

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

|  |  |  |
| --- | --- | --- |
|  | |  |
|  | |  |
|  | |  |
|  |  | |

КОНСПЕКТ ЛЕКЦИЙ

«МЕТОДОЛОГИЯ И ПРАКТИКА ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ХОЗЯЙСТВУЮЩИХ СУБЪЕКТОВ»

**Ростов-на-Дону**

**2020г**

Тема 1. ПРОЦЕСС ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Экономическая безопасность предприятия (ЭБП) — это состояние наиболее эффективного использования ресурсов для предотвращения угроз и обеспечения стабильного функционирования предприятия.

Для того чтобы достичь наиболее высокого уровня экономической безопасности, предприятие должно следить за обеспечением максимальной безопасности основных функциональных составляющих системы ЭБП.

Функциональные составляющие ЭБП — это совокупность основных направлений его экономической безопасности, существенно отличающихся друг от друга по своему содержанию.

Выделяют следующие функциональные составляющие ЭБП:

· финансовую;

· интеллектуальную и кадровую;

· технико-технологическую;

· политико-правовую;

· экологическую;

· информационную;

· силовую.

**Лекция 2: Понятие корпоративных ресурсов и принципы обеспечения экономической безопасности.**

1. **Понятие корпоративных ресурсов**

Для обеспечения своей экономической безопасности предприятие использует совокупность корпоративных ресурсов. В современных условиях экономики на предприятии вне зависимости от социально-политической системы и от уровня производственной иерархии можно выделить следующие группы корпоративных ресурсов

*Корпоративные ресурсы* — факторы бизнеса, используемые владельцами и менеджерами предприятия для выполнения целей бизнеса.

Среди них выделяют:

**а) ресурс капитала** является главным ресурсом предприятия, который позволяет приобретать и поддерживать остальные корпоративные ресурсы, изначально отсутствующие у данного предприятия.

Ресурс капитала делится 2 группы: основной капитал и оборотный капита.

Основной капитал – это часть производственного капитала, который многократно принимает участие в производстве товаров, переносит свою стоимость на готовый продукт в течение ряда лет. К нему относятся здания, сооружения, оборудование, машины, инструменты и т.д.

Оборотный капитал – это часть производственного капитала, стоимость которого полностью переносится на производственный товар, возвращается в денежной форме после его реализации в течение 12 месяцев.

Оборотный капитал формируется из:

- денежных средств,

- легкореализуемых ценных бумаг,

- дебиторской задолженности,

- материально-производственных запасов,

- готовой продукции,

- незавершенного производства,

- расходов будущих периодов.

В практике российских предприятий используют три метода оценки ресурса капитала: доходный, рыночный и затратный.

Доходный метод базируется на оценке будущих доходов от производства.

Рыночный подход базируется на оценке предприятия посредствам анализа продаж аналогичных или сопоставимых объектов, т.е. методом сравнения.

Затратный подход предусматривает, что стоимость оцениваемого предприятия может быть определена на базе анализа затрат, необходимых для воспроизводства или замены собственности за вычетом морального и физического износа.

Все три подхода не только не исключают друг друга, но и взаимосвязаны

**б) ресурс персонала** является основным, проводящим и связующим звеном, соединяющим воедино все факторы предпринимательской деятельности, обеспечивающим проведение в жизнь идеи предприятия, а также достижение целей предприятия.

Персонал является важным стратегическим ресурсом предприятия, имеющим огромные резервы для повышения результативности деятельности, *поэтому он должен рассматриваться не просто как фактор производства, а как капитал, от которого практически полностью зависит будущее благополучие, а иногда и выживание предприятия.*

*Кадры играют ключевую роль в обеспечении корректного функционирования компании - они приводят в движение и организуют взаимодействие всех остальных ресурсов, формируют стратегию предприятия.*

*Как показывает практика ведущих в своих областях производственных компаний, между качеством человеческого капитала и эффективностью использования материально-технических ресурсов существует прямая зависимость, и, как следствие, у предприятия появляется дополнительный стимул для инвестирования в человеческий капитал.*

Персонал можно разделить на 2 категории: рабочие (основной персонал, младший обслуживающий персонал и вспомогательный) и служащие (руководители и специалисты). Российские предприятия используют такие методы оценки персонала, как количественные и качественные показатели.

Первая группа показателей (Количественные) включает в себя:

− списочная численность персонала на определенную дату;

− явочная численность персонала;

- среднесписочная численность персонала за определенный период;

− темпы роста численности работников за определенный период;

− удельный вес работников отдельных подразделений в общей численности работников предприятия;

− фонд ресурсов труда в чел./дн. или чел./ч.;

− индекс численности рабочей силы;

− показатель общего оборота рабочей силы (*показатель интенсивности движения, текучести кадров);*

− показатель по приему персонала и т.д.

Вторая группа (качественные):

- производительность труда,

- трудоемкость труда ,

- фондовооруженность *(показатель, который помогает определить степень обеспеченности всех сотрудников основными средствами предприятия),*

- удельный вес работников имеющих высшее профессиональное образование в общей - численности работников предприятия,

- средний стаж работы по специализации руководителей и специалистов предприятия.

**в) ресурс информации и технологии.** Информация, касающаяся всех сторон деятельности предприятия, является в настоящее время наиболее ценным и дорогостоящим из ресурсов предприятия. Именно информация *об изменении политической, социальной, экономической и экологической ситуации, рынков предприятия, научно-техническая и технологическая информация, новое в методах организации и управления бизнесом* позволяют предприятию адекватно реагировать на любые изменения внешней среды бизнеса, эффективно планировать и осуществлять свою хозяйственную деятельность;

Методы оценки использования ресурса информации и технологий базируются на:

− оценке наличия и направлений применения технических и программных средств, средств телекоммуникаций;

− оценке препятствий на пути их внедрения и распространения;

− оценке объема и структуры затрат на информационные технологии;

- оценку численности и состава пользователей применительно к предприятиям и организациям различных отраслей экономики.

**г) ресурс техники и оборудования.** *На основе имеющихся финансовых, информационно-технологических и кадровых возможностях предприятие приобретает необходимое и доступное оборудование.*

Уровень технической оснащенности предприятия определяет эффективность изготовления продукции основным производством, обуславливает возможность бесперебойного ее выпуска.

*Техническая подготовка производства может предусматривать техническое перевооружение, реконструкцию, расширение отдельных производственных участков, а так же модернизацию оборудования.*

**д) ресурс прав**. *С развитием цивилизации, истощением природных ресурсов и повышением ценности для бизнеса нематериальных активов резко выросла роль данного ресурса.*

Данный ресурс включает в себя права на использование патентов, лицензии, квоты на использование природных ресурсов права на пользование землей *(причем в настоящее время крайне повысилась ценность городских территорий, предназначенных не для земледелия, а для административной застройки).*

*Все рассмотренные ресурсы крайне необходимы для предприятия, но только при условии их взаимодействия друг с другом. Каждый из выделенных корпоративных ресурсов не может раскрыться полностью вне связи с другими ресурсами, и невозможно, к примеру, своевременно отреагировать на произошедшие изменения, не располагая соответствующими ресурсами всех видов.*

Взаимодействие всех составляющих системы корпоративных ресурсов предприятия образует новые свойства, которыми каждый отдельный ресурс не обладает. Это означает, что, имея в своем распоряжении совокупность корпоративных ресурсов, предприятие способно не только в той или иной степени удовлетворить запросы потребителей, но и способно, как минимум, обеспечить свою устойчивость.

1. **Принципы обеспечения экономической безопасности предприятия**

**Обеспечение экономической безопасности предприятия** — это процесс реализации функциональных составляющих экономической безопасности для предотвращения возможных ущербов и достижения максимального уровня экономической безопасности в настоящее время и в будущем.

Обеспечение экономической безопасности должно осуществляться на основе следующих **принципов**:

1. Комплексность – защита разных сфер деятельности предприятия от всевозможных угроз и обеспечение нормального функционирования предприятия.

*Этот принцип предполагает создание такой системы безопасности, которая обеспечила бы защищенность предприятия, ее имущества, персонала, информации, различных сфер деятельности от всевозможных опасностей и угроз, форс-мажорных обстоятельств, т.е. система безопасности, ее составные элементы, силы, средства должны быть достаточными, чтобы обеспечить экономическую безопасность всего предприятия, а не отдельных его элементов.*

2. Своевременность – постановка задач комплексной безопасности на ранних стадиях разработки системы безопасности на основе анализа и прогнозирования обстановки, угроз.

*Система экономической безопасности должна быть построена таким образом, чтобы она могла на ранних стадиях выявлять различные деструктивные факторы, принимать меры по предотвращению их вредоносного воздействия и нанесения ущерба корпорации. Реализация данного принципа экономически значительно выгоднее, чем устранение нанесенного ущерба.*

3. Непрерывность – Система экономической безопасности предприятия (СЭБП) должна непрерывно гарантировать защиту интересов предприятия в условиях постоянно изменяющихся обстоятельств.

*СЭБП должна действовать постоянно, защищая интересы предприятия в условиях риска и противодействия злоумышленникам.*

4. Плановость - *Деятельность по обеспечению****экономической безопасности предприятия****организуется на основе единого замысла, отраженного в конкретных планах предприятия по отдельным направлениям обеспечения его безопасности.*

5. Законность – разработка системы безопасности на основе федерального законодательства в области предпринимательской деятельности, информатизации и защиты информации, частной охранной деятельности, а также других нормативных актов по безопасности.

6. Экономическая целесообразность и сопоставимость возможного ущерба и затрат на обеспечение безопасности (эффективность – стоимость)

*То есть стоимость затрат на ее обеспечение была оптимальной и не превышающей тот уровень, при котором теряется экономический смысл их применения.*

7. *С*очетание гласности и конфиденциальности. *Основные меры****системы экономической безопасности предприятия****должна быть известны всем сотрудникам предприятия. При этом ряд способов, сил, средств, методов обеспечения****экономической безопасности предприятия****должен быть засекречен и известен очень узкому кругу специалистов.*

8. Взаимодействие и координация – осуществление мер обеспечения безопасности на основе чёткого взаимодействия заинтересованных подразделений и служб.

*Для обеспечения****экономической безопасности предприятия****нужно, чтобы усилия всех обеспечивающих её лиц, подразделений, служб были скоординированы как внутри предприятия, так и с внешними организациями (правоохранительными органами, местными либо районными службами безопасности, органами власти и т.д.)*

9. Совершенствование – появление новых технических средств защиты с учетом изменений в методах и средствах разведки и промышленного шпионажа, нормативно-технических требований, накопленного отечественного и зарубежного опыта.

10. Централизация управления – самостоятельное функционирование системы безопасности по единым принципам. Особое внимание необходимо уделять принципу комплексности. Под комплексной безопасностью следует понимать полный охват объектов защиты все совокупностью форм противодействия и защиты (охрана, режим, кадры, документы и т.д.) на основе правовых организационных и инженерно- технических мероприятий.

**Лекция 4. Внешние и внутренние угрозы экономической**

**безопасности предприятия**

Все угрозы, факторы риска развития предприя­тия могут быть сгруппированы по различным классификацион­ным признакам. Наиболее распространено выделение угроз в зависимости от сферы их воз­никновения. По этому признаку различают внутренние и внеш­ние угрозы.

Внешние угрозы возни­кают за пределами предприятия. Они не связаны с его производ­ственной деятельностью и иными хозяйственными операциями. К угрозам данного типа относится такое измене­ние окружающей среды, которое может нанести ущерб предприятию.

К **внешним факторам** относят элементы макро- и микросре­ды.

*Микросреда* представлена силами, имеющими непосред­ственное отношение к самому предприятию - т. е. его контраген­тами: поставщиками, посредниками, клиентами, конкурентами и контактными аудиториями. Под «контрактными аудиторами» по­нимают организации и учреждения, а также социальные группы, которые не являются прямыми партнерами по бизнесу, однако представляют интерес с точки зрения обеспечения предпринима­тельского успеха предприятия и способны оказывать влияние на реализацию поставленных им целей. На микросреду предприя­тие может оказывать влияние посредством заключения контрак­тов и неформальных договорённостей.

Негативное воздействие со стороны микро­среды на экономическую безопасность предприятия может про­являться в следующих комбинациях:

* противоправные действия конкурентов (промышленная разведка, использование схем недружественных поглощений, в том числе посредством скупки задолженности и вхождения в ка­питал предприятия);
* переманивание клиентов со стороны конкурентов ввиду более привлекательного предложения по качеству, цене и иным условиям реализации продукции;
* сговор поставщиков между собой или сговор единствен­ного поставщика и конкурентов, существенно ограничивающий доступ к сырью и комплектующим;
* диктовка невыгодных условий со стороны крупного по­средника-дистрибьютора ввиду его доминирующего положения;
* невозможность реструктуризации кредитной задолжен­ности в кредитном учреждении, где ранее был взят кредит, и по­следующее его обращение в суд о признании предприятия- должника банкротом;
* недобросовестное поведение подрядчика, при котором срываются сроки, и страдает качество работы и другие случаи.

*Макросреда* представлена силами более широкого, институ­ционального характера, которые в том числе оказывают влияние и на микросреду. Это демографические, макроэкономические, природно-климатические, научно-технические, политические, культурные и иные факторы, формирующие условия функциони­рования предприятия. На макросреду предприятие не может ока­зывать влияния, либо его влияние ограниченно.

Один из примеров влияния макросреды на предприятие – это высокая динамика развития мировой или национальной эко­номики, значительное уменьшение вре­менного интервала между сменами технологий и со­кращение жизненного цикла продукта. Сетевая взаимозависи­мость предприятий и их гонка за инновациями предопределили молниеносный рывок технологий и внедрение инновации на рынок за кратчайшее время. В результате предприятие вынуждено принимать для себя решение: либо инвестировать в техноло­гическое лидерство, что сопряжено с высокими рисками, либо постоянно мониторить научно-технологическую среду и осу­ществлять низкозатратное копирование передовых решений, что ставит его в роли догоняющего.

К другим внешним факторам, которые оказывают сильное воздействие на развитие бизнеса, можно отнести: состояние ин­вестиционного законодательства, наличие местных сырьевых и энергетических ресурсов, развитие транспортных и других ком­муникаций, наполняемость рынка, состояние конкурентов, нали­чие свободных трудовых ресурсов, уровень их профессиональной подготовленности, уровень социальной и политической напря­женности, уровень жизни населения, его платежеспособность, криминализация хозяйственной жизни (коррумпированность чи­новников, рэкет, экономическая преступность) и многие другие.

К внешним опасностям и угрозам в макросреде для эконо­мической безопасности предприятия можно причислить:

* демографические негативные процессы (старение населения, естественная убыль населения, миграционный отток населения);
* неблагоприятное изменение политической ситуации;
* макроэкономические потрясения (финансовый кризис, падение производства, спад покупательной способности населе­ния, девальвация национальной валюты, гиперинфляция и т.д.);
* изменение законодательства, влияющего на условия хо­зяйственной деятельности (налогового, отношений собственно­сти, договорного и др.);
* чрезвычайные ситуации природного и технического ха­рактера и другие.

**Внутренние факторы** связаны с хозяйственной деятельно­стью предприятия. Они обусловлены теми процессами, которые возникают в ходе производства и реализации продукции и могут оказать свое влияние на результаты бизнеса. К основным угрозам можно отнести:

* ошибки и просчёты в планировании и принятии управ­ленческих решений, связанные с некомпетентностью собствен­ников и управленцев;
* неправильную организацию труда и демотивирующая ра­бота с персоналом, что может привести к оттоку квалифициро­ванных кадров;
* непродуманную финансовую политику предприятия, ре­зультатом которой может стать высокая финансовая зависимость от кредиторов, недостаточная финансовая устойчивость и лик­видность предприятия;
* противоправные действия сотрудников (разглашение коммерческой тайны, причинение материального ущерба, пере­ориентация клиентов к конкурентам);
* недостаточную патентную защищенность, которая может привести к копированию и тиражированию инноваций предприятия;
* нарушение режима эксплуатации машин и производ­ственного оборудования, что может привести к ускорению их фи­зического износа и к выходу из строя;
* чрезвычайные ситуации в процессе хозяйственной дея­тельности (аварии, пожары, взрывы; перебои в энерго-, водо-, теплоснабжении).

Внутреннюю среду предприятие должно полностью контро­лировать и не допускать возникновения угроз экономической безопасности, поскольку все эти риски подвластны менеджменту. Ключевой фактор успеха в этом - правильная рациональная ор­ганизация деятельности, принятие экономически обоснованных решений в соответствии с принятой стратегией развития.

Основная деятельность по обеспечению экономической без­опасности заключается в том, чтобы минимизировать влияние внешних и внутренних угроз финансовой, материальной, инфор­мационной и кадровой природы. Однако, как показывает практи­ка, часто руководители компаний более серьезно относятся к внешней безопасности бизнеса.

Внешние и внутренние угрозы в деятельности предприятия снижают эффективность и надежность функционирования пред­приятия, а в отдельных случаях приводят к прекращению их дея­тельности.

Основные угрозы экономической безопасности приведены в таблице 1.

Таблица 1 - Основные угрозы экономической безопасности предприятия

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | Угроза | Качественная характеристика угрозы | Характер угрозы | Источник опасности |
| 1 | Противозаконные действия отдельных лиц и организаций адм ин истр ати в ного аппарата, в том числе и налоговых служб | Подобные действия снижают эффек­тивность и надежность функциони­рования предприятий, а в отдельных случаях приводит к прекращению их деятельности из-за опасности эконо­мического, социального, правового, организационного, информационного и технического характера. | Правовой,  финансовый | Внешний |
| 2 | Негативное воздей­ствие на производ­ственные процессы предприятия отдель­ных лиц и организа­ций, в том числе за счет ошибок сотруд­ников предприятия | Подобные воздействия могут быть в виде осознанных или неосознанных действий людей, организаций, в том числе органов государственной вла­сти, международных организаций или предприятий-конкурентов, а также стечения объективных обстоятельств: состояние финансовой конъюнктуры на рынках данного предприятия, научные открытия и технологические разработки, форс-мажорные обстоя­тельства и др. | Технологи­ческие, финансовые, кадровые | Внешний,  внутренний |
| 3 | Недобросовестная конкуренция и про­мышленный шпионаж с целью дискредита­ции конкурентов и производимой пред­приятием продукции | Подобные противоправные посягатель­ства со стороны конкурентов и несостоя­тельных партнеров (промышленный шпи­онаж. посягательства на коммерческую тайну и интеллектуальную собственность и другие действия) снижают надежность функционирования предприятий. | Правовой,  финансовый | Внешний |
| 4 | Монополизация рынков путем сговора о ценах, получения ин­формации о составе, финансовом и эконо­мическом состоянии и производственной дея­тельности конкуриру­ющих структур | Монополизация рынков и утрата ука­занной информации приводят к мате­риальным потерям, которые прояв­ляются в не предусмотренных эконо­мическим проектом дополнительных затратах или прямых потерях обору­дования, имущества, продукции, сы­рья и энергии. | Финансовый,  правовой | Внешний |
| 5 | Отказ и выход из строя оборудования и технических средств предприятия | Низкая надежность технологического оборудования предприятия приводит к неэффективному функционирова­нию всего предприятия в целом и проблематичности потенциала его развития и роста в будущем | Организаци­онный, тех­нологиче­ский, финан­совый | внешний |
| 6 | Недоступность для отдельных руководи­телей предприятия официальной инфор­мации о новых зако­нодательных и иных нормативных актах в сфере вещественного, личного, финансового и иного капитала | Отсутствие подобной информации может привести к финансовой не­устойчивости и технологической за­висимости предприятия, снижению конкурентоспособности его техноло­гического потенциала | Правовой,  финансовый | Внешний |
| 7 | Криминальные дей­ствия отдельных групп и формирований, под­куп лиц, работающих на предприятии | Подобные действия снижают эффек­тивность и надежность функциони­рования предприятий, а в отдельных случаях приводят к прекращению их производственной деятельности | Правовой,  финансовый,  силовой | Внешний |
| В | Преднамеренные пре­ступные действия собственного персо­нала предприятия | Общая тенденция криминализации хозяйственной деятельности ведет к снижению морально-этических норм сотрудников всех рангов, часто тол­кает их на действия, наносящие урон предприятию. | Кадровый,  финансовый, силовой | Внутренний |
| 9 | Противозаконная дея­тельность юридиче­ских и физических лиц в области форми­рования, использова­ния и распростране­ния информации | Подобная деятельность юридических и физических лиц может привести к потере активов субъекта экономики в результате порчи, искажения и раз­глашения конфиденциальной инфор­мации. Потери активов исчисляются в стоимостном выражении | Правовой,  финансовый | Внешний |
| 10 | Сбои программного обеспечения средств обработки информа­ции | Прерывание информации (прекра­щение нормальной обработки ин­формации, например, вследствие разрушения, вывода из строя средств вычислительной техники, обеспечивающих производственные процессы). Такая категория дей­ствий может вызвать весьма серьез­ные последствия, если даже инфор­мация при этом не подвергается ни­каким воздействиям. | Технологи­ческий, информа-  цион­ный | Внутренний |
| 1 1 | Несанкционирован­ный доступ к конфи­денциальной инфор­мации предпринима­телей - конкурентов различными легаль­ными и нелегальными путями | Съем или кража информации путем считывания или копирования инфор­мации, хищение магнитных носите­лей информации и результатов печа­ти с целью получения данных, кото­рые могут быть использованы против интересов предприятия или его руко­водителей | Правовой,  Информаци­онный | Внешний |
| 12 | Модификации ин­формации в крими­нальных целях | Модификация (разрушение) данных (необратимое изменение информа­ции, приводящее к невозможности ее использования) приведет к сбою тех­нологических и управленческих про­цессов на предприятии | Информаци­онный | Внешний |
| 13 | Уничтожение инфор­мации с целью нане­сения морального и материального ущер­ба предприятию и его персоналу | Уничтожение информации приведет к сбою технологических и управлен­ческих процессов на предприятии | Информа-ци­онный | Внешний,  Внутренний |
| 14 | Нарушение установ­ленного регламента сбора, обработки и передачи информации в рамах производ­ственного процесса | Нарушение установленного регла­мента приведет к сбою технологиче­ских и управленческих процессов на предприятии | Информаци­онный | Внутренний |
| 15 | Утечка в информаци­онных системах кон­фиденциальной ин­формации по техни­ческим каналам | Конфиденциальная информация, циркулирующая в средствах вычис­лительной техники и беспроводных сетях, может перехватываться по аку­стическому, электромагнитному, ви­довому каналам, а также по каналу побочных электромагнитных излуче­ний, наводок и др. Перехваченная конкурентами информация может быть использована против интересов предприятия или его руководителя. | Правовой,  информационный | Внешний |
| 16 | Противоправные дей­ствия отдельных лиц и организаций, использу­ющих правовую не­урегулированность ре­жима пользования ин­теллектуальной соб­ственности предприятия | Интеллектуальный капитал предпри­ятия в виде концепций, дизайна, практических знаний и технических решений является реальным источни­ком конкурентных преимуществ для многих видов промышленного произ­водства | Правовой,  интеллектуальный | Внешний |
| 17 | Загрязнение окружа­ющей среды за счет технологических сбо­ев (аварий) оборудо­вания предприятия | Технологическая авария на предприя­тии может возникнуть за счет низкого качества применяемого оборудова­ния, отклонений параметров техноло­гических процессов от заданных ди­версий на предприятии. Устранение загрязнения окружающей среды тре­бует значительных материальных и финансовых затрат на ликвидацию этих загрязнений. | Экологиче­ский, финан­совый | Внешний |

**Лекция 5: «Конкурентная разведка как метод обеспечения экономической безопасности: особенности ее проведения современными российскими предприятиями»**

В условиях рыночной экономики руководителю предприятия для эффективно управления необходима объективная и всесторонняя информация в занимаемом им сегменте рынка об изменениях в планах, стратегии и поведении конкурентов, и другими данными, в том числе о макроэкономических процессах, колебаниях спроса и предложений на рынке, о внедрении новых технологий и достижений науки в промышленное производство.

Развитие информационной среды в Российской Федерации, правовые аспекты доступности информации и использование ее в интересах предпринимательства предопределили актуальность выбранной темы: «Конкурентная разведка особенность ее проведения современными Российскими предприятиями».

Роль информации, ее своевременность и достоверность имеет важное значение для успешного ведения бизнеса. С развитием структуры предпринимательской среды появляются новые отделы и направления оказания преимущественно информационных услуг, которые обеспечивают успешную деятельность предприятия в целом.

Одним из направлений получения информации в интересах предприятия является деятельность конкурентной разведки. На мой взгляд, основные направления деятельности или задачи конкурентной разведки сводятся к следующему:

1.  обеспечить руководителя, определяющего политику компании, объективной, своевременной и полной информацией о положении предприятия в конкурентной среде;

2.  своевременное предупреждение руководителя о всех неблагоприятных возможных изменениях в предпринимательской среде с тем, чтобы на основании заслуживающей внимание любой информации руководитель мог принять единственно правильное управленческое решение;

3.  поиск новых ниш, возможностей.

В своей деятельности сотрудники конкурентной разведки, сталкиваются с необходимостью обработки большого количества информации самого разнообразного характера. Умение ориентироваться в потоке новых сведений и данных с тем, чтобы правильно организовать свою деятельность, является чрезвычайно важным элементом в работе каждого структурного подразделения.

Профессионализм руководителя и его персональная ответственность за управленческие решения во многом зависит от осознания им внутренних сильных и слабых сторон компании и его готовности и умения оптимально использовать данные конкурентной разведки в контексте общей обстановки.

Одной из особенности деятельности конкурентной разведки является фидуциарный (лично-доверительный), индивидуальный характер между руководителем предприятия и исполнителем. Эти правоотношения могут быть основаны на трудовых обязательствах, если отдел конкурентной разведки находится в структуре предприятия, либо на ином договоре (обычно на договоре возмездного оказания услуг), если исполнителем является самостоятельное юридическое лицо (либо частное охранное предприятие).

Для обоюдного уяснения задачи необходимо представлять, какие именно факторы могут оказать наиболее существенное влияние на предмет, который изучается в настоящее время. Цикл сбора разведданных состоит из четырех базовых элементов:

1.  выбрать (определить), что именно требуется знать;

2.  собрать информацию и убедиться в ее достоверности;

3.  преобразовать собранную информацию в конечный продукт (данные);

4.  обеспечить своевременную доставку этого конечного продукта к тем, кто определяет политику предприятия.

Информация, предоставляемая подразделением конкурентной разведки, должна позволить прогнозировать действия предприятий конкурентов. Следует учитывать, что данная информация подлежит непрерывной перепроверке в динамике ее развития с учетом изменений конкурентной среды.

Конкурентная разведка является важной частью стратегического планирования. Деятельность подразделения конкурентной разведки можно отнести к механизму позволяющей компании составить хороший стратегический план и выполнить его, с учетом постоянных изменений в предпринимательской среде.

Ключевая роль аналитической составляющей менеджмента на основе предварительной и объективной информации явилось предпосылками для деятельности, связанной с получением, сбором и обработкой данной информации.

**1.1 Роль и место конкурентной разведки в системе управления бизнесом**

Получение информации, в том числе, связанной с предпринимательской средой относится к разведывательной деятельности.

Под термином «разведка» в широком смысле этого слова понимается, с одной стороны, деятельность субъекта (от человека, организованной группы людей до государства в целом) по добыванию сведений об имеющихся и потенциальных угрозах его существованию и интересам, то есть о действующем или вероятном противнике, а с другой – организационная структура, силы и средства для осуществления этой деятельности.

Существует много видов разведки, но нас интересует только:

·  Конкурентная разведка.

·  Бизнес-разведка.

·  Шпионаж.

·  Экономическая разведка.

·  Бенчмаркинг.

·  Деловая разведка.

Конкурентная разведка – стратегический инструмент управления, позволяющий высшему руководству определить основные тенденции ситуаций на рынке с помощью спланированных действий по систематическому и этичному сбору, анализу и управлению информацией о внешней среде, которая может повлиять на осуществление планов предприятия и его работу в целом.

Бизнес-разведка – инструмент управления, позволяющий получить информацию:

А) для успешного выживания и развития предприятия в сложной конкурентной борьбе

Б) для принятия оптимальных управленческих решений высшим звеном руководства компании

В) о намерениях партнеров, клиентов и контрагентов, о сильных и слабых сторонах конкурентов, имеющихся у них ноу-хау;

Г) о фактах, оказывающих влияние на позицию оппонентов в ходе деловых переговоров;

Д) о возможном возникновении кризисных ситуаций;

Е) о ходе реализации заключенных договоров и достигнутых ранее договоренностей и т.п.

По мнению Л.Д. Шарый бизнес-разведка включает в себя следующие направления: маркетинговая разведка, конкурентная разведка, шпионаж, бенчмаркинг.

Шпионаж – вид недобросовестной конкуренции, деятельность по незаконному добыванию и выведыванию сведений, представляющих производственные и деловые секреты конкурентов, их коммерческую тайну, из закрытых от широкого доступа (и посторонних лиц) источников в интересах достижения экономических выгод и преимуществ.

Бенчмаркинг – «Динамическое Управление По Лучшим Образцам»

вид деятельности по поиску и получению информации для сопоставления организации бизнес-процессов в собственной компании с аналогичными процедурами в иных, более успешных предприятиях.

особый вид деятельности по поиску и получению информации о лучших решениях, используемых в деятельности других компаний. Эти компании могут быть конкурентами, хотя наиболее удачные заимствования чаще всего удается получить от тех фирм, которые работают в иных отраслях, регионах, рынках, в других странах и так далее.

Отличием конкурентной разведки от промышленного шпионажа является то, что конкурентная разведка 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 конкурентной разведки 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, 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 очень размытой.

В нынешней России промышленный шпионаж и бизнес-разведка существуют по преимуществу в нераздельном виде, представляя своеобразный симбиоз открытых, разрешенных законом и скрытых, нелегальных методов получения экономической информации.

Экономическая разведка – это совокупность согласованных действий по добыванию, интерпретации, распространению и защите информации, полезной для негосударственных субъектов экономики и добываемой легально и при наилучших условиях в смысле качества, сроках и издержек.

Экономическая разведка боле узкое направление по получению и использованию информации, так как не рассматривает конкурентную среду в целом. А конкурентная разведка напротив является стратегическим инструментом управления. В то же время экономическая разведка осуществляет защиту информации, что не свойственно для конкурентной разведки.

Под деловой разведкой (прямой перевод с английского – business intelligence) в зарубежной практике понимается сбор и анализ сведений о партнерах и конкурентах.

Деловая разведка – составная часть корпоративной культуры ведения современного бизнеса. Для выживания предприятия в условиях конкурентной борьбы первоочередную роль начинает играть разведка намерений конкурентов, изучение основных тенденций бизнеса, анализ возможных рисков. В России понятия business intelligenсe (деловая разведка) и industrial espionage (промышленный шпионаж) рассматриваются во взаимосвязи, поскольку в России в силу недопонимания процессов разведка зачастую подразумевает шпионаж.

Деловая разведка – это легальное занятие, вписывающееся в понятие добросовестной конкуренции. Засылки агентов и использования для получения сведений технических средств в рамках business intelligence обычно не используются. Считается, что этим деловая разведка отличается от промышленного шпионажа.

**1.2 Принципы конкурентной разведки**

К принципам конкурентной разведки относится:

*I.  Законность и этичность сбора информации об основных составляющих бизнеса.*

По мере возрастания потребностей в получении ценной деловой информации возрастает роль этических норм.

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.

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.

Общество регулируется традициями, моралью и только в последнюю очередь (и по наиболее значимым вопросам) – законом. Государство в лице уполномоченных органа вмешивается при нарушении норм уголовного права. Этика очень неоднозначна и серьезно зависит от культурных ценностей и традиций, в отличие от законности не поддается однозначной идентификации. В реальной жизни грань между конкурентной разведкой и промышленным шпионажем зависит от умения того, кто ее проводит, не вступать в противоречие с нормами права.

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.

Для правильной организации своей деятельности компании нуждаются в собственном наборе этических правил – этическом кодексе деловой разведки.

Далее перечислим 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:

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, так как отсутствует признак виновность в действиях лица, необходимая для состава преступления или правонарушения. Однако после того как вы узнали об ее противозаконном приобретении, невозвращение владельцу или использование ее в своих целях уже может рассматриваться как нарушение. В действительности, специфика кодекса конкурентной разведки 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 конкурентной разведки при случайном получении запрещенной информации, например конфиденциальных заметок. 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. 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.

Положение Этического Кодекса, составленного американским «Обществом профессионалов конкурентной разведки» (Society of Competitive Intelligence Professionals) для своих членов, может быть применено в российской практике.

v  Постоянно стараться увеличить уважение и признание к профессии конкурентной разведки на всех государственных уровнях.

v  Выполнять свои служебные обязанности с рвением и прилежанием, поддерживать самый высокий уровень профессионального мастерства и избегать всех неэтичных поступков.

v  Оставаться верным политике компании, ее целям и общему курсу и выполнять обещания, данные своей компании.

v  Выполнять все действующие законы

v  Во время делового свидания предоставлять всю относящуюся к делу информацию, включая принадлежность к организации

v  Соблюдать правила работы с конфиденциальной информацией

v  Действовать в полном соответствии с этими этическими стандартами при работе внутри компании, при ведении переговоров и во всех ситуациях, когда приходится работать по специальности.

Этические нормы ведения бизнеса широко используются и закрепляются различными крупными компаниями. Это показывает высокий уровень корпоративной культуры для любых отраслей и видов деятельности. Например, этические правила поведения ведущей американской компании в области деловой разведки Fuld & Company закрепляют «десять заповедей легального сбора разведывательной информации»:

·  Не лгать, когда представляетесь.

·  Запрещается нарушать официальную генеральную линию вашей компании.

·  Не записывать на диктофон разговор с собеседником без его разрешения.

·  Не предлагать взятки.

·  Не устанавливать подслушивающие устройства.

·  Умышленно не вводить собеседника в заблуждение при переговорах.

·  Не получать от конкурента и передавать ему ценную конфиденциальную информацию.

·  Не распространять дезинформацию.

·  Не воровать промышленные секреты.

·  Осознанно не давить на собеседника с целью получения требуемой информации, если это может подвергнуть опасности его жизнь или репутацию.

Высший управленческий персонал должен следить за тем, чтобы этические нормы соблюдались не только в конкурентной разведке, но и в самой компании в целом.

Этические нормы являются необходимыми предпосылками для закрепления принципов.

*II.  Непрерывность и комплексность проводимых мероприятий*

В связи с постоянным изменением предпринимательской среды конкурентной разведке необходимо осуществлять непрерывный процесс. Такой процесс должен периодически повторяться по заданному алгоритму для обновления информации, хотя конкретные действия могут быть уникальными в каждом конкретном случае.

Информация, предоставляемая подразделением конкурентной разведки, должна позволять прогнозировать действия конкурента. Но ее необходимо непрерывно перепроверять в динамике развития**.**При проверке одной и той же информации, поступающей, похоже, из разных источников, надо быть уверенным в том, что первоисточник у нее не один и тот же.

*III.  Учет альтернативных источников влияния на бизнес*

Необходимо учитывать тенденции, имеющиеся в политике, экономике и промышленности; положение на рынке и соответствующие аспекты мировой и региональной ситуации.

*IV.  Легендирование подразделения КР*

Подразделение конкурентной разведки целесообразно вписать в ведомость по зарплате и в штатном расписании в отделе стратегического планирования, либо в отделе маркетинга с целью повысить эффективность работы конкурентной разведки. В этом случае специалисты конкурентной разведки смогут выполнять свою работу, представляясь возможным собеседникам специалистами соответствующего отдела, каковыми они формально являются, и в то же время передавать наиболее деликатные целевые данные непосредственно руководству предприятия, сохраняя при этом необходимый уровень конфиденциальности.

*V.  Ограничение доступа к продукту КР*

В своей работе мы остановимся на трех видах ограничения доступа к продукту конкурентной разведки по пользователям. Так пользователями могут выступать:

1.  Только первое лицо или исполнительный директор. Конфиденциальность информации в интересах предприятия обеспечивается ограниченным кругом должностных лиц – сотрудников конкурентной разведки. Мне представляется целесообразным, чтобы информация, подготовленная по заданию руководителя предприятия, предоставлялась лично ему (либо заместителю). Это позволит не проходить информации через избыточные каналы, чтобы она не исказилась.

2.  Предоставление продукта конкурентной разведки определенному кругу лиц. Так как большая часть продукта конкурентной разведки конфиденциальна доступ к системе можно получить, только если сотрудник обратится в группу конкурентной разведки и обоснует необходимость запроса. Таким образом, группа конкурентной разведки и директор организации решают, кто может получить доступ, а кто – нет.

3.  Весь персонал организации. Для распространения на рынке продукта своей компании сотрудники вынуждены в рамках своих должностных обязанностей исследовать работу конкурентов для этого им. Информацию о конкурентах сотрудники могут получить как в средствах массовой информации, так и внутри своей компании из отдела конкурентной разведки, например, в виде обобщенной справки.

Одна из основных проблем конкурентной разведки – слишком широкий круг получателей. Для защиты своей информации внутри компании необходимо осуществить следующие мероприятия:

При оформлении в каждом документе, отмечать что информация, содержащаяся в нем, является конфиденциальной и предназначена только для внутреннего пользования и /или доступна в применении конкретным должностным лицом.

В этом случае, при несанкционированном распространении информации виновные лица могут понести ответственность.

Обязательная регистрация служебной информации, ее предоставления внутри компании. Ограниченный доступ к служебной информации и ее циркуляция во внутренней компьютерной сети, классификация доступа для персонала.

Режим конфиденциальности устанавливает уровень доступа к конфиденциальной информации должностных лиц предприятия, а также обеспечиваются условия, необходимые для защиты информации, составляющей коммерческую тайну. Как правило, особый режим конфиденциальности подразумевает:

соблюдение необходимого порядка подбора, изучения и оформления лиц для работы на предприятии;

ограничение круга лиц, допускаемых к секретным работам, документам; определение должностных лиц предприятия, имеющих право разрешать ознакомление с той или иной категорией документов и сведений;

доведение до исполнителей только такого объема секретных сведений, который им необходим для выполнения служебных заданий;

проведение работы среди исполнителей по разъяснению требований режима секретности, повышению их ответственности за сохранение доверенных секретов;

организацию охраны помещений, в которых содержатся носители конфиденциальной информации, а также режима работы в них;

закрепление технических средств обработки конфиденциальной информации за сотрудниками, определение персональной ответственности за их сохранность;

установление порядка пользования носителями конфиденциальной информации (учет, хранение, передача другим должностным лицам, уничтожение, отчетность);

проведение мероприятий по предотвращению утечки секретов в повседневной деятельности;

организацию контроля за установленным порядком, предусматривающего проверку соответствия организации защиты информации установленным требованиям, а также оценку эффективности применяемых мер защиты информации.

Как правило, контроль осуществляется в виде плановых и внеплановых проверок силами своих сотрудников или с привлечением других организаций, которые специализируются в этой области. По результатам проверок специалистами по защите информации проводится необходимый анализ с составлением отчета, который включает: вывод о соответствии проводимых на предприятии мероприятий установленным требованиям; оценку реальной эффективности применяемых на предприятии мер защиты информации и предложения по их совершенствованию.

**Лекция 6: продолжение темы ««Конкурентная разведка: особенности ее проведения современными российскими предприятиями»»**

**1.3 Анализ и обработка информации в конкурентной разведке**

Процесс конкурентной разведки представляет собой последовательность определенных этапов, которые ведут аналитика к наиболее точным и адекватным умозаключениям, основанным на имеющейся в данный момент информации. На каждом этапе сотрудник выполняет определенные функции, а сам процесс представляется как единая система, компоненты которой образуют сложную структуру.

Процесс конкурентной разведки состоит из следующих элементов:

1.  Постановка задачи

2.  Сбор информации

3.  Оценка и упорядочение информации

4.  Анализ информации

5.  Формирование отчетов

6.  Доведение до руководства.

2.  Сбор информации

От того, насколько удачно будет собрана первичная информация, зависит успешность решения конкретной задачи предстоящего анализа. При этом именно цель направленного анализа определяет содержание информации, подлежащей отбору, основные направления ее исследования, а также выбор методики анализа.

Конкретный объем данных, необходимых для анализа и принятия решения, в каждом случае индивидуален. Тем не менее, можно выделить ряд требований, которыми следует руководствоваться при определении объема информации: минимальность, достаточность и всесторонность. Избыточность информации засоряет информационный массив и влечет неоправданные затраты на его переработку. Недостаточность информации ведет к поверхностной, неглубокой оценке факторов. Отсутствие всесторонности приводит к однобоким решениям. Собранная информация должна быть также достоверной, непротиворечивой и полезной для достижения конкретно поставленной цели. Данный этап процесса аналитической разведки имеет важнейшее значение для работы всей системы, поскольку он позволяет минимизировать непроизводительные затраты времени и средств.

Следует четко определить сроки сбора информации. Нельзя допускать ни преждевременного сбора информации, когда еще не созрели условия для появления факта или изменения обстановки, ни ее получения с опозданием.

Большое значение для правильного сбора информации имеет знание источников, откуда могут быть почерпнуты сведения, необходимые для анализа. Круг источников информации в значительной мере зависит oт цели исследования, направленности анализа, отдела, в интересах которой он осуществляется, и т.д.

Информация выбирается из всех доступных источников, но с учетом специфики, с тем, чтобы не расширять круг источников до бесконечности. По отдельным вопросам сбор информации может осуществляться негласным путем с использованием разведывательных возможностей органов внутренних дел.

Источники конкурентной разведки делятся на первичные и вторичные:

·  К первичным относятся: выступления на выставках и конференциях, годовые отчеты, бухгалтерская отчетность, правительственные документы.

·  Вторичные – Интернет, пресса, книги, аналитические материалы, телевидение и радио.

3.  Оценка и упорядочение информации

На следующем этапе собранная информация должна быть оценена. Это делается для того, чтобы критично воспринять весь аналитический процесс, а следовательно и вытекающие в результате заключения. Оценка качества исходной информации имеет очень большое значение, т. к. выдвигаемая в результате анализа гипотеза есть величина вероятностная. Вероятность истинности гипотезы зависит от достоверности исходного материала как составляющей процесса.

Обобщение и оценка (первичный анализ) собранной информации начинается, как правило, с определения ее качества, полноты и достоверности.

Уровень достоверности, с которой могут быть сделаны заключения, зависит от качества данных, лежащих в их основе. Наиболее полной и достоверной считается информация статистической отчетности. Однако следует учитывать, что статистическая информация различных ведомств может оказаться несовпадающей, противоречивой и даже несопоставимой. Кроме того, на данные статистики оказывает влияние механизм ее формирования, который может исказить реальную картину анализируемого явления (процесса). Это требует подтверждения статистической информации сведениями из других источников.

Для оценки достоверности следует разграничивать два понятия: надежность источника и достоверность данных. Надежность источника определяется, исходя из его характеристик. Если источником информации является человек, то необходимо учитывать его физическое и психологическое состояния, от которого зависят уровень и качество восприятия окружающей обстановки.

Если источниками информации являются различные банки данных, то необходимо учитывать дату их обновления.

Для избегания возможных ошибок, оценка данных должна быть основана на двух фундаментальных принципах:

– на оценку не должны влиять личные эмоции, т.е. она должна производиться на основе объективных профессиональных суждений;

– оценка источника информации всегда должна производиться раздельно с оценкой самой информации.

Особо следует подчеркнуть, что подтвержденная информация не всегда бывает одновременно правдивой. Соответствующая оценка должна сопровождаться указанием на степень надежности источника и достоверности информации. Для этой цели западные коллеги применяют специальные шкалы, использующие следующую градацию надежности.

Упорядочение первичной информации – это группировка показателей по наиболее существенным для исследователя качественно однородным признакам.

Так происходит систематизация собранной информации. Первым шагом для этого является представление всех данных в виде объектов различных типов и описание их атрибутов. На втором шаге устанавливаются связи между объектами и описываются атрибуты связи. Таким образом, организуется хранение данных и создание системы ссылок для последующего их поиска.

Упорядочение первичных данных – это группировка показателей по наиболее существенным для исследователя качественно однородным признакам.

Так происходит систематизация собранной информации. Первым шагом для этого является представление всех данных в виде объектов различных типов и описание их атрибутов. На втором шаге устанавливаются связи между объектами и описываются атрибуты связи. Таким образом, организуется хранение данных и создание системы ссылок для последующего их поиска.

4.  Анализ информации

Первичный анализ информации уже начат на этапе ее оценки и даже раньше – на этапе ее получения. Присвоение определенных атрибутов конкретной информации уже ведет к структурированию данных и как следствие к их анализу (к структуризации и категоризации).

Процесс собственно анализа информации состоит из следующих этапов:

1.  Рефенирование информации

2.  Сопоставление информации

3.  Синтез данных

1. Реферирование информации.

Реферирование особенно полезно в случае большого объема информации из разных источников (СМИ, БД) и при необходимости дальнейшего цитирования. Но реферирование всегда ориентировано на объект интереса, т.е. тот, кто реферирует – определенным образом сам искажает информацию, поэтому лицу, проводящему реферирование, важно понимать зачем он это делает (какова конечная цель) и для кого он это делает. Последнее важно для наиболее точной и полной передачи информации (вопрос согласованности каналов обмена информацией). Реферирование заключается в выборке из всего массива информации ключевых моментов и их фиксировании.

2. Сопоставление информации

Данный этап имеет важное значение для последующего использования материала и осуществляется в два приема:

- систематизация сведений – разбиение всего массива информации на блоки по какому то признаку – выделение фактов;

- собственно сопоставление – поверхностный анализ с целью выявления явных и возможных связей с объектом изучения и с иными «кусочками» информации;

- фиксация этих связей.

При использовании компьютерного анализа такие связи можно выявлять по датам, по действующим лицам, по месту свершения события, по названиям, по сферам интересов, по телефонам и т.д. Работая вручную, можно выявить и неявно выраженные связи.

3. Синтез данных

Синтез данных – наиболее важная процедура обработки информации – логическое объединение элементов информации, внешне не обладающих связями, в систему единой направленности. Здесь упор делается на выдвижение обоснованной гипотезы. На этом этапе работы с информацией решаются следующие задачи:

- установление связей между разрозненными элементами и укладывание их в единую логическую схему (например, описательная модель объекта или модель поведения);

- формулирование на основе полученных моделей гипотезы;

- определение потребностей в недостающих сведениях и постановка задачи по их нахождению;

4)  Резюмирование текста.

На первом этапе использовалось реферирование, а теперь используется близкий по приемам метод – резюмирование.

Технология следующая. Исследуемый текст читается три раза.

При первом прочтении выделяются слова, несущие основную смысловую нагрузку – ключевые слова – они выделяются. Это могут быть имена, названия, даты, профессиональные выражения и т.п.

При втором прочтении внимание концентрируется на ключевых словах, при этом выделяются короткие, не содержащие ничего лишнего словообразования (словосочетания), отражающие основные мысли исследуемого текста и характеризующие ключевые слова – также выделяются.

На третьем прочтении внимание обращается только на выделенные словообразования и на их основе строятся простые, краткие предложения, описывающие смысл сообщения. После чего делается вывод об основном смысле изучаемого текста.

5.  Формирование отчетов

6.  Доведение до руководства

Конечная цель подразделения (сотрудника) конкурентной разведки довести до заказчика результат анализа о характере и масштабах экономически выгодных процессов, а также о задействованных в них конкретных лицах и организациях.

При этом очень важно иметь в виду, что заключение имеет ограниченную ценность, если оно не сопровождается вероятностной оценкой его достоверности.

**1.4 Тактические и стратегические задачи конкурентной разведки**

Конкурентная разведка как дисциплина первоначально занималась процессами и средствами для сбора, анализа и распространения разведывательных данных, позволяющих сотрудникам принимать качественные и эффективные решения. Эти решения могут быть по своему характеру либо стратегическими, либо тактическими.

Тактическая (ориентированная на продукцию) конкурентная разведка обеспечивает потребности производственного отдела, служб маркетинга и продаж.

Стратегическая обеспечивает потребности топ-менеджмента (для принятия кратко- и долгосрочных решений).

Специалист конкурентной разведки при нахождении информации и ее анализе должен определить является ли данный материал конкурентной информации стратегической, тактической или «иной» информацией. При нахождении стратегической информации, она передается ключевым лицам, принимающим решения. Тактическая информация анализируется для выполнения запроса, а «иная» информация вносится в каталог, и сохраняться, пока не будет получена новая информация.

Необходимо отметить, что любая информации может быть стратегической, тактической или «иной» в разный промежуток времени. Это временное измерение определяет, является ли данная информация важной в тот или иной день.

Отдел продаж и отдел маркетинга предоставляют широкие возможности для анализа многоуровневой деятельности конкурентной разведки. Таким образом отделы продаж и маркетинга часто используются в качестве модели для исследования процесса координации стратегической и тактической разведывательной информации.

Для типичных отделов продаж и маркетинга характерно достаточно четкое разграничение основной деятельности по трем иерархическим уровням. Сотрудники, отвечающие за продажи на стратегическом уровне, участвуют в прогнозировании, установлении квот, стратегическом контроле, проникновении на рынок, планировании и распределении ресурсов. Сотрудники, отвечающие за продажи на тактическом уровне, сосредотачиваются на реализации стратегических целей, взаимодействии с крупными клиентами, обмене «оперативной» информацией с высшим руководством и управлении сотрудниками отдела продаж. Сотрудники, отвечающие за продажи на оперативном уровне, концентрируют свои усилия на формулировании предложений потребителям, определении цен, взаимодействии с покупателями, обслуживая выделенный им регион или территорию. Сотрудники, отвечающие за маркетинг на стратегическом уровне, определяют диапазон предлагаемых на рынке продуктов, составляют бюджеты и маркетинговые планы и участвуют в разработке позиционировании продуктов. Сотрудники, отвечающие за маркетинг на тактическом уровне, сосредотачиваются на управлении продуктами компании, развитии рынка, ценообразовании, продвижении и распространении. Наконец, сотрудники, отвечающие за маркетинг на оперативном уровне, участвуют в изучении рынка и потребителей и в сборе маркетинговой разведывательной информации. Наиболее подходящие виды продуктов и услуг КР будут варьировать в зависимости от статуса руководителя, принимающего решения в организации. Эти потребности необходимо координировать, чтобы добиться «симбиоза» стратегической и тактической информации.

Тесное общение и различные виды оперативно взаимодействия между отделами продаж и маркетинга могут увеличить способность фирмы координировать стратегическую и тактическую разведывательную информацию.

В конкурентной разведке стратегическая и тактическая информация часто разделяется и в концептуальном плане, и в реальности. Это привело к тому, что практики конкурентной разведки либо сосредотачиваются на одном из видов информации в ущерб другому, либо создают независимые системы и методы для управления своей стратегической и тактической разведывательной информацией. Это неправильно, потому что в стратегическая и тактическая разведывательная информация тесно взаимосвязаны и усиливают друг друга.

Лекция 7: Методический подход к интегральному оцениванию безопасности предприятия

Оценка уровня безопасности хозяйствующего субъекта является одним из краеугольных камней деятельности по обеспечению его безопасности. С постановки и решения этой задачи следует начинать формирование или совершенствование системы обеспечения безопасности. Результаты этой

работы фактически формируют мотивацию акционеров и руководства предприятия к построению и развитию системы обеспечения его безопасности, позволяют выявлять «тонкие» места в защите его ресурсов и интересов, прогнозировать ущерб, служат аналитической базой для рационального распределения средств на развитие системы обеспечения безопасности. При этом использование для оценивания числовых методов позволяет во многом «очистить» оценку от субъективизма и при разработке бюджета применять хорошо разработанные в теории и широко используемые в практике методы математического программирования.

Исходя из определения категории «безопасность», оценка уровня безопасности предполагает интегральную оценку потенциального ущерба хозяйствующему субъекту, который может быть ему нанесён в рассматриваемый период времени. Для этого необходимо каким-то образом сопоставить всю совокупность угроз предприятию, учитываемых в модели безопасности предприятия и минимизации возможного ущерба.

Обобщённые структурные элементы механизма оценки безопасности предприятия следующие.

1. Составляется (идентифицируется) перечень угроз.
2. Определяется совокупность рисковых событий с учётом их возможного совпадения, повторения и т. п. Рисковые события определяются до уровня типов по отношению к объектам защиты и видам ущерба. Каждое рисковое событие идентифицируется по объекту защиты, виду ущерба и характер нанесения ущерба. Для решения рассматриваемой задачи непосредственно важны не угрозы, а рисковые события.
3. Рассчитывается ожидаемый ущерб в результате рисковых событий с учётом их взаимного влияния.
4. Оценивается возможность системы ХС предотвратить рисковые события или сократить ущерб, который они влекут.
5. Уточняется ожидаемый ущерб в результате рисковых событий с учётом их взаимного влияния и противодействия со стороны системы ХС.
6. Рассчитывается интегральный риск как степень недостижения интересов.

Схема механизма оценки безопасности предприятия представлена на рисунке 1

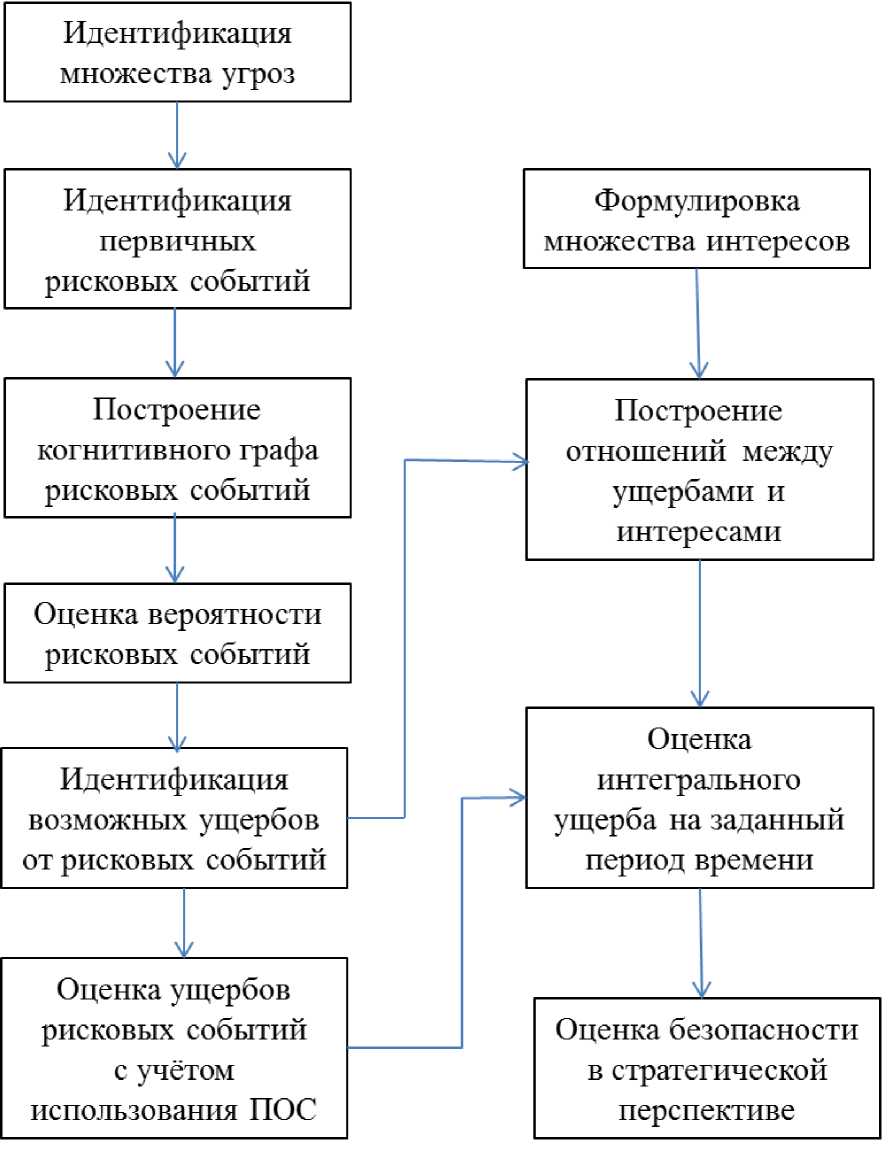


Рисунок 1 - Схема механизма оценки безопасности предприятия

Идентификация множества угроз

Перечень угроз задаёт тематику мониторинга неблагоприятных воздействий, позволяет организовать систематическую работу по совершенствованию методического обеспечения выявления угроз. Однако это не может быть единственно верным и исчерпывающим поведением.

Во-первых, этот перечень может уточняться в соответствии с представлениями лиц, готовящих и принимающих решения, по месту и времени.

Во-вторых, необходимо постоянно осуществлять анализ отношений внутри хозяйствующего субъекта и с внешней средой для выявления новых (ранее невыявленных, неучтённых) угроз и вызовов.

Идентификация первичных рисковых событий

Рисковое событие представляет собой деструктивное воздействие на какой-либо объект защиты. Одна и та же угроза из перечня угроз может приводить к различным рисковым событиям в зависимости от формы проявления угрозы. Рисковые события могут прогнозироваться, в том числе на основе статистики (для статистических угроз) и представляют собой свершившиеся факты.

Целесообразно установить отношения между множеством угроз и множеством рисковых событий, которые описываются матрицей вероятностей появления рискового события в результате актуализации угроз.

Перечень рисковых событий так же, как и угроз, не является ни универсальным и незыблемым, ни исчерпывающим. В каждом конкретном случае может быть составлен перечень «по месту». При этом всегда надо предполагать возможность появления предварительно неописанных вариантов.

Рисковые события могут быть импульсными и приводить к разовому ущербу, а могут иметь продолжающийся характер. К первым, например, относится утрата ТМЦ, авария, ко вторым - повышение тарифов естественных монополий, снижение качества труда в результате деградации кадров или снижения зарплаты.

Построение когнитивного графа рисковых событий

(когнитивный граф – это когнитивная карта в виде графа, позволяющей описывать субъективное восприятие человеком или группой людей какого-либо сложного объекта, проблемы)

Рисковые события могут порождать другие рисковые события неизбежно или с некоторой вероятностью, практически мгновенно или через некоторое время. В этих случаях возникает сценарий, совокупность сценариев или совокупность возможных сценариев развития ситуации возникновения ущерба.

Большое значение имеет определение того, в какой степени угроза является причиной генерации рисковых событий, так как в результате должен быть оценен приоритет действий по её предупреждению и (или) нейтрализации. Кроме того, взаимовлияние рисковых событий должно учитываться при прогнозировании нарастания угроз, которое может приобрести лавинообразный характер.

Взаимное влияние рисковых событий описывается отношениями между ними, которые определяются величиной ущерба V и вероятностью его появления р(V).

Оценка вероятности рисковых событий

Оценка вероятности рисковых событий может осуществляться либо на основе статистики, либо с помощью расчётов, либо экспертным путём.

Третий случай возникает, когда для оценки не хватает предыстории и суждения о вероятности приходится выносить на интуитивном уровне.

Идентификация возможных ущербов от рисковых событий

Строго говоря, ущерб бывает разного вида и это следует учитывать в модели наиболее общего характера. Однако в контексте безопасности хозяйствующего субъекта часто можно ограничиться только ущербом, исчисляемым в денежных единицах.

Для каждого рискового события существует своя модель оценки ущерба. Как правило, величина ущерба носит вероятностный характер, поэтому может быть оценена математическим ожиданием или верхней границей некоторого доверительного интервала.

Оценка ущербов рисковых событий с учётом использования ПОС(системы защиты)

Оценка безопасности определяется не только наличием и реализацией угроз, но и возможностью объекта защиты предотвращать их, т. е. наличием и эффективностью применения ПОС (системы защиты).

Формулировка множества интересов

В процессе оценки безопасности в качестве интересов могут использоваться основные задачи, стоящие перед предприятием.

Интересы формулируются таким образом, что они должны быть независимы по полезности, другими словами, достижение одного из них не должно влиять на отношение к степени удовлетворения.

Построение отношений между интересами и ущербами

Основная задача и трудность этого этапа механизма оценки безопасности заключается в определении тех ущербов, которые непосредственно оказывают воздействие на интересы. Например, задержка поставок со стороны контрагента непосредственно не влияет на интересы проекта или предприятия, однако это может привести к задержке следующих этапов жизненного цикла продукции, к штрафным санкциям со стороны заказчиков и т. д.

Авария серийного образца может не привести к существенным финансовым потерям вследствие получения страховых выплат, однако приводит к потере доверия со стороны потребителей. С другой стороны, авария при проведении испытаний может привести к удорожанию стоимости проекта, затягиванию его сроков, однако может и не отразиться на безопасности, если подобная ситуация предусмотрена в системе финансирования и страхования работ проекта.

В одних случаях влияние ущерба может быть рассчитано исходя из финансовых потерь, других, например, если в числе интересов «авторитет производителя», степень удовлетворения интереса может быть установлена на основе экспертного опроса.

Целесообразно при оценке безопасности (степени удовлетворения интересов) учитывать затраты на её обеспечение.

Оценка интегрального удовлетворения интересов на заданном периоде

Оценку интегрального удовлетворения интересов целесообразно осуществлять с использованием моделей теории полезности

В упрощённой форме допустимо использование средневзвешенной суммы удовлетворения совокупности интересов.

Оценка безопасности в стратегической перспективе

Предыдущие этапы механизма оценки безопасности описывали процедуры оценки на некоторый заданный период времени. Однако для стратегической оценки необходимо прогнозировать безопасность на достаточно длительную временную перспективу с учётом предпочтений к уровняю её обеспечения на различных этапах в будущем.

В качестве модели оценки используется форма, объединяющая уровни безопасности на каждом интересующем этапе в будущем, при этом оценка может производится на длительную перспективу (период более 12 лет) либо на единичный период равный одному году.

Ранжирование угроз

Ранги угроз определяют приоритетность деятельности по их предупреждению ранг определяется тем, в какой степени соответствующая угроза снижает интегральную оценку безопасности.

Лекция 8: «Подходы к анализу безопасного существования предприятия»

8.1 «Оценка ущерба и его распространения в условиях

аналитической неопределённости

* 1. Частные модели оценки основных проектных рисков
  2. Механизм оценки безопасности предприятия в режиме использования автоматизированной информационной технологии

8.1 «Оценка ущерба и его распространения в условиях

аналитической неопределённости

Под аналитической неопределённостью понимается отсутствие объективной с точки зрения обоснования естественными закономерностями модели описания ущерба при каком-то рисковом событии, возникшем в результате некоторых других рисковых событий.

При этом ущерб может накапливаться в соответствии с динамикой распространения, отражаемой с выбранной тактовой частотой изменения рисковых событий.

В случаях, если ущерб заключается в прямых финансовых потерях, он может элементарно суммироваться. Однако, если речь идёт о снижении уровня мотивации персонала, переменах во внешнеполитической обстановке, изменениях платёжеспособности потребителей и т. п., то вызываемые подобными обстоятельствами ущербы не очевидны и могут быть оценены экспертным путём.

Рассматриваемая нами оценка, в условиях аналитической неопределенности является экспертно-аналитической, позволяющей отразить общее состояние, прогноз и, главное, направленность динамики уровня безопасности в условиях множества разнохарактерных угроз и последствий их реализации при приемлемых трудозатратах на аналитическую и экспертную работу.

С помощью этой оценки есть возможность определить критичные точки распространения рисков. Эти данные необходимы для планирования рационального развития системы экономической безопасности, совершенствования механизмов его использования.

Область применения рассматриваемой оценки определяется наличием множества разнохарактерных угроз, а следовательно, рисковых событий. Используя ее можно моделировать состояния безопасности на продолжительный период. Такая оценка используется, как правило, не для текущих оценок в конкретных ситуациях, а для выявления складывающихся тенденций.

Для построения модели оценки необходимо учитывать следующие моменты:

* ущерб имеет накопительный характер;
* взаимное влияние угроз происходит с некоторой тактовой частотой, т.е. с определённым ритмом. И в данном случае за один такт, т.е. определённый ритм, принимают одну-две недели, если речь идет о каком-то проекте и месяцу для предприятия в целом;
* воздействие нескольких рисковых событий описывается как их сумма с учётом характера накопления ущерба.

Распространение риска в общем случае аналогично процессу размножения в условиях определенных ресурсных ограничений.

В результате воздействия исходного рискового события размножаются негативные микрособытия, или ущербы. Однако необходимо учесть, что ущерб не может быть более чем, стоимость объекта защиты, или сокращения выручки в результате потери сектора рынка, или увольнения всех работников и т. п.

На основе этого рассчитывается математическая модель взаимовлияния рисковых событий, которая позволяет прогнозировать значения ущербов от рисковых событий в различные будущие моменты времени с учётом взаимовлияния этих рисковых событий.

В модели используются такие значения как:

- номер такта (единичного, элементарного временного интервала) изменения рисковых событий в интересующей предметной сфере (либо это проект, либо предприятие),

- значение ущерба в результате случившегося рискового события, полученное на определенном такте;

- значение ущерба после такта;

- параметр, описывающий влияние случившегося рискового события, который отражает интенсивность наращивания ущерба.

Для прогнозирования рисков на заданную временную перспективу рассчитываются значения всех определенных ущербов.

При работе такой модели значения ущербов на каждом шаге следует уточнять по результатам их прогнозирования в зависимости от всей совокупности факторов, включая известные плановые.

* 1. Частные модели оценки основных проектных рисков

В настоящее время существует множество вариантов классификации рисков, включающих десятки позиций. В соответствии с принятой методологией классифицировать следует не столько риски, сколько рисковые события, которые определяются угрозами. При этом сама классификация в практическом аспекте имеет смысл для организации мониторинга состояния безопасности и создания библиотеки моделей оценки рисков в результате рисковых событий.

Модели оценки рисков можно разделить на три класса: нормативные, экспертные и статистически-математические.

Возможны их комбинации. Например, модель оценки рисков с учётом взаимодействия рисковых событий предполагает, как математическую модель, так и экспертные оценки частных параметров.

Представить все модели частных рисков невозможно и нецелесообразно в рамках нашей с вами дисциплины. Их большое количество и можно найти в специальной литературе.

Для практических целей следует разрабатывать различные модели и методики в рамках реализации информационной технологии оценки безопасности конкретного хозяйствующего субъекта в конкретных условиях его функционирования и пополнять библиотеку моделей и методик в процессе эксплуатации этой технологии. Далее, в качестве иллюстрации рассмотрены наиболее актуальные математические модели частных рисков применительно к проектам. Методы экспертного оценивания описаны в соответствующей тематической литературе.

Для наукоёмких, новаторских проектов высока степень неопределённости успешности результатов, объёма затрат и других проектных параметров. Это приводит к тому, что проекты, как правило, осуществляются поэтапно. По результатам выполнения каждого из этапов принимается решение о возможности и целесообразности дальнейших работ.

Возникшие проблемы реализации проекта, включая те, которые вызваны внешними угрозами, в том числе макроэкономического характера, рассматриваются как рисковые события, которые можно считать факторами реализации проекта. В зависимости от этих факторов может быть оценена функция распределения ущерба, который в зависимости от принятия решения по проекту и требований к его выполнению может описываться следующими показателями:

* величина потерь, т. е. зря потраченный объём финансов, или недополученное финансирование на следующие этапы в случае прекращения проекта;
* увеличение затрат на проект;
* увеличение сроков реализации проекта, что может вести и к штрафным санкциям, и к имиджевым потерям (административным наказаниям), и к потере выручки (по коммерческим проектам).

Ниже будут рассмотрены частные модели оценки ущерба за счёт зря потраченных средств, потери финансирования при прекращении проекта, оценки увеличения затрат и оценки увеличения сроков.

Оценка риска зря потраченных средств

Обычно процесс выполнения проекта разбит на несколько этапов, который имеет в модели свой условный порядковый номер. В каждый из этапов закладывается размер расходов. Модель строится на использовании показателя вероятности успешного выполнения каждого из этапов, в результате чего определяется вероятность успешного выполнения всего проекта. Так же эта модель предусматривает расчет вероятности срыва выполнения всего проекта либо после одного из этапов.

В том случае, если финансирование проекта выполняется за счёт внутренних ресурсов необходимо рассчитать ожидание потерь в результате прекращения проекта. Для этого используется математическая модель, где применяются:

- показатель затрат на выполнение определенного этапа проекта;

- возможный положительный результат за счёт капитализации или реализации результатов интеллектуальной деятельности, полученных на каждом этапе.

Такие оценочные расчеты целесообразно проводить до начала проекта.

В действительности необходимость оценки возможного ущерба может возникать после некоторого этапа проекта в результате возникновения новых факторов вследствие рискового события. Для этого рассчитывается оценка возможного ущерба из-за срыва проекта на следующем этапе.

Переоценка вероятностей в результате рискового события приводит к переоценке ожидаемого ущерба на рассматриваемом периоде оценки безопасности. Среднеожидаемый ущерб за счёт зря потраченных ресурсов оценивается уже после выполненного этапа.

Оценка риска потери финансирования

Если финансирование осуществляется из внешних источников, то срыв проекта приводит к прекращению дальнейшего финансирования и сокращению входного денежного потока. В этом случае ущерб в период оценивания безопасности рассчитывается аналогичным образом как в случает финансирования за счет внутренних ресурсов.

Оценка риска удорожания проекта

Для данной модели оценки риска используется показатель удорожания проекта на одном из этапов; сами этапы проектов, каждый из которых планируется выполнять в период, на котором оценивается безопасность.

Если факторы, влияющие на удорожание, механизм и степень их влияния предопределены (детерминированы), то удорожание может быть вычислено путём прямого пересчёта.

В более сложных случаях, когда выделяются варианты действия факторов, удорожание может быть вычислено как математическое ожидание (т.е. среднее значение случайной величины) результатов действия таких вариантов.

Когда имеет место аналитическая неопределённость воздействия рискового события, повлекшего факторы удорожания, подходящей аналитической структурой удорожания на каком-либо этапе может быть распределения величины удорожания:

Удорожание проекта в общем случае неопределенности определяется удорожанием различных работ, услуг, продукции поставщиков по различным причинам, в том числе в результате ошибок прогнозирования их стоимости, т. е. в результате некоторых первичных причин. Общее удорожание определяется набором таких первопричин. Предполагая их появление независимым друг от друга, можно считать, что их количество распределено по закону Пуассона. Соответственно, по этому же закону будет распределено значение удорожания, если полагать, что каждая первопричина влечёт некоторое усреднённое значение удорожания.

Оценка риска задержки выполнения проекта

Среднеожидаемая задержка выполнения проекта вычисляется аналогично. Эти расчёты проводятся, если существует возможность рассчитать конкретную задержку из-за конкретных факторов, например, практически достоверно прогнозируемой задержки поставок.

Если задержка выполнения проекта влечёт какие-либо потери и, например, недополученная прибыль, дополнительные расходы (аренда, зарплата, др.), штрафы и т. п., то среднеожидаемый ущерб.

Здесь и должно вычисляться с учётом дисконтирования. При этом ставка дисконтирования может назначаться в соответствии с банковской кредитной ставкой, нормативной рентой на капитал предприятия или исходя из других соображений, вытекающих из финансовой политики предприятия.

* 1. Механизм оценки безопасности предприятия в режиме использования автоматизированной информационной технологии

Отличительной особенностью предложенной методологии является её ориентация на учёт конкретной специфики деятельности, отказ от простых, обобщённых до примитивности подходов в пользу более тонких многоаспектных моделей и методик, учитывающих взаимосвязи объектов проблемы безопасности, позволяющих осуществлять прогноз.

В данной методике используются глубинные особенные знания экспертов по множеству узких вопросов и, в конечном итоге, учитывать непредсказуемость процессов, влияющих на обеспечение безопасности, их масштабируемые и немасштабируемые результаты. учитывается вероятностная и невероятностная недетермированность (т.е. несколько путей обработки одних и тех же входных [данных](https://ru.wikipedia.org/wiki/%D0%94%D0%B0%D0%BD%D0%BD%D1%8B%D0%B5)) различных явлений и взаимосвязей.

Применение такой методологии ввиду необходимости оперирования большим количеством исходных данных и алгоритмов их обработки предполагает использование автоматизированной информационной технологии, снабжённой дружественным интерфейсом, системой управления знаниями, банком данных и знаний, библиотекой моделей, прецедентов и ситуаций, имеющей разнообразные возможности адаптации к конкретному объекту защиты, предлагающей возможность анализа и оценки состояния безопасности в режиме сценариев.

Автоматизированная информационная технология позволяет реализовать имитационное моделирование воздействия угроз, образования ущербов и их механизм распространения.

Имитационное моделирование

Имитационная модель позволяет использовать всю доступную информацию вне зависимости от формы представления и степени формализации, что приобретает особую значимость при отсутствии надёжной статистической базы и достоверных знаний о структуре исследуемых объектов, а также когда они не могут быть адекватно описаны только с помощью аналитических математических моделей.

Имитационное моделирование позволяет исследовать сложные производственные системы, подверженные разным угрозам. Не существует аналитических моделей поиска оптимальных структурных решений, поскольку структура - это форма, а форма принципиально не может быть описана числом. Ввиду уникальности подобных решений для крупных предприятий и их интегративных структур не может здесь помочь и статистика. В связи с этим для анализа влияния реструктуризации на различные аспекты функционирования отрасли, предприятия, включая их безопасность, невозможно найти достойную замену имитационному моделированию.

Для имитационного моделирования широко применяются потоковые модели, представляющие функционирование предприятия в виде схем финансовых и материальных потоков, а также потоков рисковых событий и их последствий. Имитационные потоковые модели предприятия, включая технологические и финансовые потоки, могут быть разработаны в одной из широко используемых ныне программных сред структурно-функционального или потокового моделирования.

Имитационная модель может воспроизводить динамику функционирования хозяйствующего субъекта за несколько базовых периодов и генерировать многочисленные варианты реализации для каждого периода.

После того, как модель построена, происходит генерирование сценариев развития системы для различных неблагоприятных событий. На этом этапе вычисляются численные оценки, как отдельных видов риска, так и интегрального значения по всему предприятию.

Имитационная модель безопасности предприятия позволяет получать интегральные оценки риска.

На основе имеющихся ретроспективных, расчётных и экспертных данных, а также информации о характере функционирования системы предприятия можно задать основные факторы риска - рисковые события и ущербы в виде псевдослучайных величин с заданным распределением. Затем в результате многократного применения модели на данном массиве данных получаются расчётные значения частных рисков, либо интегрального на рассматриваемом временном интервале.

Уровень доверия (вероятности попадания значений риска в доверительный вариант) при этом выбирается исходя из удовлетворения интересов предприятия.

Полученные в результате имитационного моделирования численные оценки риска могут служить критериями оценки эффективности управления рисками и выбора оптимальных решений.

Во многих ситуациях, характеризующихся сложностью исследуемых процессов и недостатком надёжной информации, имитационное моделирование, является единственным действенным инструментом оценки безопасности.

Идентификация угроз и рисковых событий

Идентификация угроз осуществляется в результате мониторинга угроз и рисковых событий. Мониторинг проводится на основе рубрикатора угроз и рисковых событий, который содержится в базе знаний угроз и рисковых событий. Этот перечень является тематическим рубрикатором для осуществления мониторинга. В каждом конкретном случае угроза и рисковое событие имеют конкретное содержание. Кроме того, следует учитывать, что указанный перечень не является исчерпывающим, поскольку невозможно априорно учесть все возможные обстоятельства и сценарии нанесения ущерба ресурсам крупного хозяйствующего субъекта.

При выявлении угроз или возникновении рисков, не предусмотренных рубрикатором, они индексируются и вносятся в базу данных.

Для оценки безопасности на некотором рассматриваемом интервале времени необходимо учитывать не только возникшие рисковые события, но и прогнозируемые с некоторой вероятностью.

Для мониторинга используются внутренние и внешние источники информации и данных.

К внутренним источникам относятся система плановой отчётности о состоянии различных объектов, ресурсов, отношений и процессов, а также оперативные сообщения, как регламентированные, так и нерегламентированные от ответственных лиц или любых лиц. Кроме того, при наличии технической возможности используются сигналы в различной форме, параметрическая, звуковая и видео информация от технических систем контроля, наблюдения, установленных на объектах встроенных в технологические циклы и внутренние телекоммуникационные системы.

Внешние источники информации, как правило, предоставляют сведения о состоянии экономики, глобальных и региональных рынках, достижениях научно-технического прогресса, действиях и решениях государственных регуляторов, социально-экономической обстановке в регионе деловых интересов, военно-политической обстановке, состоянии и намерениях поставщиков и потребителей. К внешним источникам относятся средства массовой информации, глобальные телекоммуникационные сети, деловые контакты, информация государственных и муниципальных органов, отраслевые издания, в том числе электронные. Для их обработки целесообразно использовать автоматизированные технологии обработки потоков неструктурированной информации.

Лекция 9 «Модель проверки потенциала обеспечения экономической безопасности предприятия»

Проверка потенциала обеспечения ЭБ отражает возможности обеспечения нейтрализации угроз, и может быть использована для оценки безопасности в качестве более простой методологии. Такая проверка выявляет возможности для снижения ущербов, когда применение выше названных методик и моделей по каким-либо причинам затруднительно.

Проверка ПОТЕНЦИАЛА ОБЕСПЕЧЕНИЯ ЭБ должна отвечать на три вопроса:

* *Какие силы и средства используются или привлечены для обеспечения безопасности?*
* *Достаточен ли уровень ПОТЕНЦИАЛА ОБЕСПЕЧЕНИЯ ЭБ по отдельным составляющим (компонентам)?*

К таким компонентам относятся:

* основные и оборотные производственные фонды;
* товарно-материальные ценности и финансовые ресурсы;
* непроизводственные фонды;
* кадровый потенциал: наличие, квалификация;
* качество коллектива: идентификация интересов работников с интересами предприятия, атмосфера сотрудничества и творчества, дисциплина;
* информационные ресурсы, в том числе и интеллектуальная собственность;
* внутренний организационный ресурс: бизнес-процессы и их регламентация, система мотивации, цели, миссия, этический кодекс, традиции предприятия и т. п.;

Миссия - это генеральная цель, выражение основного смысла существования и философии компании. Миссия показывает то, к чему компания стремится, показывает то, что руководство хотело бы достичь. Вся дальнейшая работа зависит от выбора именно миссии, исходя из ее формирования ставится цель, задачи, разрабатываются планы по их достижению.

Этический кодекс представляет собой свод разработанных на предприятии правил работы и каких-то норм поведения, которым должен следовать каждый сотрудник компании, для того, что бы создать систему взаимоотношений и корпоративных ценностей в результате приводящей к эффективной деятельности и долгосрочному успеху компании.

* гудвилл: клиентская база (долговременные договора и контракты), деловые связи, положительная репутация в обществе и государственных органах.
* *Каков интегральный уровень ПОТЕНЦИАЛА ОБЕСПЕЧЕНИЯ ЭБ?*

Ответы на первые два вопроса могут служить основой для анализа состояния безопасности хозяйствующего субъекта и подготовки предложений по её укреплению.

Интегральная оценка состояния ПОТЕНЦИАЛА ОБЕСПЕЧЕНИЯ ЭБ может быть использована в тех случаях, когда требуется рационально распределить ресурсы, выделенные на развитие сил и средств обеспечения безопасности.

В этом случае интегральная оценка является целевой функцией, а ресурсы следует израсходовать, или распределить между компонентами ЭБ таким образом, чтобы обеспечить её максимизацию. Кроме того, такая оценка может быть полезна для характеристики общей картины состояния сил и средств обеспечения безопасного существования, анализа её динамики и аргументации предложений по выделению средств для укрепления состояния безопасности.

Проверка ПОТЕНЦИАЛА ОБЕСПЕЧЕНИЯ ЭБ предполагает объективное описание существующих реалий, для чего необходимо, прежде всего, составить полный перечень позиций, подлежащих рассмотрению, и скрупулёзно их заполнить. Для этого может быть использована «Карта обследования ПОТЕНЦИАЛА ОБЕСПЕЧЕНИЯ ЭБ». Карта не может быть исчерпывающей, поскольку существует большое количество различных сил и средств для обеспечения безопасности и к каждому конкретному объекту защиты эти силы и средства должны быть соответствующим образом адаптированы.

Карта служит для характеристики наличных сил и средств, для оценивания обеспечиваемого ими потенциала существования, а также для рекомендаций эксперту: каким образом лучше собрать сведения о потенциале обеспечения ЭБ. Проверка проводится по множеству показателей, которые отражают наличие организационных структур, регламентирующих документов, технических средств контроля и защиты и т.д.

Для достижения большей объективности целесообразно к оцениванию привлекать нескольких специалистов и затем выводить групповые экспертные оценки.

Для интегрального оценивания состояния ЭБ можно использовать два вида оценок - абсолютные и относительные.

Абсолютная оценка отражает уровень оснащения предприятия силами и средствами обеспечения существования в сравнении с максимальным уровнем, когда все численные значения оценки компонент ОБЕСПЕЧЕНИЯ ЭБ принимают значения равные «1». Такая оценка не учитывает ни требования к ПОТЕНЦИАЛУ ОБЕСПЕЧЕНИЯ ЭБ, ни уровень угроз.

Относительная оценка, наоборот, призвана соотнести состояние ОБЕСПЕЧЕНИЯ ЭБ с некоторым требуемым уровнем и поэтому имеет большее практическое значение.

Для определения требуемого уровня ПОТЕНЦИАЛА ОБЕСПЕЧЕНИЯ ЭБ возможны три подхода:

1. требования определяются на основе анализа угроз и рисков, в том числе с учётом их прогноза - объективный подход;
2. требования выдвигаются руководством предприятия - это субъективный подход;
3. требования диктуются положениями правовой нормативной базы - нормативный подход.

Формулирование требуемого уровня ПОТЕНЦИАЛА ОБЕСПЕЧЕНИЯ ЭБ при субъективном подходе предполагает выяснение и описание образа состояния обеспечения безопасного существования в представлении руководителей. Сложность решения этой задачи зависит от того, насколько ясно руководство представляет себе этот образ, а также, с практической точки зрения, насколько оно доступно для интервьюирования специалистами, проводящими проверку. Если руководитель имеет сложившееся мнение о качественных параметрах сил и средств обеспечения безопасности, то задача сводится к формализованному описанию этого мнения и сопоставлению ПОТЕНЦИАЛА ОБЕСПЕЧЕНИЯ ЭБ с требованиями руководства. Для решения таких задач существуют хорошо разработанные методы, один из которых описан ниже. Корректность решения определяется тем, насколько адекватно представление ЛПР о требуемых параметрах ПОТЕНЦИАЛА ОБЕСПЕЧЕНИЯ ЭБ объективному положению вещей.

На практике руководитель не всегда имеет правильное представление об объективных потребностях обеспечения безопасности, соотносимых с необходимыми для их удовлетворения затратами. Следует отметить, что руководитель хозяйствующего субъекта зачастую выдвигает требования, руководствуясь аналогиями с подобными производственными объектами, соображениями имиджа и т. д., что не всегда хорошо отражает объективные потребности. В силу этого возникает непростая задача подготовки мнения руководства на основе, если не научной обработки, то хотя бы экспертного анализа имеющихся данных об уровне угроз.

Нормативный подход к определению требований к ОБЕСПЕЧЕНИЮ ЭБ заключается в том, что уровень обеспечения безопасности и некоторая совокупность мер и способов диктуются требованиями нормативной правовой базы.

Это касается, в частности, предприятий, использующих радиоактивные, взрывчатые, сильнодействующие ядовитые вещества и т. п., работающих со сведениями, составляющими служебную и(или) государственную тайну, прибегающие к услугам вневедомственной охраны России и др. Так, органы вневедомственной охраны России берут под свою опеку лишь те объекты, которые оборудованы в соответствии с требованиями, установленными в нормативных документах об оказании услуг по охране коммерческим организациям. К предприятиям, участвующим в выполнении государственного оборонного заказа, предъявляются требования уполномоченных государственных органов, отраслевые требования в части, касающейся обеспечения защиты от несанкционированного доступа, защиты ТМЦ, финансовой устойчивости и т.д.

Выбор подхода к определению требуемого уровня ПОТЕНЦИАЛА ОБЕСПЕЧЕНИЯ ЭБ осуществляется исходя из особенностей, присущих каждому конкретному случаю проведения проверки, и зачастую является комбинацией трёх указанных подходов, диктуемой конкретными условиями деятельности и уровнем информационно-аналитической проработки вопросов обеспечения его безопасного существования.

Для численной интегральной оценки ПОТЕНЦИАЛА ОБЕСПЕЧЕНИЯ ЭБ используется показатель степени соответствия уровня защиты предъявляемым требованиям. В расчёте участвует коэффициент важности оснащённости, который отражает «цену вопроса» укрепления выбранной компоненты ОБЕСПЕЧЕНИЯ ЭБ и в связи с этим должен определяться на основе риска, для предотвращения которого служит (предназначена) рассматриваемая компонента. Однако практически сопоставить все компоненты с оценками рисков весьма трудоёмко и зачастую невозможно.

Во-первых, отношения между множеством рисков и множеством компонент ОБЕСПЕЧЕНИЯ ЭБ не являются парными отношениями, т. е. один риск может быть связан с несколькими компонентами и, наоборот, состояние некоторой компоненты может повлечь несколько рисков.

Во-вторых, ПОТЕНЦИАЛА ОБЕСПЕЧЕНИЯ ЭБ по своей природе влияет на потенциальные риски, которые с трудом поддаются объективной оценке по финансовому показателю (или какому-либо другому универсальному физически измеряемому показателю).

Состояние (уровень оснащённости) компоненты должно быть таким, которое позволит нейтрализовать все рисковые события в сфере «ответственности» компоненты кроме тех, вероятность появления которых меньше некоторого заданного значения %.

**Лекция 10. «Отраслевые особенности предприятий при обеспечении экономической безопасности»**

**10.1. Влияние отраслевых особенностей**

Предприятия различных отраслей различаются в первую очередь удельным весом тех или иных этапов в производственном цикле.

Так, в основе деятельности предприятий промышленности лежит производство одних товарно-материальных ценностей из других товарно-материальных ценностей.

У предприятий торговли этап производства как преобразования ТМЦ из сырья в продукцию практически отсутствует. Основу деятельности торгового предприятия составляют закупка, хранение и сбыт товаров. Определенный вес имеют логистика и подразделения, занимающееся упаковкой, фасовкой и т.д.

Строительные предприятия не производят и не продают товары. Результатом строительных работ являются различные объекты - здания и сооружения различного назначения, дороги, мосты и пр. Закупаемые ТМЦ преобразуются в результат выполнения работ непосредственно на месте расположения объекта строительства.

У предприятий, оказывающих услуги, поток ТМЦ в обороте гораздо меньше, чем у торговых или производственных предприятий. Основными расходами являются заработная плата персонала и расходы на содержание офиса. У предприятий связи поток ТМЦ в обороте весьма невелик, однако основными расходами являются расходы на приобретение и содержание основных средств. У транспортных предприятий помимо расходов на приобретение и содержание основных средств существенными являются расходы на ГСМ.

Отличия от предприятий по отраслям, характеризующие отраслевую специфику предприятий той или иной отрасли, можно классифицировать по следующим группам:

- правовое регулирование в отрасли;

- сложившаяся практика хозяйственной деятельности;

- организационные особенности предприятий;

- технологические особенности производства.

**10.2. Промышленность**

Деятельность промышленных предприятий в ряде случаев регламентируется и контролируется государством. Многие виды продукции подлежат обязательной сертификации.

Обеспечение нормальной производственно-хозяйственной деятельности предприятий промышленности можно представить как совокупность мероприятий по обеспечению уровня платежеспособности промышленных предприятий,   ликвидности их  оборотных средств, повышению качества планирования и осуществления финансово-хозяйственной деятельности предприятий по всем направлениям стратегического и оперативного планирования,  и управления,  в том числе в вопросах технологического, информационного и кадрового потенциалов.

Обеспечение экономической безопасности промышленных предприятий необходимо рассматривать как процесс прогнозирования и предотвращения всесторонних ущербов от негативных воздействий на их экономическую безопасность по различным аспектам финансово-хозяйственной деятельности.

Промышленные предприятия, составляющие промышленный комплекс региона, действующие в условиях рыночной экономики, представляют собой, как правило, сложный, инженерно-технический комплекс,

Промышленные предприятия так же являются собственниками технической и коммерческой информации, интеллектуальной собственности, торговой марки, несанкционированное использование которых несет в себе ущерб финансовому положению конкретного промышленного предприятия, что не замедлит сказаться на той или иной составляющей экономической безопасности промышленности региона в целом.

Часто крупные и средние предприятия являются так называемыми градообразующими предприятиями. Ряд предприятий так или иначе связан с социальной сферой, с городским и коммунальным хозяйством. Деятельность промышленных предприятий всегда находится под пристальным вниманием государственной и местной властей. Это влечет за собой ряд угроз:

- использование административных возможностей для получения выгоды;

- использование административных возможностей для усиления давления со стороны конкурентов либо так называемых рейдеров;

- рост влияния административных рисков. Здесь и изменение законодательства, иных нормативных и регулирующих документов, смена сотрудников администрации и контролирующих органов, изменение их позиции в отношении промышленного предприятия в силу каких-либо причин;

- попадание предприятия в зависимость от должностных лиц либо посредников, в том числе от своих сотрудников.

Кроме того, для большинства промышленных предприятий характерна специализация в каком-либо направлении. Характер производства не позволяет быстро в случае необходимости перейти на выпуск другой продукции. Это также формирует специфические угрозы:

- обострение конкуренции на рынке продукции, производимой узкоспециализированным предприятием;

- обострение конкуренции на ограниченном географическом пространстве, существенно для случаев, когда перевозка продукции приводит к ее существенному удорожанию для потребителя (сырьевая промышленность, производство ряда строительных материалов);

- падение спроса на выпускаемую продукцию, обусловленное объективными причинами;

- недобросовестная конкуренция во всех ее проявлениях;

- монополизация рынка;

Производство является технически сложным процессом, что формирует следующие угрозы:

- нанесение ущерба основным средствам, технике, порча ТМЦ;

- нанесение ущерба персоналу (производственный травматизм);

- угроза появления брака;

- угроза появления брака, обусловленного низким качеством поставляемых предприятию и используемых им сырья и комплектующих;

Даже небольшой брак или незначительное несоблюдение технологий может впоследствии привести к серьезным финансовым потерям.

Производство имеет также следующие особенности.

Проблема персонала. Многие промышленные предприятия в силу особенностей технологического процесса могут использовать труд только высококвалифицированных специалистов. В случае их ухода, а еще хуже перехода к конкурентам может возникнуть дефицит квалифицированного персонала. В годы перестройки была подорвана система профессионального технического образования. Престиж инженерных специальностей был невысок еще в советское время, когда инженер часто имел более низкий оклад, чем рабочий. Теряется преемственность, производственная культура. Вкладывать средства в подготовку кадров могут позволить себе далеко не все предприятия, к тому же такие вложения могут дать результат только по истечении достаточно длительного времени.

Как правило, предприятия являются локализованными и физически трудно перемещаемыми объектами. Выбор места расположения обусловлен наличием ресурсов и близостью к району сбыта, Перевод предприятия с одного места на другое обычно связан с высокими затратами и на практике производится в самых крайних случаях. В связи с этим:

- чрезвычайную важность приобретают отношения с органами местной власти;

- необходим постоянный мониторинг окружающей обстановки.

Учет бухгалтерский и управленческий, а также аудит имеют свою специфику. Как следствие, возникают следующие угрозы:

- связанные с неквалифицированным ведением учета;

- связанные с неквалифицированным проведением аудита.

Система обеспечения экономической безопасности промышленных предприятий, в зависимости от конкретных условий (масштабы финансово-хозяйственной деятельности, объемы производства, территориальные особенности.  состояние основных фондов, кадровый потенциал и т.д.) должна иметь определенные средства собственного обеспечения, опираясь на которые, она будет способна выполнять свои задачи, а также нормативно-правовое обеспечение, куда входят нормы деятельности служб организации, средства, методы, нормативные документы, определяющие статус службы экономической безопасности и требования, которые являются обязательными в рамках сферы действия

Все это обуславливает ряд отраслевых особенностей экономической безопасности промышленного предприятия. СБ промышленного предприятия помимо осуществления обычных мероприятий должна уделять особое внимание:

- мониторингу отношений собственных сотрудников с представителями органов власти, потенциальными заказчиками либо их представителями, распорядителями заказов;

- мониторингу отношений конкурентов, в том числе возможных, с потенциальными заказчиками либо их представителями, распорядителями заказов, представителями органов власти, а также с акционерами предприятия;

- мерам противодействия недружественным поглощениям;

- строгому сохранению коммерческой тайны внутри предприятия, охраны технологий;

- борьбе с угрозами внутреннего мошенничества;

- персоналу - как собственному, так и контрагентов;

- использовать специальные методические рекомендации, разработанные в соответствии со спецификой каждого конкретного предприятия.

Однако обеспечение экономической безопасности промышленных предприятий, не должно,  по своей сути,  сводить данную работу лишь к организации и проведению отдельных мероприятий, а должно представлять собой непрерывный, целенаправленный процесс требующий:

-         постоянного прогнозирования возможных угроз;

-         обоснования и реализации эффективных форм и методов создания, совершенствования и развития системы экономической безопасности предприятий;

-         непрерывного контроля и управления системой;

-         комплексного, эффективного использования имеющихся средств защиты всех элементов производственно-хозяйственной системы;

-         соответствующего требованиям уровня профессиональной подготовки персонала промышленных предприятий.

**10.3. Строительство**

Деятельность строительных предприятий на многих уровнях ФХД ничем не отличается от деятельности предприятий других отраслей экономики, в частности, промышленных. Но, безусловно, строительство имеет определенные отличия, хотя они не столь велики.

Деятельность строительных предприятий регламентируется и контролируется государством. Кроме этого она является лицензируемой.

Начало процесса строительства также контролируется государством через процедуры получения разрешения на проектирование, строительство. Требуется согласование ряда служб. Эти же службы ведут контроль самого процесса строительства; Госсанэпиднадзор, Госгортехнадзор, Госпожнадзор, Архитектурно-строительный надзор, Административно-техническая инспекция и пр. Кроме того, органами власти в ряде случаев устанавливается либо рекомендуется и порядок ценообразования в строительной отрасли.

Таким образом, деятельность строительного предприятия в значительной мере зависит от отношений со структурами государственной и местной властей. Это влечет за собой ряд угроз;

- использование административных возможностей для получения выгоды;

- использование административных возможностей для давления со стороны конкурентов;

- рост влияния административных рисков. Здесь и изменение законодательства, иных нормативных и регулирующих документов, смена сотрудников администрации и контролирующих органов, изменение их позиции в отношении строительного предприятия в силу каких-либо причин;

- попадание предприятия в зависимость от должностных лиц либо посредников, в том числе от своих сотрудников.

Кроме того, для большинства строительных предприятий строительство носит позаказный характер. Характер выполняемых строительных работ часто не позволяет заранее точно определить конечную стоимость работ по объекту (заказу). Это также формирует специфические угрозы;

- обострение конкуренции на ограниченном рынке заказов;

- обострение конкуренции на ограниченном географическом пространстве;

- недобросовестная конкуренция во всех ее проявлениях;

- монополизация рынка;

- коррупционные отношения при распределении государственных и муниципальных заказов;

- явления коммерческого подкупа при получении заказов и распределении субподрядов, так называемые откат и обратный откат;

- внутреннее мошенничество.

Строительство является технически сложным процессом, что формирует следующие угрозы:

- нанесение ущерба объекту строительства, технике, порча ТМЦ;

- нанесение ущерба персоналу (производственный травматизм);

- угроза появления брака, в том числе скрытого, по работам, выполненным силами субподрядчиков, а также обусловленного низким качеством использованных стройматериалов;

- угроза появления брака, в том числе скрытого, по работам, выполненным собственными силами;

- угроза появления брака, обусловленного низким качеством работы проектных организаций, а также генподрядчиков;

- даже небольшой брак или незначительное несоблюдение технологий может впоследствии привести к серьезным финансовым потерям.

Проблема персонала. Многие строительные предприятия привлекают ряд сотрудников, обычно строительных рабочих без должного оформления. Зарплата им, как правило, выплачивается так называемым черным налом, выдача ее неоформленным сотрудникам ничем не гарантирована и остается вопросом добропорядочности работодателя. Размер зарплаты таких сотрудником существенно меньше зарплаты нормальных штатных сотрудником. При этом такие сотрудники зачастую недостаточно квалифицированы, не имеют регистрации, разрешения на работу, медицинской страховки, нормальных условий для питания, проживания, отдых.

Проблема неоформленного персонала несет ряд угроз:

- ухудшение криминогенной обстановки на объекте и вокруг него;

- падение качества выполняемых работ;

- повышение травматизма на объекте;

- повышение угрозы хищения ТМЦ на объекте;

- санкции уполномоченных органов, в случае обнаружения фактов такого найма;

- необходимость проведения незаконных финансовых операций для получения официально неучтенных денежных средств в наличной форме для оплаты труда, со всеми финансовыми и прочими рисками по таким операциям.

Что характерно, почти все эти угрозы появляются как при использовании неоформленных сотрудников самим предприятием, так и его контрагентами: генподрядчиком, субподрядчиком.

Сезонность и аритмичность работ в строительства повышает непроизводственные издержки. Порождает следующие угрозы:

- фактор погодных рисков;

- нанесение экономического ущерба вследствие ошибок планирования;

- также усугубляет проблему персонала: предприятие вынуждено либо содержать большой штат сотрудников с вынужденными простоями в периоды с низкой загрузкой, либо привлекать дополнительных сотрудников в периоды с высокой нагрузкой.

Удаленность и территориальная разобщенность объектов. Порождает следующие угрозы:

- падение управляемости процессом строительства на объекте;

- рост транспортных рисков;

- хищение ТМЦ на приобъектных складах и объектах.

Что касается бухгалтерского, управленческого учета и аудита – та же специфика, что и на промышленных предприятиях, то есть риск возникновения угроз, связанных с неквалифицированным ведением учета; и неквалифицированным проведением аудита.

Характерными способами совершения большинства преступлений экономического характера и нарушений законодательства при осуществлении строительной деятельности являются:

- не оприходование наличной выручки за продукцию предприятия реализуемую через доверенных лиц, документальное занижение выручки при реализации построенных объектов;

- включение подрядчиком в затратную часть сметы оплаты по фиктивным договорам за работы и услуги, которые в действительности не выполнялись, а также проведение финансовых взаимозачетов без отражения по счетам;

- списание сырья и материалов строительной фирмы в объемах, заведомо превышающих необходимые, а также включение в затратную часть сметы стоимости материалов заказчика;

- использование при проведении коммерческих операций подложных документов, накладных на стройматериалы, фиктивных закупочных и иных документов, оформленных на подставных лиц;

Кроме того, на строительных объектах хищения совершаются путем списания стройматериалов свыше установленных норм либо укрытия от учета неизрасходованных материалов, а также необоснованное списание стройматериалов на потери в связи, с якобы устранением брака, на порчу, потери при перевозке и хранении.

Также отмечено, что правонарушения и преступления в сфере строительства характеризуются чрезвычайно высоким уровнем латентности в силу специфики отрасли.

Отраслевые особенности экономической безопасности строительного предприятия должны быть учтены службой безопасности строительного предприятия при организации эффективной системы экономической безопасности. В частности,:

- контроль субподрядных отношений;

- борьба с угрозами внутреннего мошенничества;

- контролю качества проводимых строительных работ;

- использование специальные методические рекомендации, положений, стандартов, разрабатываемых государственными органами для строительной отрасли.

**10.4. Транспорт и связь**

Для этих отраслей, оказывающих услуги, в целом характерна следующая особенность. При оказании услуг связи (телефон, телеграф), как правило, не происходит никакого существенного физического перемещения или преобразования товарно-материальных ценностей. В результате факт оказания услуг часто не имеет материального подтверждения. При оказании услуг в сфере транспорта происходит перемещение товарно-материальных ценностей или пассажиров, но спустя некоторое время после транспортировки факт оказания услуг или же их объем также трудно определить.

Поэтому связь и транспорт являются отраслями, близкими по идеологии нанесения ущерба предприятиям данных отраслей экономики и достаточно легким получением выгоды.

На транспорте основными угрозами являются осуществление неучтенных услуг, а также списание товарно-материальных ценностей и иных ресурсов (ГСМ, электроэнергия, ремонт, запчасти) сверх обусловленных производственной необходимостью.

В сфере связи наиболее характерными являются следующие угрозы:

- административные риски;

- оказание неучтенных услуг («неучтенный трафик»).

Трафик - это фактически объем оказанных услуг связи. Технологические особенности предприятий отрасли приблизительно следующие.

Информация об оказанной услуге связи (разговоре, переданной информации, сообщении, пр.) накапливается в специальной программе, управляющей средствами связи. Далее эта информация чаще всего передается в другую программу, где происходит учет расчетов с потребителями оказанной услуги. Существуют и другие алгоритмы предоставления услуг связи. Например, перед предоставлением услуги связи программа управления средствами связи может делать запрос - оплачена ли запрашиваемая услуга абонентом или нет. После тарификации информация поступает в базу данных, откуда ее получают бухгалтерия и соответствующие подразделения предприятия связи (клиентский отдел, например).

Важным здесь является наличие достаточно длинной цепочки передачи и обработки информации, объективно обусловленной технологией процесса предоставления услуг связи. При передаче информации от программы к программе в силу ряда причин могут происходить искажения передаваемой информации.

В случае, если впоследствии невозможно абсолютно достоверно установить для каждого из звеньев этой цепочки входящую и исходящую информацию, то это обстоятельство, вероятно, будет использовано для нанесения ущерба предприятию. (Пример с предприятием связи был приведен выше.) Для получения выгоды, скорее всего, будет использована структура-посредник. В отрасли связи таким посредником может быть дилер, виртуальный оператор, пр.

**10.5. Торговля**

Торговля как вид деятельности имеет свои характерные особенности. В торговле как в отрасли товарно-материальные ценности в цикле «товар - деньги - товар» претерпевают, наименьшие изменения. Возможные изменения - это фасовка, придание товарного вида, предпродажная подготовка. Известно, что торговля бывает двух видов - оптовая и розничная.

10.5.1. Оптовая торговля

Покупателями для предприятий оптовой торговли, как правило, выступают (мелко)оптовые предприятия торговли, предприятия розничной торговли, предприятия других отраслей экономики. Товар отгружается относительно крупными партиями, Доставка товара может осуществляться как силами покупателя, так и силами продавца или силами третьей стороны по договору с продавцом или покупателем.

Для хранения, затаривания, отгрузки товара обычно используется склад. Склад может быть собственный или арендуемый. Также возможны варианты размещения товара на специализированных складах, их использование может быть обусловлено как особенностями финансово-хозяйственной деятельности, так и требованиями законодательства (например, акцизный склад, таможенный склад). Также могут иметь место прямые поставки, при которых товар, минуя склад торговой организации, поступает со склада поставщика непосредственно на склад покупателя.

Производственный цикл оптовых торговых предприятий обычно выглядит следующим образом (при ряде допущений об особенностях финансово-хозяйственной деятельности предприятий торговли):

- решение о закупке товара;

- заключение договора на поставку товара в адрес торговой организации;

- оплата товара продавцу;

- отгрузка продавцом товара;

- доставка товара от склада продавца (производителя) на склад предприятия;

- разгрузка товара и его приемка, составление актов приема-передачи;

- оприходование товара;

- размещение товара на складе и его хранение;

- принятие решения о продаже товара;

- заключение договора на поставку товара торговой организацией покупателю;

- получение предоплаты;

- отгрузка товара и его списание;

- доставка товара покупателю;

- разгрузка товара покупателем и его приемка, подписание накладных или составление актов приема-передач и.

На каждой из этих фаз может наноситься ущерб предприятию и, соответственно, существуют угрозы экономической безопасности.

Некоторые из критериев нормальности для двух первых этапов вышеприведенной последовательности:

Решение о закупке товара можно считать правильным, если товар закупается по цене не выше рыночной и может быть перепродан с выгодой в течение разумного времени в количестве, соответствующем закупке.

Соответствующие угрозы:

- товар закупается в большем или меньшем количестве, чем необходимо;

— товар закупается по цене более высокой, чем рыночная цена.

Договор на поставку можно считать нормальным, если его существенные условия соответствуют технологии работы торгового предприятия и соответствуют сложившимся обычаям хозяйственной деятельности. Для торговых предприятий можно отметить следующие существенные условия:

I. Сроки поставки. Вообще, срок поставки для договора поставки с юридической точки зрения является существенным условием. Без его указания заключенный договор вообще не является договором поставки. Кроме того, сроки поставки должны обеспечивать торговому предприятию возможность планировать свою деятельность и эффективно управлять запасами. Предусмотренные договором отклонения в сроках поставки должны быть таковы, чтобы не сказываться на бесперебойном обеспечении торгового предприятия товаром. Соответственно договором должны быть предусмотрены эффективные санкции за срыв сроков поставки.

Способ доставки товара. Транспортные издержки, разгрузоч-но г- погрузочные расходы составляют весьма существенную часть себестоимости получаемого товара. Кроме того, при доставке товара могут происходить хищения части товара, его порча. При перегрузках может также возникать пересортица. Выбор способа доставки - серьезная логистическая задача, и от ее решения может зависеть выгодность торговли данным товаром вообще. 3. Момент перехода права собственности (и соответственно рисков) на товар.

Соответственно любое возможное нарушение критериев нормальности должно рассматриваться как угроза экономической безопасности торгового предприятия.

5.2. Ровничная торговля

С точки зрения экономической безопасности в части закупок товара предприятие розничной торговли практически ничем не отличается от предприятий оптовой торговли.

В зависимости от организации продажи товара предприятия розничной торговли можно разбить на несколько категорий. Впрочем, деление это довольно условное и не претендует на полноту:

- магазины самообслуживания (гипермаркеты, супермаркеты, универсамы);

- магазины с «классическими» витринами и продавцами.

Рассмотрим критерии «нормальной» работы торгового зала универсама. При этом контроль качества товара, сроков его реа¬лизации отнесем к вопросам управления, а не безопасности. Будем считать, что продажа идет нормально, если:

- весь товар с прилавка проходит через кассу;

- весь товар правильно идентифицируется на кассе;

- кассир правильно принимает денежные средства за прошедший через кассу товар.

Возможные нарушения;

— товар скрыто проносится покупателями при'проходе через кассу;

- товар скрыто проносится покупателями при проходе через выход «без покупок»;

- товар неправильно идентифицируется на кассе;

- кассир принимает денежные средства в ненадлежащем количестве, неплатежеспособными или фальшивыми денежными знаками;

- кассир, находящийся в сговоре с покупателем, проносит товар мимо сканера без его фактического сканирования.

Рассмотрим данные ситуации подробно. Товар может проноситься скрыт покупателем:

- в одежде и под одеждой;

- в сумке, ранце, портфеле;

- в товаре;

- товар также может быть вывезен, будучи оставленным в тележке для товара.

Методы предупреждения по выносу под одеждой:

- визуальный контроль торгового зала с использованием средств видеонаблюдения;

- визуальный контроль торгового зала нейтрально одетыми сотрудниками службы безопасности;

- визуальный контроль выходящих покупателей кассирами и сотрудниками службы безопасности;

- доставка мелких дорогостоящих товаров на кассу сотрудниками предприятия либо реализация такого товара в отдельных кассах на площади торгового зала.

Методы предупреждения по выносу в ручной клади:

- визуальный контроль торгового зала с использованием средств видеонаблюдения;

- визуальный контроль торгового зала переодетыми сотрудниками службы безопасности;

— доставка мелких дорогостоящих товаров на кассу сотрудниками предприятия либо реализация такого товара в отдельных кассах на площади торгового зала

- сдача сумок, портфелей, рюкзачков и пр. в места хранения;

- запечатывание сумок, портфелей, рюкзачков и пр. в пластиковый пакет.

Метод предупреждения по вывозу в тележках:

- визуальный контроль тележек кассирами и сотрудниками службы безопасности. Для обеспечения контроля могут использоваться зеркала, позволяющие кассиру видеть дно тележки, не вставая с рабочего места.

Товар неправильно идентифицируется на кассе. Возможные варианты:

- случайная ошибка маркирования/считывания штрих-кодов;

— переклейка покупателем штрих-кодов с одного товара на другой;

- замена покупателем штрих-кодированной упаковки с одного товара на другой;

- добавление однородного товара в уже штрих-кодированную упаковку.

Методы противодействия:

- все виды визуального контроля зала,

- контроль кассирами соответствия товара его штрих-кодовой этикетке по номенклатуре и приблизительно либо точно -по количеству.

Кассир, находящийся в сговоре с покупателем, проносит товар мимо сканера без его фактического сканирования либо пропускает товар с неправильными штрих-кодами. При этом внешне вся ситуация выглядит нормально и от обычной «нормальной» продажи неотличима.

Методы противодействия:

- визуальный контроль работы кассиров сотрудниками службы безопасности;

- организация сверки чеков выходящих покупателей с товаром, приобретенным ими.

Безусловно, внимательность во время работы как кассиров, так и сотрудников службы безопасности требует постоянной проверки и оценки. Одним из наиболее эффективных способов являются тестовые «покупки». Сотрудник службы безопасности, незнакомый кассирам торгового зала, собирает (либо получает готовую от службы безопасности) тележку, в которой имеются товары с переклеенными штрих-кодами, измененной упаковкой, перевесом товара и т.д. После этого он в роли обычного покупателя проходит через кассу.

Рассмотрим отраслевые особенности торговых предприятий.

Территориальный фактор. Для торговли, особенно розничной, фактор местонахождения места сбыта (магазина) играет первоочередную роль. Магазин, расположенный в удачном («проходном») месте, может быть гораздо выгоднее другого аналогичного исключительно в силу месторасположения. Количество удачных для торговли мест ограничено. Соответственно, все моменты, связанные с организацией места торговли, имеют повышенное значение. Следует уделять особое внимание:

- отношениям с местными властями;

- отношениям с арендодателями в случае аренды торговых площадей;

— мониторингу выделения новых площадей, строительства новых торговых объектов, центров, рынков.

Разобщенность объектов. Обычно характерна для сетевых предприятий розничной торговли, оптовых и розничных предприятий в случае территориального разнесения управляющего офиса и склада (магазинов). Порождает следующие угрозы:

- падение управляемости процессом поставок и продаж;

— рост транспортных рисков;

— хищение ТМЦ на складах, при перевозке и в магазинах.

Сезонность продаж. Обусловливает более высокую требовательность к управлению закупками и продажами. Закупка большего количества сезонного товара, чем требуется, может повлечь за собой задержку его реализации почти на год, до следующего сезона. В случае со скоропортящимся товаром ситуация особенно сложная, так как он может просто прийти в негодность. Порождает следующие угрозы:

- фактор погодных рисков;

- нанесение экономического ущерба вследствие ошибок управления;

- также усугубляет проблему персонала: предприятие вынуждено либо содержать большой штат сотрудников с вынужденными простоями в периоды с низкой загрузкой, либо привлекать дополнительных сотрудников в периоды с высокой нагрузкой.