	4			4	10	0,40	5			5	16	0,31	**0,36**
10	3			3	11	0,27	5		4	1	18	0,06	**0,16**
11	10		4	14	18	0,78	9			9	12	0,75	**0,76**
12	7			7	17	0,41	9			9	16	0,56	**0,49**
13	5			5	14	0,36	4		4	0	14	0,00	**0,18**
14	11	2		13	19	0,68	10			10	19	0,53	**0,61**
15	6			6	15	0,40	6		4	2	17	0,12	**0,26**
16	8			8	16	0,50	4			4	15	0,27	**0,38**
17	6			6	15	0,40	3	2		1	12	0,08	**0,24**
18	8	2		10	17	0,59	7			7	16	0,44	**0,51**
19	6			6	14	0,43	8			8	14	0,57	**0,50**
20	5			5	12	0,42	6			6	15	0,40	**0,41**
21	6	2		8	16	0,50	6			6	14	0,43	**0,46**
22	9			9	17	0,53	7			7	17	0,41	**0,47**
ИТОГО	**146**	**8**	**8**	**162**	**316**	**0,51**	**140**	**4**	**12**	**124**	**326**	**0,38**	**0,45**
P<0,02, t=0,35, F=2,35													

Результаты эффективности боевых действий по штурмовому бою контрольной группы рукопашного боя второго года обучения РБ-2

Таблица 2-3

Номера испытуемых	Количество результативных атак				Общее кол-во атак К (а)	Коэффициент атаки К (атк)	Количество нейтрализованных атак				Общее кол-во атак прот. К (апп)	Коэффициент защиты К(защ)	**Коэффициент боеспособности К (бсп)**
	I кта	II кта	III кта	К(рат)			I ктз	II ктз	III ктз	К(нап)			
1	4			4	10	0,40	6			6	14	0,43	**0,41**
2	3			3	9	0,33	5			5	12	0,42	**0,38**
3	5			5	12	0,42	6	2		4	13	0,31	**0,36**
4	6			6	11	0,55	5			5	12	0,42	**0,48**
5	4	2		6	10	0,60	3			3	11	0,27	**0,44**
6	5	2		7	11	0,64	6			6	14	0,43	**0,53**
7	4			4	10	0,40	5			5	14	0,36	**0,38**
8	5			5	12	0,42	6			6	15	0,40	**0,41**
9	7			7	13	0,54	5			5	13	0,38	**0,46**
10	6			6	12	0,50	4			4	12	0,33	**0,42**
11	5			5	11	0,45	4			4	11	0,36	**0,41**
12	7			7	14	0,50	4	2		2	13	0,15	**0,33**
13	7			7	12	0,58	4			4	11	0,36	**0,47**
14	5			5	11	0,45	6			6	13	0,46	**0,46**
15	4			4	10	0,40	5			5	12	0,42	**0,41**
16	6			6	13	0,46	4			4	11	0,36	**0,41**
17	7			7	12	0,58	3			3	10	0,30	**0,44**
18	7			7	14	0,50	4			4	11	0,36	**0,43**
ИТОГО	**97**	**4**	**0**	**101**	**207**	**0,49**	**85**	**4**	**0**	**81**	**222**	**0,36**	**0,43**
P<0,02, t=0,17, F=1,45													

Результаты эффективности боевых действий по штурмовому бою экспериментальной группы штурмового боя второго года обучения ШБ-2

Таблица 2-4

Номера испытуемых	Количество результативных атак				Общее кол-во атак К (а)	Коэффициент атаки К (атк)	Количество нейтрализованных атак				Общее кол-во атак прот. К (апп)	Коэффициент защиты К(защ)	**Коэффициент боеспособности К (бсп)**
	I кта	II кта	III кта	К(рат)			I ктз	II ктз	III ктз	К(нап)			
1	5			5	11	0,45	7			7	11	0,64	**0,55**
2	6			6	12	0,50	8		4	4	15	0,27	**0,38**
3	6			6	11	0,55	7	2		5	13	0,38	**0,47**
4	7		4	11	16	0,69	9			9	14	0,64	**0,67**
5	7			7	12	0,58	9			9	17	0,53	**0,56**
6	9	2		11	12	0,92	9			9	16	0,56	**0,74**
7	7	2		9	15	0,60	8			8	15	0,53	**0,57**
8	6			6	16	0,38	8		4	4	14	0,29	**0,33**
9	5			5	13	0,38	7			7	12	0,58	**0,48**
10	7	2	4	13	17	0,76	9			9	16	0,56	**0,66**
11	4			4	10	0,40	8			8	12	0,67	**0,53**
12	6			6	11	0,55	9			9	15	0,60	**0,57**
13	5		4	9	15	0,60	8			8	16	0,50	**0,55**
14	8			8	18	0,44	9			9	17	0,53	**0,49**
15	7			7	17	0,41	7		4	3	12	0,25	**0,33**
16	9	2		11	17	0,65	7			7	14	0,50	**0,57**
17	7			7	12	0,58	9			9	15	0,60	**0,59**
18	9			9	19	0,47	8			8	17	0,47	**0,47**
ИТОГО	**120**	**8**	**12**	**140**	**254**	**0,55**	**146**	**2**	**12**	**132**	**261**	**0,51**	**0,53**
P<0,02, t=0,17, F=1,45													

Результаты эффективности боевых действий по штурмовому бою контрольной группы рукопашного боя третьего года обучения РБ-3

Таблица 2-5

Номера испытуемых	Количество результативных атак				Общее кол-во атак К (а)	Коэффициент атаки К (атк)	Количество нейтрализованных атак				Общее кол-во атак прот. К (апп)	Коэффициент защиты К(зап)	**Коэффициент боеспособности К (бсп)**
	I кта	II кта	III кта	К(рат)			I ктз	II ктз	III ктз	К(нап)			
1	6			6	11	0,55	7	2	4	1	12	0,08	**0,31**
2	4	2	4	10	10	1,00	6			6	11	0,55	**0,77**
3	4			4	9	0,44	5		4	1	9	0,11	**0,28**
4	5	2		7	9	0,78	8	2		6	14	0,43	**0,60**
5	7	2		9	12	0,75	7			7	12	0,58	**0,67**
6	5		4	9	12	0,75	8			8	13	0,62	**0,68**
7	5			5	8	0,63	7			7	13	0,54	**0,58**
8	3	2		5	9	0,56	7	2		5	12	0,42	**0,49**
9	4			4	8	0,50	5			5	9	0,56	**0,53**
10	3			3	8	0,38	5	2		3	8	0,38	**0,38**
11	4		4	8	10	0,80	6			6	10	0,60	**0,70**
12	5			5	12	0,42	5			5	8	0,63	**0,52**
13	7	2	4	13	14	0,93	5			5	12	0,42	**0,67**
14	7			7	13	0,54	5	2		3	9	0,33	**0,44**
15	7			7	12	0,58	6	2		4	13	0,31	**0,45**
16	4			4	10	0,40	7		4	3	14	0,21	**0,31**
ИТОГО	**80**	**10**	**16**	**106**	**167**	**0,63**	**99**	**12**	**12**	**75**	**179**	**0,42**	**0,53**
P<0,02, t=0,13, F=1,2													

Результаты эффективности боевых действий по штурмовому бою экспериментальной группы штурмового боя третьего года обучения ШБ-3

Таблица 2-6

Номера испытуемых	Количество результативных атак				Общее кол-во атак К (а)	Коэффициент атаки К (атк)	Количество нейтрализованных атак				Общее кол-во атак прот. К (апп)	Коэффициент защиты К(защ)	**Коэффициент боеспособности К (бсп)**
	I кта	II кта	III кта	К(рат)			I ктз	II ктз	III ктз	К(нап)			
1	8	2	4	14	15	0,93	7			7	12	0,58	**0,76**
2	7			7	16	0,44	8			8	14	0,57	**0,50**
3	8	2		10	15	0,67	6			6	14	0,43	**0,55**
4	6			6	14	0,43	7		4	3	12	0,25	**0,34**
5	8			8	14	0,57	7	2		5	13	0,38	**0,48**
6	9	2		11	16	0,69	10			10	17	0,59	**0,64**
7	10			10	18	0,56	6			6	14	0,43	**0,49**
8	8	2	4	14	14	1,00	10			10	15	0,67	**0,83**
9	7			7	17	0,41	8		4	4	14	0,29	**0,35**
10	10		4	14	18	0,78	7			7	12	0,58	**0,68**
11	8	4	4	16	14	1,14	9			9	12	0,75	**0,95**
12	7		4	11	12	0,92	7	2		5	11	0,45	**0,69**
13	6	2		8	11	0,73	7			7	12	0,58	**0,66**
14	9			9	15	0,60	8	2	4	2	16	0,13	**0,36**
15	8	4		12	14	0,86	8			8	13	0,62	**0,74**
16	9	2	4	15	13	1,15	9			9	11	0,82	**0,99**
ИТОГО	**128**	**20**	**24**	**172**	**236**	**0,73**	**124**	**6**	**12**	**106**	**212**	**0,50**	**0,61**
P<0,02, t=0,13, F=1,2													

Идеи гуманизма в истории педагогики

Рожков Н.Т.
к.п.н., доцент кафедры «Русский язык и педагогика»
ФГБОУ ВПО «Государственный университет-УНПК»

Ключевые слова: развитие, воспитание, гуманизм, идентичность, человековедение

Анализ развития образования и воспитания в мировой науке и практике свидетельствует о том, что в большинстве своем ученые и педагоги-практики отдают предпочтение гуманной педагогике.

Гуманизация обучения и воспитания – это развитие и формирование учащихся с учетом их интересов, потребностей, способностей, задатков, ценностных ориентаций, создание при этом оптимальных условий жизнедеятельности. Объяснить это можно тем, что истинно человеческая мораль всегда гуманистична. Она проявляется в совестливости перед другим за свое поведение, свои мысли, свои чувства и в стыде перед самим собой за допущенные ошибки. Здесь берут свое начало чувства сострадания, милосердия, сопричастности, уважения, а, следовательно, и соответствующие действия по отношению к окружающим. У человека развивается способность в понимании другого, в оказании ему помощи и поддержки.

Гуманная педагогика – общечеловеческая ценность, имеющая начало в природе человека. Сущность ее заключается в том, что педагог должен идти к своему воспитаннику не от самого себя, а от его потребностей, интересов, мотивов, установок, идеалов, ценностных ориентаций, определяя те границы, в пределах которых возможно педагогическое воздействие. Чем глубже педагог познает внутренний мир учащегося, тем лучше последний чувствует себя в процессе познания и учения, развивая свои задатки и способности.

Педагогика гуманизма ориентируется на лучшие качества воспитанника – в этом ее главный отличительный признак. Она утверждает, что растущий человек должен сам создавать себя, творить самого себя и свою судьбу. Задача же педагога помочь ему в этом, ориентируясь на идеалы и общечеловеческие ценности, поддерживая стремления в разрешении возникающих противоречий. Истинная педагогика начинается с анализа жизнедеятельности учащегося, с содействия ему в преодолении трудностей, потому что он изначально не стремится к самостоятельности и педагог должен вести его к саморазвитию и самореализации.

Нам часто приходится слышать высказывания педагогов в адрес неуспевающих учащихся такие как: «Они не хотят учиться», «У них нет желания учиться» и т.д., хотя правильно было бы сказать: «Они не осознали значения учебно-познавательной деятельности». Это ориентировало бы педагогов не на различные проработки учащихся и жалобы их родителям, а на обращение к потребностно-эмоциональной сфере таких учащихся, оказании им помощи в осознании значимости познания и учения, а затем и в преодо-

лении отставания. Такой подход позволил бы по-новому взглянуть на процесс развития и формирования личности. Задача педагога, в этом случае, состоит в том, чтобы возбудить у учащихся потребности, интересы, ценностные ориентации, мысли, чувства, переживания и т.д., которые находятся в зачаточном, неразвитом состоянии. Учащийся должен их осознать и пережить, то есть эмоционально закрепить. Только тогда можно говорить об истинном обучении и воспитании, потому что осознание учащимся значимости познания и учения происходит не за счет каких-то потусторонних сил, а идет оно изнутри – за счет собственной активности. По существу, в этом и проявляется гуманизм педагога по отношению к учащемуся.

Гуманизм подразумевает ненасильственное развитие личности учащегося. Идея ненасилия родилась не сейчас и не вчера. Педагогика как отрасль научного знания выросла из недр философии в глубокой древности. Уже тогда гуманистический подход в воспитании нашел свое отражение в методах обучения. Например, метод сократической беседы как способ рождения истинного знания, практикуемый Сократом, предполагал полный отказ от принуждения воспитанника к определенному образу мышления и понимания. Знание должно возникнуть в результате свободного творчества – это положение было незыблемым для Сократа. Утверждение его о том, что «я знаю, что ничего не знаю», можно считать приемом, запрещающим педагогу делать попытку принуждать ученика к познанию. В свою очередь, пифагорейцы стремились из дружбы и учения устранить состязательность и соперничество, полагая, что они способствуют принуждению и насилию над личностью, негативно влияют на развитие мудрости. Осторожность, сдержанность, внушение в мягких выражениях рассматривались ими как основные приемы воспитания детей. Эти мысли созвучны с высказываниями Марка Фабия Квинтилиана – римского педагога. Он утверждал, что все дети от природы сообразительны и нуждаются в правильном воспитании. Гуманист был убежден в том, что настоящий учитель – это тот, который любит детей, является для них примером, осторожно подходит к каждому ученику, устраняя дурное влияние окружающих.

Эпоха Возрождения ознаменовала собой зарождение новых общественных отношений. На первое место ставится культ человека, пробуждается интерес к знанию. В этот период Витторино де Фельтре – итальянский педагог закладывает основы гуманной педагогики. Он организовал школу «Дом радости», в которой создал необходимые условия для обучения и воспитания детей. Большое внимание уделял их физическому воспитанию. Стремился развивать у них любознательность и интерес к знаниям.

Принципы гуманной педагогики нашли свое отражение в творчестве французского писателя-гуманиста Ф. Рабле. В романе «Гаргантюа и Пантагрюэль» он говорил о соблюдении режима для ребенка, многосторонности образования, развитии мышления учащихся, их творчества и активности. Он считал, что усвоение знаний должно носить сознательный характер путем бесед с применением наглядных пособий. Эти взгляды разделял и другой французский мыслитель М. Монтень. В своем произведении «Опыты», про-

возглашая принципы гуманной педагогики, он решительно выступил против схоластов, которые заставляли учеников зубрить, брать на веру без анализа и критического осмысления чужие суждения. М. Монтень требовал от преподавателей, чтобы они объясняли сотни раз явление со всех сторон, не навязывая своего мнения. Ученик должен сам делать выводы, сопоставляя различные мнения, утверждал он. Такой подход к обучению ранее никто еще не практиковал.

Идеи М.Монтеня оказали сильное влияние на творчество Я.А. Коменского, Д. Локка, Ж.Ж. Руссо и других мыслителей прошлого. В своем главном труде «Великая дидактика» Я.А. Коменский освещает почти все проблемы обучения и воспитания детей. Его идеи о природосообразности, народности воспитания проникнуты духом патриотизма, гуманизма и демократизма. Согласно Я.А. Коменскому, «тот порядок, который мы желаем сделать универсальной идеей для искусства – всему учить и всему учиться, - должен быть заимствован и может быть заимствован не из чего иного, как только из указаний природы…»[1]. Природосообразность он представлял как соответствие воспитания природе и тем закономерностям, которые существуют в ней независимо от нас. В природе все протекает естественным путем, поэтому воспитание ребенка как частицы природы так же должно проводиться естественным путем. Природосообразность обучения для Я.А. Коменского означало соответствие как природе вообще, так и природе ребенка.

Педагогическая мысль эпохи Возрождения выдвинула положение об особенностях психофизиологического развития ребенка, обосновавшее необходимость гуманного отношения к нему, что наиболее ярко проявилось в деятельности английского философа и педагога Д. Локка. Для него гуманное отношение к ребенку стало принципом, определяющим выбор педагогических средств в воспитании. Он решительно отверг догматизм в обучении, подавлении личности воспитанника. В трактате «Мысли о воспитании» Д. Локк рассматривает процесс развития и формирования человека как единство физического, психического и умственного совершенствования. Как педагог и психолог он отмечал, что дети ненавидят праздное время препровождение, им присуще естественное стремление к свободе, разнообразной деятельности, в условиях которой раскрываются их природные характеры, наклонности и способности. Только опираясь на естественные склонности детей, ничего им не навязывая и не превращая занятия в бремя, педагог может успешно руководить их обучением. Говоря о развитии способностей человека, Д. Локк подчеркивал, что «у людей существует: и это видно большое разнообразие умов и природные конструкции людей создают в этом отношении такие различия между ними, что искусство и усердие никогда не бывает в состоянии эти различия преодолеть; по-видимому, в самой природе одних людей не хватает той основы, на которой они могли бы достичь того, чего легко достигают другие» [2]. Он был убежден в том, что среди людей одинакового воспитания существует большое неравенство способностей. Тем самым Д. Локк указывал на необходимость изучения индивидуальных особенностей учащихся, без чего деятельность педагога невозможна.

Неоценимый вклад в развитие идей и принципов гуманной педагогики внес французский просветитель Ж.Ж. Руссо. Он провозгласил природную доброту человека, сообразно с которой предлагал осуществлять воспитание. Великий гуманист выступал за превращение воспитания в активный, исполненный оптимизма процесс, когда ребенок живет в радости, самостоятельно осязая, слушая, наблюдая мир, духовно обогащаясь, удовлетворяя жажду познания. Естественное воспитание должно быть живительным процессом, в котором учитываются склонности и потребности ребенка, а внутренней мотивацией этого процесса становится стремление ребенка к самосовершенствованию. Отвергая всякое насилие в воспитании ребенка, Ж.Ж. Руссо полагал, что единственно эффективным методом обучения является собственное желание ребенка обучаться. Он, в частности, писал: «Каждый человек при своем рождении имеет характер, наклонности и талант, ему свойственный. Чтобы изменить их надо изменить темперамент, от которого они зависят. Слышали ли вы когда-нибудь, чтобы вспыльчивый человек сделался флегматиком или чтобы методический и холодный ум приобрел воображение! По-моему, так же легко сделать блондина из брюнета или умного человека из глупца. Отсюда следует, что прежде чем человека воспитывать, надо знать к чему он способен» [3]. По существу, взгляды Ж.Ж. Руссо и Д. Локка были очень близки.

Говоря о гуманизме, нельзя обойти стороной творчество выдающегося русского педагога К.Д. Ушинского. Свою «Педагогическую антропологию» он начинает с определения места человека в природе. Человек, как и всякий живой организм, развивается, являясь частью природы, поэтому необходимо объяснить причины его развития. Он впервые понял, что требуется всестороннее изучение человека для его образования и воспитания. В истории педагогической мысли впервые была поставлена фундаментальная проблема необходимости изучения, раскрытия и понимания природы человека во всех ее сложных аспектах. Он был убежден в том, что сущность педагогики, состоит в изучении человеческой природы в ее физическом, духовном и душевном развитии, понимание этой природы и использование ее для целенаправленного воспитания и развития человека. При этом, К.Д. Ушинский, обращаясь к педагогам говорил: «Воспитатель должен стремиться узнать человека, каков он есть в действительности, со всеми его слабостями и во всем его величии, со всеми его будничными, мелкими нуждами и со всеми его великими духовными требованиями. Воспитатель должен знать человека в семействе, в обществе, среди народа, среди человечества и наедине со своей совестью; во всех возрастах, во всех классах, во всех положениях, в радости и горе, в величии и унижении, в избытке сил и в болезни, среди неограниченных надежд и на одре смерти… Тогда только он будет в состоянии почерпать в самой природе человека средства воспитательного влияния – а средства эти громадны!» [4]. Ставя такую задачу перед педагогикой, он понимал всю сложность и трудность ее решения. Поэтому рассматривал связь педагогики с другими науками, такими как психология, физиология, логика, подчеркивая особую роль психологии.

Последующее развитие идей гуманной педагогики ярко представлено в трудах В.А. Сухомлинского. Как педагог-гуманист, он считал, что педагогическая теория должна быть проникнута психологией. Нельзя быть гуманным, не зная души ребенка, его духовного мира. Гуманность в его представлении – это, прежде всего, человечность, доброта, справедливость. Добрые чувства, эмоциональная культура – это средоточие человечности, если они не воспитаны в детстве, их никогда не воспитаешь, утверждал педагог. Помимо двух проблем: обучение-воспитание, обучение-развитие, В.А. Сухомлинский поднимает еще одну – научить учащегося учиться. Он обнаружил, что лучшим способом учить и развивать ребенка, является возбуждение страсти к учению постоянными успехами. Исходя из этого, В.А. Сухомлинский писал: «Умственный труд детей отличается от умственного труда взрослого человека. Для ребенка конечная цель овладения знаниями не может быть главным стимулом его умственных усилий, как у взрослого. Источник желания учиться – в самом характере детского умственного труда, в эмоциональной окраске мысли, в интеллектуальных переживаниях. Если этот источник иссякает, никакими приемами не заставишь ребенка сидеть за книгой» [5]. По его мнению, профессии врача и педагога самые гуманные в мире. До последней минуты борется врач за жизнь человека, никогда он не даст почувствовать больному, что его состояние плохое, даже безнадежное. Это азбучная истина врачебной этики. «Мы, учителя, - говорил В.А. Сухомлинский, - должны развивать, углублять в своих коллективах нашу педагогическую этику, утверждать гуманное начало в воспитании как важнейшую черту педагогической культуры каждого учителя» [6].

Идеи гуманизма получили развитие в современных педагогических и психологических концепциях. Вследствие этого, к личности воспитателя предъявляются определенные требования по выработки у них особых черт профессиональной гибкости, терпимости, осмотрительности, взвешенности, владении своими эмоциями, способности к диалогу, позволяющих легко снимать внутреннее напряжение, вызванное конфликтами, стрессами, переживаниями и т.д. Эти идеи разрабатываются как отечественными педагогами и психологами, так и зарубежными. В частности, неогуманистические идеи в западной педагогике основаны на взглядах американского психолога А. Маслоу. В гуманистической теории личности он говорит об изначально заданной сущности человека, заложенной в нем от момента рождения как бы в «свернутом» виде. Человек, так или иначе, подвластен ей и поэтому не может обладать полной свободой воли. Выступив с идеей первичности личности по отношению к обществу, А. Маслоу считал главным предназначением человека «открытие своей идентичности, своего подлинного «Я» [7]. Он сформулировал ряд важных положений процесса обучения неогуманистического направления. «Полное, здоровое, нормальное и желательное развитие состоит в актуализации человеческой природы в реализации ее потенциальных возможностей и в развитии ее до уровня зрелости по тем путям, которые диктует эта скрытая, слабо различимая основная природа. Ее актуализация должна обеспечиваться скорее ростом изнутри, а не формированием извне»

[8]. Поскольку общество, социокультурные условия, по А. Маслоу, определяют лишь до какой отметки на шкале своих изначальных потребностей, включая самоактуализацию, сможет подняться личность, под этим углом зрения следует, и рассматривать образование. Оно должно быть гуманистическим в смысле наиболее полного и адекватного соответствия подлинной природы человека. Главная задача педагога, по его мнению, состоит в том, чтобы «помочь человеку обнаружить то, что в нем уже заложено, а не обучать его, «отливая» в определенную форму, придуманную кем-то заранее» [9].

Важным является то, что идеи А. Маслоу нашли широкую поддержку западных педагогов педоцентристского направления. Они призывают к созданию в школах условий для самопознания и поддержки уникального развития каждого учащегося в соответствии с унаследованной им природой. В неопедоцентристском понимании гуманистическая школа должна предоставить учащимся как можно больше эмоционального раскрепощения и свободы выбора познавательной деятельности в образовательных структурах.

Теоретики гуманистической школы учитывают сложности духовного мира человека, «многофакторность» его мотивационной сферы. Они выступают против структурно очерченного, систематического обучения, предполагающего регулярный контроль знаний, поскольку считают, что это сковывает инициативу, как учащегося, так и учителя, которому необходима свобода поиска нестандартного подхода в решении задачи. Центр тяжести образовательного процесса переносится ими в иную плоскость: дать в школе простор широкому спектру учебных курсов, вести занятия в неформальной обстановке с большим объемом ничем не ограничиваемого самостоятельного поиска. Например, американский педагог Р. Барт говорит о том, что «хорошее образование уходит своими истоками в индивидуальное понимание учителем того, как дети учатся наилучшим образом. Хорошее образование неизбежно варьирует от «класса к классу и от учителя к учителю» [10].

Один из ведущих теоретиков гуманистического образования К. Паттерсон утверждает, что «значение знания заключено в ученике, а не в содержании учебного предмета, и учащийся открывает для себя это значение, а уже затем соотносит его с содержанием». Такого же мнения придерживается и К. Роджерс, который выдвинул концепцию «свободы учения», содержание учебного предмета воспринимается каждым учеником сквозь призму, непосредственного отношения к его собственным заботам, интересам и целям» [11]. Однако Т. Грин пишет о том, что «гуманистическое образование удовлетворит идеологические запросы педагогов, но меджеральное направление будет по-прежнему отражать реальность. Совокупные ценности последнего будут доминировать в деятельности педагогов. Таким образом, идеология профессии, вероятно, будет иметь гуманистическую направленность, в то время как оперативные установки – ориентироваться на социальную полезность» [12].

Сторонники гуманистического направления в своих доводах опираются на такие ценности, как взаимозависимость, сотрудничество, равенство,

доброжелательность и отвергают состязательность, конкуренцию, иерархию и контроль над другими людьми. Видят роль учителя как источника познания, диагноста, наставника и помощника в учебно-познавательной деятельности. Направляют познавательную деятельность на индивидуальные нужды учащихся, развивая их самостоятельность с опорой на собственные силы и ответственность за свой собственный выбор. Например, в концепции Х. Джинотта акцент переносится на психотерапевтическую технику вербального общения, понимание «чувств других». Обосновывается мысль о том, что преподавание, как профессиональная деятельность несовместима с язвительностью, саркатическим тоном и т.д., что резко подрывает у учащихся уверенность в себе и самоуважение. А, умение педагога пользоваться психотерапевтическими средствами в преподавании повышает его личную значимость в жизни учеников, содействует их устойчивой идентификации с ним, и тем самым служит важным фактором внутренней мотивации к учению. Благодаря такой гуманизации преподавательской деятельности возникает продуктивный механизм педагогического общения с учащимися, а это снимает многие проблемы, в частности такую «вечную» проблему в педагогике, как нежелание учиться, особенно в старших классах.

По мере того, как мы ближе знакомимся с идеями гуманизма, все больше убеждаемся в их жизнеспособности, так как будущее настоятельно требует, чтобы образовательные процессы были обращены в первую очередь на внутренний мир учащегося, проявляющийся в ценностных ориентациях, самооценках, потребностях, переживаниях, интересах, установках и т.д. Было бы большой ошибкой думать, что в сфере образования можно обойтись без изучения внутреннего мира личности, познания закономерностей ее развития и формирования. Поэтому в настоящее время усилия большинства педагогов-новаторов направлены на решение данной проблемы.

Ярким примером развития идей гуманной педагогики является педагогическая деятельность Н.М. Таланчука. Он разработал системно-синергети ческую концепцию педагогики и учебно-воспитательного процесса, включающей в себя системный подход к формированию личности и системно-функциональный подход к воспитательной деятельности педагога. Ученый дает обоснование новых представлений о сущности воспитания, его цели, задачах, критериях воспитанности личности, содержании и методах педагогической деятельности и т.д. В своей работе «Введение в неопедагогику» Н.М. Таланчук пишет: «Новая педагогика отказывается от противоестественной, не согласующейся с генезисом социальной жизни, социоцентрической стратегией и соответствующей ей манипулятивной тактики воспитания. Она исходит из того, что высшей целью общественного развития является человек (гомо сапиенс), он должен быть в соответствии с логикой социального генезиса в центре этого развития, и для его блага должна существовать социальная система, а в школе, в которой воспитывается подрастающая личность, центром воспитательной системы должен быть ребенок, и процесс его воспитания должен строиться не как манипулирование его сознанием и поведением, а как человековедение, согласуясь с логикой социальной генеалогии и ге-

неалогии личности» [13].

Отвечая на вопрос: почему прежняя воспитательная система была неэффективной, автор говорит: «В ней ученик никогда не был главным. Кроме того, будучи технократической, эта система не имела основополагающего элемента – человековедческого. Ученик не овладевал главными знаниями и умениями, касающимися его самого, как человека, как личности, как самоуправляющейся системы, а потому не становился социально дееспособным» [14].

Таким образом, понимание насущности именно гуманистического образования выходит на передний план. Гуманизм в обучении и воспитании – не абстрактные понятия, а реальность, поскольку учение есть не что иное, как глубоко человеческий, личностный процесс, затрагивающий внутреннюю культуру человека. Реализация идей и принципов гуманной педагогики – это сознательная попытка осуществить на практике все лучшее, что мы знаем о закономерностях становления культуры человека. В то же время, следует помнить, что характер человека формируется характером, ум – умом, а культура – культурой. Поэтому к педагогу в настоящее время предъявляются повышенные требования, связанные с овладением им человековедческой культурой.

Литература:

1. Лордкипанидзе, Д.О. Ян Амос Коменский. М.: Педагогика, 1970. – с. 440.

2. Локк, Д. Сочинения в трех томах: т.2 /Пер. с англ.; Ред. кол.: М.Б.Митин/. – М.: Мысль, 1985. – с.148 – 150.

3. Асмус, В.Ф. Историко-философские этюды. Изд. Мысль, 1986. - с.27.

4. Ушинский, К.Д. Собрание сочинений в 6т., т.5. - М.:Педагогика, 1990. - с.22.

5. Сухомлинский, В.А. Сердце отдаю детям. Киев, Рядянська школа, 1969, с.57.

6. Сухомлинский, В.А. Разговор с молодым директором. Народное образование, 1965-1966, с.11.

7. Maslow, A. Some enducational implikations of the humanistic psychology //Harvard Enducational Review. 1968 V, 38, №4 p. 688.

8. Maslow, A. Motivation and personality N. Y., 1970. P.340.

9. Maslow, A. Some enducational implikations of the humanistic psychology //Harvard Enducational Review. 1968 V, 38, №4 Op. cit.

10. Barth, R. Run school run. Cambridge (Mass), 1980. P.22.

11. Rogers, C.R. Freedom tolearn: A view of what enducation mightbe-

come. Columbus (Ohio), 1969. P.158.

12. Creen, T.F. Schoolsand communitionalies: Harvard Educational Review. 1969. Vol. 39 №2 p.23 6-237.

13. Таланчук, Н.М. Введение в неопедагогику. М.: Издат. фирма Логос, 1999. – с.24.

14.Таланчук, Н.М. 100 новых идей в педагогике, связанных с открытием фундаментальных законов системного синергетизма. Эвристический тезаурус. – Казань: Ин-т сред. спец. образов. РАО, 1993. – с.9.