

**МИНИСТЕРСТВО ВЫСШЕГО ОБРАЗОВАНИЯ, НАУКИ И  
ИННОВАЦИИ РЕСПУБЛИКИ УЗБЕКИСТАН  
ТАШКЕНТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ВОСТОКОВЕДЕНИЯ**

**НАРОВ УЛУГБЕК ИРИСКУЛОВИЧ**

**УГРОЗЫ  
ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ**

**УЧЕБНОЕ ПОСОБИЕ**

Специальность: 7041902      Внешнеэкономическая деятельность  
(внешнеторговая деятельность)

Ташкент - 2023

## **Угрозы экономической безопасности - учебное пособие.**

Автор **Наров Улугбек Ирискулович**, доктор экономических наук, профессор кафедры Внешнеэкономической деятельности и туризма Ташкентского Государственного университета востоковедения.

*В учебнике раскрывается концепция и стратегия экономической безопасности государства и хозяйствующего субъекта. Выделены и детально рассмотрены важнейшие элементы, из которых складывается экономическая безопасность предприятия. Подробно рассмотрены технико-технологическая, информационная, финансовая, интеллектуальная, кадровая и экологическая безопасности. Представлены экономические показатели и индикаторы оценки эффективности экономической безопасности. Показаны этапы создания службы безопасности предприятия. Дана оценка системы обеспечения национальной безопасности отдельных государств. Приведена характеристика системы экономической безопасности Республики Узбекистан. В учебнике имеется достаточный материал для самостоятельной работы, решения тестов, кейсов и выполнения рефератов. Для оценки знаний по данному предмету студенты смогут подготовиться к экзаменам, вопросы билетов которых также приведены в учебнике.*

*Учебник подготовлен по специальности: 7041902 Внешнеэкономическая деятельность (внешнеторговая деятельность) для магистратуры.*

### **Рецензенты:**

**Собиров А.Х.**, к.э.н., доцент кафедры экономики труда и управления Ташкентского филиала РЭУ им. Г.В. Плеханова

**Уркенбаев Т.А.**, к.э.н., доцент кафедры Внешнеэкономической деятельности и туризма Ташкентского Государственного университета востоковедения.

## СОДЕРЖАНИЕ

	стр.
Предисловие .....	4
Тема 1. Концепция экономической безопасности.....	6
Тема 2. Стратегия экономической безопасности.....	11
Тема 3. Техничко-технологическая безопасность предприятия.....	19
Тема 4. Информационная безопасность предприятия.....	23
Тема 5. Финансовая безопасность государства и хозяйствующего субъекта.....	33
Тема 6. Показатели финансовой безопасности хозяйствующего субъекта .....	39
Тема 7. Интеллектуальная и кадровая безопасность предприятия...	46
Тема 8. Индикаторы интеллектуальной и кадровой безопасности предприятия.....	51
Тема 9. Экологическая безопасность предприятия.....	62
Тема 10. Оценка эффективности экологической безопасности предприятия.....	69
Тема 11. Организация службы безопасности предприятия.....	75
Тема 12. Система организации экономической безопасности государств.....	87
Глоссарий.....	97
Вопросы для самопроверки по темам.....	102
Тесты.....	107
Темы рефератов.....	125
Контрольные вопросы для самостоятельных работ.....	129
Задания для самостоятельных работ (кейсы).....	131
Вопросы к экзамену.....	134
Список литературы.....	137

## ПРЕДИСЛОВИЕ

Современный мир представлен обостряющейся борьбой за ресурсы. Дефицит минеральных, сырьевых, энергетических, водных ресурсов предопределяет определенную угрозу суверенитету и экономической безопасности многих государств. Возрастающая конкуренция на мировом рынке за право пользоваться большей частью известных ресурсов, их дележ и перераспределение является поводом для беспокойства и укрепления экономической безопасности. В этой связи изучение основ экономической безопасности государства, защита ее от внешних и внутренних угроз является актуальной проблемой современности. Представляется обоснованным изучение данной проблемы как на уровне государства так и на уровне хозяйствующего субъекта, общества и личности. В самом общем виде безопасность - это состояние и тенденции развития защищенности жизненно важных интересов общества, государства и человеческой личности, а также всех их структур от внутренних и внешних угроз. Экономическая безопасность - это состояние экономики, при котором обеспечиваются устойчивый экономический рост, оптимальное удовлетворение общественных потребностей, рациональное управление, защита экономических интересов на национальном и международном уровнях. Экономическая безопасность предприятия представляет собой совокупность условий, обеспечивающих защищенность экономического потенциала организации, ее финансового состояния и положения на рынке от внешних и внутренних угроз, связанных с неблагоприятными воздействиями внешней среды, которые способствуют достижению целей функционирования организации в условиях конкуренции и хозяйственного риска.

Целью изучения настоящего учебного пособия служит формирование знаний в области теоретико-методологических основ обеспечения экономической безопасности государства и хозяйствующих субъектов. Задачами являются изучение концептуальных и стратегических направлений экономической безопасности, овладение методологией и инструментарием исследования безопасности хозяйствующих субъектов; приобретение умения анализировать

развитие экономических процессов и оценивать уровень экономической безопасности государства и хозяйствующих субъектов; освоение навыков построения корпоративной защиты на основе оценки рисков и аудита экономической безопасности.

Учебное пособие состоит из двенадцати взаимосвязанных разделов, в которых отражен генезис экономической безопасности, начиная с описания концепции и стратегии категории, обоснования обеспечения безопасности важнейших ее составляющих элементов и, заканчивая рекомендациями по организации системы безопасности на предприятии и национальной безопасности государства. В учебном пособии использованы материалы специалистов, которые внесли вклад в развитие теории и методологии проблем экономической безопасности.

## **Тема 1. Концепция экономической безопасности**

Потребность в безопасности является важнейшей составляющей жизни человека. Эта потребность актуальна также для государства и общества в целом. С усилением конкуренции в экономике в условиях рынка рамки безопасного существования значительно сузились. Возможный очередной мировой кризис в экономике и других сферах жизни предопределяет необходимость по-новому взглянуть на проблему безопасности, переосмыслить вероятные угрозы, подготовить механизмы их предупреждения и обеспечить условия безопасного существования.

В самом общем виде безопасность - это статика и динамика защищенности важнейших интересов человека, государства и общества от различных видов угроз.

Выделяют следующие наиболее часто проявляющиеся виды угроз:

- Военные,
- Политические,
- Демографические,
- Социальные,
- Научно-технические,
- Информационные,
- Экономические

Из представленного спектра угроз наиболее значимыми являются угрозы экономического характера. Легко согласиться с этим утверждением, если вспомнить, что в основе всех угроз лежат вопросы, связанные с недостаточным финансированием затрат на предотвращение тех или иных угроз. Отсюда становится понятным актуальность изучения проблем обеспечения экономической безопасности.

Экономическая безопасность описывает состояние и развитие экономики, при котором достигается стабильность экономического роста, состояние насыщения потребностей общества основными необходимыми продуктами, эффективный менеджмент во всех сферах экономики и обеспечивается

защита национальных интересов как внутри самой экономической системы, так и за ее пределами.

Элементы экономической системы страны, такие как природные ресурсы, работники, производственные и непроизводственные фонды, недвижимость, финансовые ресурсы, хозяйственные структуры, регионы, предприятия, семья и человек, являются объектами экономической безопасности.

Субъектами экономической безопасности являются функциональные и отраслевые министерства и ведомства, государственные комитеты, налоговые и таможенные службы, банки, биржи, страховые компании, производители и продавцы продуктов, работ и услуг, а также общества потребителей.

Угрозы экономической безопасности представляют опасность для жизненно важных интересов общества, государства и человека. Угрозы подразделяются на внутренние и внешние.

Среди внутренних угроз экономической безопасности можно выделить нарастание структурной деформации экономики, снижение инвестиционной и инновационной активности, разрушение научно-технического потенциала страны, устойчивую тенденцию к превращению страны в топливно-сырьевую периферию развитых стран, усиление имущественного расслоения общества и криминализацию экономики.

Среди внешних угроз экономической безопасности можно выделить такие факторы, как "утечка умов" за границу, "бегство капитала" за рубеж, рост государственного долга, нарастание импортной зависимости по продовольствию и потребительским товарам, излишняя открытость экономики, скупка иностранным капиталом предприятий в целях вытеснения национальной продукции на внешнем и внутреннем рынках, а также низкий уровень развития транспортной инфраструктуры для экспортно-импортных операций.

Различают два уровня экономической безопасности. Первый уровень – международная безопасность, второй уровень – национальная безопасность.

Международная безопасность состоит из

- глобальной безопасности,

- региональной безопасности.

Национальная безопасность состоит из:

- государственной безопасности,
- региональной безопасности,
- безопасности общества,
- безопасности фирмы,
- безопасность личности.

Экономическая безопасность формируется из множества направлений, обеспечивающих ее целостность и состоятельность. Они включают:

- производственную,
- технологическую,
- промышленную,
- продовольственную,
- демографическую,
- экологическую,
- финансовую,
- информационную,
- внешнеэкономическую и другие.

Что касается предприятия, то экономическая безопасность предприятия означает ее защищенность от негативного влияния внутренней и внешней среды на его деятельность, а также способность предприятия быстро оперативно устранять различные угрозы или приспосабливаться к новым условиям хозяйствования, вызванные объективными и субъективными обстоятельствами негативного характера. Экономическая стабильность предприятия и стабильный рост доходов работников является определяющим фактором ее экономической безопасности

Если детализировать состояние экономической безопасности предприятия, то следует выделить следующие условия. Это:

- защищенность экономического потенциала фирмы,
- безопасность финансового состояния,

- стабильность позиции на рынке,
- гарантирование эффективного функционирования фирмы,
- обеспечение эффективного функционирования информационно-аналитической, организационной, правовой, плановой, контрольной, и других служб предприятия.

Внешние и внутренние угрозы для каждого предприятия индивидуальны, но включают в себя отдельные элементы, которые присущи практически всем субъектам хозяйствования. Существует также целый ряд специфических угроз. Для определения экономических угроз конкретного предприятия следует его идентифицировать по имеющейся классификации угроз в зависимости от таких факторов, как специфика функционирования предприятия, направления деятельности, ее отраслевая принадлежность, специфика рынка и др.

После анализа результатов можно определить какие угрозы оказывают на развитие предприятия наибольшее негативное влияние. Правильная идентификация позволит минимизировать количество угроз, выделить главные угрозы и определить эффективные направления обеспечения экономической безопасности предприятия.

Для разработки программы экономической безопасности предприятия следует определить объекты и субъекты потенциальных угроз. К объектам экономической безопасности предприятия, то есть то, что должно охраняться относятся имущество и ресурсы, персонал и различные структурные подразделения. К субъектам экономической безопасности предприятия, то есть, кто должен обеспечить безопасность, относятся ответственные лица, службы и подразделения, занимающиеся обеспечением безопасности.

Экономическая безопасность предприятия обеспечивается специальным инструментом, который представляется в виде программы, которая позволяет поэтапно принимать решения в области управления устойчивого развития. Программа систематически обновляется и дополняется в соответствии с опе-

ративными данными об изменениях во внутренних и внешних средах функционирования предприятия.

Обеспечения экономической безопасности предприятия необходимо рассматривать как непрерывный процесс, основанный на системном мониторинге индикаторов экономической безопасности, который позволяет получать объективную оценку состояния экономической безопасности предприятия и применять соответствующие механизмы её корректировки. Выбор соответствующих рычагов управления определяется состоянием экономической безопасности предприятия.

Экономическая безопасность предприятия поддерживается деятельностью ее подразделений. Планирования деятельности службы безопасности должна быть гибкой и оперативно реагировать на малейшие изменения в работе предприятия.

## Тема 2. Стратегия экономической безопасности

Стратегия развития - это долгосрочный план, который позволяет достигать поставленных целей и задач, адаптироваться к изменяющейся внешней и внутренней среде бизнеса и рынка, но при этом без конкретизации методов и тактических действий.

В отношении экономической безопасности, стратегия означает состояние защищенности национальной экономики от внешних и внутренних угроз. Хотя в научной литературе существуют различные точки зрения на это понятие, определение, которое основывается на идее о "защищенности" экономического суверенитета страны, единстве ее экономического пространства и создании условий для реализации стратегических национальных приоритетов, является достаточно обоснованным.

Теоретической и методологической базой стратегии экономической безопасности могут выступать основные законы философии и подкрепляться теориями стратегии экономической безопасности. Для развития теории стратегии экономической безопасности важны исследования в области теории экономической безопасности регионов, областей, районов и отраслей.

Таким образом, стратегию экономической безопасности можно сформулировать следующим образом. Стратегия экономической безопасности это выбор стратегически важных решений, которые обеспечивали бы удовлетворительный уровень безопасности деятельности субъекта экономики, локализовали угрозы и обеспечили быстрое возмещения полученного ущерба.

Стратегия экономической безопасности состоит из ряда мер методического, организационного, нормативного, и правового характера. Эти меры направлены на достижение единственной цели - обеспечение экономической безопасности и мониторинга оценки ее состояния.

Рассмотрим важнейшие угрозы экономической безопасности. Они заключаются в следующем:

1. Углубляющийся разрыв в уровни развития экономики стран;
2. Ограничение доступа к иностранным ресурсам и технологиям;

3. Конфликты в зонах экономических интересов государств и на границах;
4. Колебания конъюнктуры мировых товарных и финансовых рынков;
5. Изменение структуры мирового спроса на энергоресурсы и развитие зеленых технологий;
6. Деятельность межгосударственных экономических объединений, которая может нанести ущерб национальным интересам государства;
7. Глобальные риски для финансовой системы;
8. Уязвимость информационной инфраструктуры финансово-банковской системы;
9. Исчерпание экспортно-сырьевой модели экономического развития;
10. Недостаточная инновационная активность;
11. Недостаточный объем инвестиций в реальный сектор экономики;
12. Отставание в разработке новых технологий и низкий уровень квалификации специалистов;
13. Истощение ресурсной базы топливно-сырьевых отраслей;
14. Низкие темпы экономического роста;
15. Недостаточно эффективное государственное управление;
16. Высокий уровень криминализации и коррупции в экономической сфере;
17. Теневая экономика;
18. Дифференциация населения по уровню доходов;
19. Снижение качества образования и медицинской помощи;
20. Международная конкуренция за кадры высшей квалификации;
21. Недостаток или избыток трудовых ресурсов;
22. Неравномерность пространственного развития территорий;
23. Избыточные требования в области экологической безопасности и рост затрат на их выполнение.

Оценка уровня экономической безопасности может проводиться посредством мониторинга экономических процессов. Для этого важно использовать индикаторы, оперативно показывающие текущее состояние экономики. В качестве индикаторов экономической безопасности можно использовать известные

экономические и другие показатели:

- Динамика ВВП (валовый внутренний продукт);
- Уровень жизни населения;
- Уровень инфляции;
- Уровень безработицы;
- Структура экономики;
- Государственный долг;
- Расслоение общества по имущественному признаку;
- Криминализация экономики и общества;
- Техническое состояние производства;
- Объемы золотовалютных запасов;
- Конкурентоспособность экономики;
- Степень импортной зависимости;
- Уровень теневой экономики.

Современное предприятие представляется как сложный технический, технологический и финансово-экономический организм, систематически подвергающийся внутренним и внешним угрозам в своей деятельности. Ликвидировать или смягчить эти угрозы могут обеспечить мероприятия, вытекающие из комплексной программы экономической безопасности предприятия. Экономическая безопасность в совокупности со многими его составляющими элементами, такими как технико-технологическая, интеллектуальная, кадровая, финансовая, экологическая и другие - выступает не только главным условием обеспечения жизнедеятельности предприятия, но и фактором достижения его конкурентоспособности.

Так как безопасность предприятия в первую очередь зависит от защищенности ее экономических интересов, то представляется важным создать условия, которые обеспечивали бы защиту экономического потенциала, финансового положения, технического и технологического состояния предприятия. Устойчивость на рынке и возможность противостоять конкурентам, нивелировать

внешние и внутренние угрозы не допустить повторения возникших угроз и позволить предприятию функционировать в будущем еще стабильное и эффективнее. Решение этой задачи видится в систематическом проведении на предприятии аналитической, организационно-административной, плановой, учетно-контрольной работы, нормативно - правовом и информационном обеспечении.

Каждый хозяйствующий субъект в силу специфики производства подвержен индивидуальным угрозам. У одних предприятий внутренние угрозы более значительные, у других внешние угрозы сильнее. Однако, анализ всех видов и типов угроз позволяет выявить однотипные угрозы, схожесть которых позволяет их сгруппировать. Систематизация похожих угроз позволяет их классифицировать, по важнейшим элементам экономической безопасности. В основе такой классификации могут лежать функциональные составляющие различных угроз. Среди этих угроз можно выделить достаточно значимые. Они в первую очередь оказывают негативное влияние на деятельность хозяйствующего субъекта. Среди большого многообразия видов экономической безопасности, предупреждающие различные угрозы, просматривается наиболее часто встречающиеся, такие как информационные, производственно-технологические, экологические, кадровые, интеллектуальные, финансовые.

Стратегия экономической безопасности предприятия предполагает выделение контура работ по разработке комплексной программы экономической безопасности хозяйствующего субъекта. Такая программа позволит обеспечить защищенность предприятия от негативных влияний внешней среды и внутренних факторов, дестабилизирующих бизнес среду. Реализация программы приведет к возможности адаптировать предприятие к условиям, при котором возникают угрозы, путем разработки дорожной карты, позволяющей быстро устранять негативные влияния на производство, восстановить эффективность и создать предпосылки для ее роста.

Комплексная программа экономической безопасности хозяйствующе-го субъек-

екта должна формироваться из локальных программ безопасности предприятия, таких как:

- локальная программа технико-технологической безопасности,
- локальная программа информационной безопасности,
- локальная программа финансовой безопасности,
- локальная программа интеллектуальной и кадровой безопасности,
- локальная программа экологической безопасности.

При этом допустима разработка и включение в стратегию безопасности предприятия дополнительных программ, учитывающих угрозы предприятия, вызванных спецификой функционирования предприятия. Важным моментом выступает необходимость организации системы обеспечения безопасности предприятия, слаженную работу которой может осуществлять служба безопасности предприятия.

Давайте разберемся в сущности каждой из вышеназванных локальных программ безопасности предприятия.

Локальная программа технико-технологической безопасности предприятия предполагает определить насколько уровень используемых на данном предприятии технологий соответствует лучшим мировым аналогам. На основе глубокого технического анализа предприятия: состояния оборудования, техники и технологий выдается заключение о способности предприятия производить конкурентную продукцию. Приводится обоснование источников и объемов инвестирования в целях преодоления отставания предприятия от своих конкурентов в техническом и технологическом аспектах.

Следующей локальной программой является программа информационной безопасности. Значимость этой программы очевидна, так как в настоящее время спрос на информацию значительно возрос, а возможности утечки и незаконного использования информации при развитии информационных технологий - возросли еще больше. Поэтому защита коммерческой информации, информационных систем и информационных ресурсов предприятий от внеш-

них и внутренних угроз, предотвращение несанкционированного использования конфиденциальной информации становится важной задачей экономической безопасности предприятия. В их круг входят задачи выявления, оценки и предотвращения угроз информационным системам и информационным ресурсам; защиты прав юридических и физических лиц на интеллектуальную собственность, а также сбор, накопление и использование информации; защиты служебной, коммерческой и личной тайны.

Важной основой экономической безопасности выступает локальная программа финансовой безопасности предприятия. В масштабах страны финансовая безопасность определяется возможностью государства проводить самостоятельную финансово экономическую политику, отвечающей своим национальным интересам. Она предполагает необходимость устранения влияния финансовых кризисов, теневых структур на национальную социально экономическую систему, предотвращение утечки капитала за рубеж из реального сектора, активную борьбу с коррупцией, привлечение иностранного капитала на выгодных для национальной экономики условиях. На уровне предприятия финансовая безопасность предполагает возможность проведения самостоятельной финансовой стратегии в рамках финансово экономической политики страны. Она оценивается показателями платежеспособности, а также показателями ликвидности активов. К показателям платежеспособности относятся показатели финансовой устойчивости, деловой активности, рентабельности и другие. К показателям ликвидности активов в свою очередь можно отнести коэффициенты быстрой (промежуточной) ликвидности, текущей ликвидности и абсолютной ликвидности. Проведя комплексный анализ финансовых показателей предприятия можно будет формировать основу локальной программы финансовой безопасности предприятия. Важность этой программы, при формировании концепции экономической безопасности, трудно переоценить, поскольку степень финансовой независимости предприятия во многом определяет его самостоятельность, а, следовательно, свободу действий по достижению поставленных целей.

Следующей составляющей комплексной программы экономической безопасности предприятия является локальная программа интеллектуальной и кадровой безопасности предприятия. Способность кадрового потенциала осваивать созданные инновационные продукты, а равно и генерировать, то есть создавать собственные новации для производственных нужд, представляется особым видом ресурсов предприятия. Этот вид ресурса необходимо создавать и развивать, поскольку от него в большей степени зависит конкурентоспособность, а стало быть выживаемость предприятия в условиях рыночной экономики. Интеллектуальный потенциал предприятия, являясь его наибольшей ценностью предполагает такие качества человека, как моральные устои, знания, образование, практические навыки и опыт, творческие способности людей, мотивацию, культуру, талант и прочие. Эти личностные качества человека при эффективном их использовании могут приносить огромные дивиденды предприятию. Кадровая безопасность предприятия обеспечивается путем нейтрализации рисков, связанных с недобросовестной работой персонала, снижением уровнем развития его интеллектуального потенциала, а также ухудшением системы организации трудовых отношений. Важно подчеркнуть, что снижения угроз именно кадровой безопасности предприятия является очень важным моментом в системе экономической безопасности предприятия. Это видно из такого известного факта, что до 90% угроз всех элементов экономической безопасности лежат в плоскости кадрового фактора. Разработка действенных мер, направленных на устранение угроз кадровой безопасности, которая, в первую очередь, заключается в мотивации труда является барьером для многих опасностей, окружающих предприятие.

Функционирование современного предприятия трудно представить в отрыве от проблем загрязнения окружающей среды. В этой связи значительно возрастает роль такой составляющей комплексной программы экономической безопасности как локальная программа экологической безопасности. Причем под экологической безопасностью предприятия необходимо понимать не

только обеспечение соответствия природоохранной деятельности предприятия нормативным требованиям, но и элементарную культуру бытия, то есть охрану среды своего обитания и труда от загрязнения. Разработка локальной программы экологической безопасности предприятия является важнейшим условием хозяйствования. Программа обеспечит не только выполнение санитарных норм и правил, усилит экологическую безопасность, но также будет способствовать росту конкурентоспособности предприятия, возникающей при выпуске экологически чистой продукции.

Итак, мы представили важнейшие аспекты локальных программ, которые должны явиться составной частью общей комплексной программы экономической безопасности предприятия. Разработка локальных программ должна осуществляться соответствующими профильными структурами предприятия. Комплексная программа экономической безопасности должна сводиться и формироваться ответственным подразделением предприятия, которая будет осуществлять ее мониторинг. Примером такого подразделения может явиться управление финансового менеджмента или экономическое управление предприятия.

### **Тема 3. Техничко-технологическая безопасность предприятия**

Суть техничко-технологической составляющей экономической безопасности предприятия состоит в определении степени соответствия технологий предприятия лучшим мировым аналогам. Обеспечение техничко-технологической безопасности достигается поэтапным решением следующих задач:

Во первых - следует провести маркетинг рынка технологий и технологических оборудований, которые могут производить продукции, выпускаемой на данном предприятии;

Во вторых - необходимо проанализировать собственные технологии и оборудования предприятия.

В третьих – нужно определить перечень перспективных товаров, для производства на предприятии.

В четвертых целесообразно составить план новых технологий для производства этих перспективных товаров и использования внутренних ресурсов для улучшения используемых технологий;

В пятых - следует разработать технологическую стратегию развития предприятия, включающей в себя планирование технологического развития предприятия и затрат на приобретение новых технологий.

В шестых - необходима оперативная реализация планов, контроль за выполнением планов и анализ результатов принятых мер по обеспечению техничко-технологической безопасности предприятия.

Обеспечение техничко-технологической безопасности предприятий нематериальной сферы производства сопряжено с кадровой и информационной безопасностью, так как меры безопасности заключаются в повышении кадрового потенциала сотрудников и защиты информации предприятия, представляющие коммерческую ценность.

Обеспечение техничко-технологической составляющей является приоритетной задачей для промышленных предприятий, так как она имеет важное

значение для их экономической безопасности. Определение объемов капитальных вложений и их распределение во времени в эту сферу возможно только при наличии индикаторов, которые позволяют оценить степень угроз предприятию.

В качестве индикаторов технико-технологической безопасности предприятия можно выбрать известные экономические показатели. Для таких индикаторов как:

- эффективность использования основных производственных фондов (ОПФ) используются показатели – фондоотдача и фондоемкость продукции,
- степень износа ОПФ используется показатель – коэффициент выбытия ОПФ,
- обновление ОПФ ) используется показатель – коэффициент обновления ОПФ,
- интенсивность производства используется показатель - реальный уровень загрузки производственных мощностей,
- новизна используемой техники и технологий используется показатель - доля НИОКР в общем объеме работ,
- конкурентоспособности выпускаемой продукции используется показатель - процент выпускаемой продукции, соответствующей лучшим аналогам или превосходящей их и т.д.

Перечень индикаторов мониторинга технико-технологической безопасности предприятия может быть увеличен. Он широко представлен в специальной литературе. Система показателей будет включать в себя темп обновления ОПФ, динамику производства (рост, спад, стабильное состояние, темп изменения), стабильность производственного процесса (ритмичность, уровень загруженности в течение определенного времени), загрузку специализированного оборудования, возрастную структуру и технический ресурс парка машин и оборудо-

дования, доступ к НОУ-ХАУ, количество продаваемых и покупаемых предприятием лицензий, количество имеющихся в распоряжении предприятия патентов, соотношение получаемых уплачиваемых предприятием лицензионных выплат, Кроме того, также могут быть оценены показатели соответствия мировым аналогам используемые на предприятии видов технологического оборудования, процент выпускаемой продукции предприятия, защищенной патентами, принадлежащими данному предприятию, удельный вес технологического оборудования предприятия, разработанного на предприятии и защищенного патентами предприятия, удельный вес оборудования, приобретенного на основе лицензионных договоров, средняя заработная плата научного сотрудника за месяц, и оценка конкурентоспособности продукции и другие показатели, прямо или косвенно характеризующие технико-технологическое состояние предприятия.

Кроме индикаторов, которые информируют о состоянии технико-технологической безопасности предприятия в практике применяется обобщающий показатель, дающий представление об эффективности мер, принятых на предприятии для обеспечения его технологической безопасности. В литературе он представляется как частный функциональный критерий (ЧФК). Для расчета ЧФК необходимо сопоставить суммы ущербов, предотвращенных благодаря мерам по обеспечению технико-технологической безопасности и затраты на реализацию этих мер.

Для расчета частного функционального критерия (ЧФК) используется следующая формула:

$$\text{ЧФК} = \text{Упр} / (\text{З} + \text{Упо}),$$

где ЧФК - частный функциональный критерий;

Упр - суммарный предотвращенный ущерб от реализации комплекса мер по обеспечению технологической безопасности предприятия;

З - общая сумма затрат, понесенных предприятием при реализации указанного комплекса мер;

Упо - суммарный понесенный предприятием ущерб его экономической безопасности.

Чем выше значение ЧФК, тем выше уровень технико-технологической безопасности предприятия.

Для проведения всесторонней оценки технологической безопасности необходимо проанализировать общий технический уровень производства, который отражает уровень развития средств производства и прогрессивность технологий. Значение частного функционального критерия (ЧФК) уровня технологической безопасности может быть использовано при расчете совокупного критерия экономической безопасности предприятия.

Алгоритм обеспечения технико-технологической безопасности предприятия включает в себя следующие шаги:

- 1) детальное изучение рыночного сегмента, в котором действует фирма, а также политических, экономических и криминогенных факторов в стране, регионе и городе, которые могут повлиять на деятельность предприятия. Цель - понимание текущей экономической ситуации предприятия, прогнозирование его будущего состояния и формирование списка угроз, которые могут помешать достижению поставленных целей;
- 2) разработка комплекса мер, направленных на предотвращение выявленных угроз или снижение ущерба, который может возникнуть при их реализации, включая меры по локализации и ликвидации последствий угроз;
- 3) создание организационной структуры системы безопасности, включая определение целей и задач по обеспечению экономической безопасности, разработку положений и инструкций по экономической безопасности, распределение обязанностей между должностными лицами и подразделениями, назначение ответственных лиц, создание специальных структурных подразделений и службы безопасности;
- 4) организация контроля за соблюдением установленного режима экономической безопасности с использованием методик, разработанных в организации.

#### **Тема 4. Информационная безопасность предприятия**

Информация - это сведения или знания. Чтобы получить и использовать информацию, необходимо знать такие понятия, как: информация (И), информационные процессы (ИП), информационные системы (ИС), информационные ресурсы (ИР), собственник информационных ресурсов, пользователь и информация о гражданах.

- Информация - это данные о людях, объектах, фактах, событиях и процессах, независимо от формы их представления. Документированная информация (документ) - это информация, зафиксированная на материальном носителе с реквизитами, позволяющими ее идентифицировать.
- Информационные процессы - это процессы сбора, обработки, накопления, хранения, поиска и распространения информации.
- Информационные системы (ИС) - это организационно упорядоченная совокупность документов и информационных технологий, включая использование средств вычислительной техники и связи, которые реализуют информационные процессы.
- Информационные ресурсы - это отдельные документы и массивы документов, документы и массивы документов в информационных системах ИС (библиотеках, архивах, фондах, банках данных других ИС).
- Собственник информационных ресурсов, информационных систем ИС, технологий и средств их обеспечения - это субъект, который полностью реализует полномочия владения, пользования и распоряжения указанными объектами.
- Пользователь (потребитель информации) - это субъект, обращающийся к ИС или посреднику за получением необходимой ему информации и

пользующийся ею.

- Информация о гражданах (персональные данные) - это данные о фактах, событиях и обстоятельствах жизни граждан. Персональные данные относятся к категории конфиденциальной информации.
- Информационная безопасность означает защищенность информационных систем и информационных ресурсов от внешних и внутренних угроз, которые могут препятствовать эффективному использованию информации обществом, государством и отдельными лицами.

Для достижения информационной безопасности необходимо решить несколько задач:

- Выявление, оценка и предотвращение угроз, которые могут возникнуть в информационных системах и информационных ресурсах.
- Защита прав юридических и физических лиц на интеллектуальную собственность и обеспечение правильного сбора, накопления и использования информации.
- Защита государственной, служебной, коммерческой и личной тайны.

Существуют различные группы угроз, которые могут угрожать информационной безопасности, включая следующие:

- Программные угрозы - это внедрение "вирусов", программных и аппаратных закладок, а также уничтожение и модификация информации в информационных системах.
- Технические угрозы, включая радиоэлектронные - это перехват информации в линиях связи, радиоэлектронное подавление сигнала в системах управления и т.д.
- Физические угрозы - это уничтожение средств обработки информации и носителей информации, кража носителей, а также аппаратных или программных парольных ключей.
- Информационные угрозы - это нарушение регламентов информацион-

ного обмена, незаконный сбор и использование информации, несанкционированный доступ к информационным ресурсам, незаконное кодирование данных в информационных системах, дезинформация, сокрытие или искажение информации, хищение информации из баз данных.

Существуют различные меры для обеспечения информационной безопасности, включая следующие:

- Юридические меры - это использование правовых норм и законодательства для защиты информации и информационных ресурсов.
- Организационно-экономические меры - это реализация организационных и управленческих мер, таких как создание политик и процедур, обучение сотрудников, управление доступом к информации и т.д.
- Технологические меры - это использование технических средств и технологий, таких как системы шифрования, брандмауэры, системы обнаружения вторжений и т.д., для защиты информации и информационных ресурсов.

Вышеупомянутые меры для обеспечения информационной безопасности основаны на следующих принципах:

- Нормативно-правовая база информационных отношений в обществе должна ясно определять механизм обеспечения права граждан на свободный доступ к информации любым законным способом.
- Интересы собственников, владельцев и управляющих информационными ресурсами охраняются законом.
- Закрытие информации для доступа является исключением из общего правила для доступа к информации.
- Ответственность за сохранность информации, ее закрытие и раскрытие персонифицируется.
- Государство обеспечивает развитие сферы информационных услуг, предоставляемых населению и специалистам на основе современных

компьютерных сетей, системы общедоступных баз и банков данных, содержащих справочную информацию социально-экономического, культурного и бытового характера, с правом доступа к которым, гарантированным и регулируемым законодательством.

Информационная безопасность тесно связана с функционированием информационного рынка, который является разветвленным и включает в себя «область информации», а экономическая информация является главным сектором этого рынка. Обеспечение экономической безопасности страны в целом, различных хозяйствующих субъектов и личности напрямую связано с проблематикой информационной безопасности.

Необходимость в защите информации возникла по следующим причинам:

- Развитие информационных технологий привело к формированию открытого информационного общества.
- Информация имеет ценность, так как ее неизвестность третьим лицам является товаром и подлежит защите.
- Информация формирует новый уровень знаний, который является основным фактором, обеспечивающим прибыль предприятий, и, следовательно, должен быть защищен.
- Информация распространяется по формальным и неформальным каналам, что затрудняет ее защиту.

Информация в настоящее время является объектом права и собственности. Процессы информатизации экономики усугубляют противоречие между правами граждан на доступ к информации и необходимостью ограничения этого права для защиты прав хозяйствующих субъектов. Поэтому установление правового режима информации и обеспечение ее защиты приобретают особое значение.

Основные направления обеспечения информационной безопасности в бизнесе включают:

- Защиту информации о состоянии и движении материальных активов, которая обычно понимается как обеспечение экономической безопасности.

- Защиту информации о состоянии нематериальных активов и их носителях, таких как персонал, которая определяется как информационная безопасность.
- Защиту средств хранения, обработки и передачи информации.

Существуют различные виды информации в зависимости от степени доступа к ним:

- Государственная тайна, которая включает информацию особой важности, совершенно секретную и секретную.
- Коммерческая тайна, включающая защищенную информацию и информацию с ограниченным доступом.
- Информация без права ограничения, которая является общедоступной.

Рассмотрим основные цели защиты информации:

1. Предотвращение утечки, хищения, утраты, искажения и подделки информации.
2. Предотвращение угроз безопасности личности, общества и государства.
3. Предотвращение несанкционированных действий, таких как уничтожение, модификация, искажение, копирование или блокирование информации, а также других форм незаконного вмешательства в информационные ресурсы и системы. Обеспечение правового режима документированной информации как объекта собственности также является важной целью.
4. Защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, хранящихся в информационных системах.
5. Сохранение государственной тайны и конфиденциальности документированной информации в соответствии с законодательством.
6. Обеспечение прав субъектов в информационных процессах, а также при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Защита должна быть обеспечена для любой документированной информации, неправомерное использование которой может причинить ущерб ее собственнику, владельцу, пользователю или другим лицам.

Режим защиты информации устанавливается на основании соответствующих государственных законов:

- Для сведений, отнесенных к государственной тайне, режим устанавливается уполномоченными лицами на основании соответствующих законов государств о государственной тайне.
- Для конфиденциальной документированной информации режим устанавливается собственником информационных ресурсов или уполномоченным лицом на основании закона.
- Для персональных данных режим устанавливается на основании соответствующих законов.

Исходя из вышеизложенного, можно сформулировать условия формирования системы информационной безопасности для предприятия (организации):

1. Необходимо четко определить понятие "система информационной безопасности" и проводить постоянную деятельность по выявлению, предупреждению, локализации и нейтрализации угроз потери и утечки информации, а также минимизировать ущерб от реализации угроз.

2. Необходимо учитывать мнения и позиции собственника, акционеров и топ-менеджмента, поскольку они могут различаться.

3. Следует соблюдать принципы и алгоритм формирования системы информационной безопасности фирмы, основанные на том, что любое действие, нарушающее нормальное функционирование организации, может быть рассмотрено как угроза информационной безопасности фирмы.

Информационные системы, сама информация и персонал являются основными объектами угроз информационной безопасности.

Угрозы информационной безопасности обычно вызываются действиями человека и имеют антропогенную основу. Эти угрозы могут проявляться через:

- Нанесение вреда путем внедрения в состав персонала;

- Несанкционированный доступ на территорию организации неавторизованным лицом;
- Вербовку сотрудников организации;
- Дистанционное наблюдение.

При осуществлении угроз могут быть использованы следующие методы:

- Копирование или кража носителей информации;
- Внесение несанкционированных изменений в данные;
- Уничтожение информации;
- Разрушение информационных систем и т.д.

Широкое распространение информационных технологий вызвало появление новых угроз информационной безопасности организаций, таких как:

- Умышленный ввод ложных данных или изменение информации на носителе;
- Передача информации третьим лицам;
- Незаконное использование машинного времени.

Причины утечки информации могут быть связаны со следующими факторами:

- Не квалифицированность и не компетентность нанимаемых на работу сотрудников, что может привести к страху, угодничеству и боязни принимать самостоятельные решения у некоторой части персонала;
- Не соответствие системы оплаты количеству и качеству работы, что может вызвать недовольство среди сотрудников и привести к непредсказуемому поведению.

Эти причины могут привести к неадекватным формам поведения отдельных специалистов в сфере информационных технологий, таких как:

- Предоставление пользователям заведомо ложных объяснений о неисправностях и объеме работы;
- Саботирование работы, пользуясь тем, что руководство не полностью осведомлено о сути работы;
- Некачественное выполнение работы в надежде на то, что пользователи не осведомлены об этом;

- Сознательное завышение требований к материальным ресурсам организации на обслуживание информационных систем.

При оценке информационных рисков могут использоваться следующие показатели:

- Стоимостная оценка информации, отнесенной к коммерческой тайне;
- Суммарные затраты на восстановление утраченной информации;
- Финансовые потери и упущенная прибыль, связанные с принятием решений на основе недостоверной информации и т.д.

Для обеспечения информационной безопасности организации необходимо реализовать комплекс мер, включающий технические, технологические, организационные, экономические и социально-психологические аспекты в рамках программы экономической безопасности. Некоторые из этих мер включают:

- Распределение информации между сотрудниками;
- Учет ознакомления сотрудников с особо важной информацией;
- Распространение информации только через контролируемые каналы;
- Назначение ответственных лиц за контроль документации;
- Уничтожение неиспользованных копий документов и записей;
- Четкое определение коммерческой тайны для персонала;
- Составление, регулярная оценка и обновление перечня информации, являющейся коммерческой тайной;
- Включение положения о неразглашении коммерческой тайны в трудовой договор, правила внутреннего распорядка и должностные инструкции;
- Включение положений о неразглашении тайны в соглашения и договоры с партнерами;
- Дополнительную проверку компетентности работников при найме;
- Предварительное профессиональное обучение сотрудников.

Для увеличения безопасности работы с информационными технологиями (ИТ) могут быть приняты организационные меры.

1. Оценка квалификации персонала - аттестация, при которой уровень квалификации оценивается по шкале, включающей три уровня:

- нулевой уровень (начинающий пользователь): владение элементарными навыками, такими как включение и выключение ПК, а также базовые операции.
- базовый уровень (пользователь): уверенное владение программным обеспечением общего назначения.
- специальный уровень (специалист): способность определять, какое программное обеспечение оптимально решит задачи, самостоятельная установка и настройка, а также автоматизация отдельных операций с помощью встроенных в ПО инструментов.

2. Обучение пользователей ИТ который включает:

- составление квалификационных требований, таких как сертификат пользователя, определенный уровень квалификации или перечисление необходимых навыков, и отражение их в должностной инструкции для вакантной позиции.
- подбор персонала на соответствие требованиям, включая профессиональный отбор, интервью, анкетирование и испытания.
- испытательный срок для освоения программного продукта и достижения уровня самостоятельности в решении профессиональных задач с помощью ИТ.
- аттестация, результатом которой является оценка эффективности использования ИТ для решения профессиональных задач. Эта оценка может быть проведена с помощью интервью, наблюдения и анализа тестовых заданий.
- непрерывное повышение квалификации, которое может быть реализовано через обеспечение доступа к программам, специальной литературе, обмен опытом между пользователями и специальные курсы.

При увольнении сотрудника и возможной угрозе информационной безопасности организации необходимо учитывать определенные особенности. Если имеются признаки того, что сотрудник намеревается уволиться, такие как посещение сайтов по поиску работы или отправка резюме, рекомендуется

выполнить следующие действия:

- Взять под контроль всю переписку с рабочего адреса и некоторые операции на ПК.

- Сделать резервную копию всех файлов пользователя в его отсутствие.

3. Для предотвращения угрозы информационной безопасности после объявления сотрудником о своем увольнении, могут быть применены следующие меры:

- информировать всех сотрудников о предстоящем увольнении и запретить им передавать сотруднику любую информацию, связанную с работой.

- создать резервную копию файлов пользователя.

- организовать передачу дел.

- постепенно ограничивать права доступа к информации по мере передачи дел.

- при необходимости обеспечить сопровождение увольнения специалистом по информационной безопасности.

В случае обнаружения факта промышленного шпионажа со стороны сотрудника, следует принять следующие меры:

- немедленно отключить сотруднику все права доступа к ИТ.

- незамедлительно скорректировать права доступа к общим информационным ресурсам, таким как базы данных, принтеры, факс. Также необходимо перекрыть или изменить внешние входы в сеть.

- поручить всем сотрудникам сменить свои пароли, сообщив им следующую информацию: "Сотрудник N с (дата) больше не работает. При любых попытках контакта с ним немедленно сообщайте в службу безопасности".

- в течение некоторого времени осуществлять усиленный контроль над информационной системой.

## **Тема 5. Финансовая безопасность государства и хозяйствующего субъекта**

Финансовая безопасность является неотъемлемой частью экономической безопасности страны, регионов и предприятий. Она является основой экономически эффективного государства и позволяет проводить самостоятельную финансово-экономическую политику в интересах нации. Она также отражает способность государства обеспечить устойчивость финансово-экономического развития страны, предотвращать финансовые кризисы, избежать утечки капитала, привлекать иностранный капитал на выгодных условиях для экономики страны.

В настоящее время государственные и трансгосударственные финансовые системы перешли на новую ступень влияния на государства. Среди экономических аналитиков существует, и не безосновательно, мнение о том, что главное влияние на так называемую геоэкономику оказывают геофинансы и это должно настораживать государства, поскольку риск их суверенитета непомерно возрастает.

Для государства важно обеспечить финансовую безопасность, что является необходимым условием для осуществления самостоятельной финансово-экономической политики в соответствии с его национальными интересами.

Финансовая безопасность государства при условии ее состоятельности позволит ему, в лице его органов обеспечить:

- проведение политики устойчивого экономического развития,
- формирование платежного баланса и важнейших финансовых параметров;
- смягчение влияния мировых кризисов, действий транснациональных, политических, экономических и финансовых формирований (ТНК, ФТК, субгосударственные группировки и др.), теневых структур на национальную экономику страны,
- заслон утечке капитала за границу, из реального сектора экономики,

- возможность привлекать и использовать иностранные средства в национальных интересах,
- пресечение уголовных и административных правонарушений в финансовой сфере.

Сущность финансовой безопасности предприятия заключается в его способности разрабатывать и реализовывать финансовую стратегию, соответствующую общей корпоративной стратегии в конкурентной и неопределенной среде. Основным условием обеспечения финансовой безопасности предприятия является способность справляться с возникающими опасностями и угрозами, которые могут привести к финансовым потерям, изменению структуры капитала или ликвидации предприятия. Для достижения этого предприятие должно поддерживать финансовую устойчивость, обеспечивать равновесие, достаточную финансовую независимость и гибкость при принятии финансовых решений.

Финансовая устойчивость и финансовая безопасность фирмы являются неразрывно связанными и взаимодополняющими понятиями. Они представляют собой две стороны одной медали. Финансовая устойчивость - это необходимое, но недостаточное условие для обеспечения финансовой безопасности фирмы. Если фирма обладает финансовой безопасностью, то она должна также обладать и финансовой устойчивостью. Однако обратное утверждение не всегда является истинным. Обеспечение финансовой безопасности и финансовой устойчивости стали чрезвычайно актуальными проблемами в последнее время. Это связано не только с финансовыми и экономическими кризисами, ростом нестабильности, но также с глобализацией экономического пространства, что приводит к увеличению количества угроз, таких как нестабильность финансовых рынков и аномальные колебания цен на энергоносители, в частности, на нефть, газ. В этих условиях государства, регионы и хозяйствующие субъекты вынуждены использовать принципиально новые подходы для обеспечения безопасности и устойчивого развития. Финансовая

устойчивость является важной характеристикой, которая определяет эффективность финансового управления предприятием. Она широко используется при анализе финансового состояния предприятия и определении его инвестиционной привлекательности. Финансовая устойчивость предприятия представляет собой сложное понятие, которое отражает состояние финансов, позволяющее предприятию стабильно развиваться и сохранять финансовую безопасность в условиях дополнительных рисков. В узком смысле, финансовая устойчивость предприятия определяется оптимальным соотношением различных видов финансовых ресурсов, привлекаемых предприятием, и их использованием. Финансовая устойчивость предприятия тесно связана с другими финансовыми характеристиками, такими как финансовая безопасность, гибкость, стабильность и равновесие. Очевидно, что обеспечение финансовой безопасности фирмы возможно только при условии финансово устойчивого развития, которое обеспечивает создание такого финансового механизма, способного адаптироваться к изменяющимся условиям внутренней и внешней среды. При этом особое значение приобретают уровни финансовой устойчивости, так как для обеспечения финансовой безопасности фирмы важен не абсолютный, а оптимальный уровень финансовой устойчивости.

Факторами взаимосвязи и взаимодействия между финансовой устойчивостью и финансовой безопасностью фирмы, то есть то что их объединяет, являются финансовая гибкость, финансовая стабильность, финансовое равновесие. Разберемся в этих понятиях.

Финансовая гибкость фирмы означает ее способность изменять объем и структуру финансирования, а также направления вложения финансовых ресурсов в соответствии с изменяющимися внешними и внутренними обстоятельствами. Это качественная характеристика, которая может быть оценена по наличию управленческих опционов у предприятия.

Финансовая стабильность фирмы - это сохранение оптимальных финансовых показателей, удовлетворяющих финансовой политики фирмы.

Финансовое равновесие фирмы, определяется оптимальным сочетанием доходности и риска и характеризует сбалансированность развития фирмы.

Возникновение вышеуказанных факторов взаимосвязи и взаимодействия между финансовой устойчивостью и финансовой безопасностью фирмы безоговорочно приводят к общим угрозам, которые влияют на финансовую безопасность и финансовую устойчивость фирмы.

Финансовая самостоятельность предприятия (фирмы) подвержена различным видам угроз. Выделяются два основных вида угроз. Это внутренние угрозы финансовой безопасности и внешние угрозы финансовой безопасности.

Среди угроз внутреннего характера можно выделить следующие:

1. Ошибки менеджмента в области управления финансами фирмы, связанные с выбором стратегии, управлением и оптимизацией активов и пассивов;
2. непрофессиональный контроль и управление дебиторской и кредиторской заимствованиями;
3. Ошибки в выборе инвестиционных проектов и обосновании источников их финансирования;
4. Неверная политика в области амортизации основных производственных фондов (ОПФ) и налоговых отчислений.

К внешним угрозам финансовой безопасности предприятия относятся:

1. Несанкционированное приобретение активов предприятия (акций и долгов);
2. Образование финансовых долгов (обязательств), превышающих нормативных размеров;
3. Отсутствие рынков капитала или недостаточное их развитие;
4. Недостаточная развитость элементов рыночной инфраструктуры;
5. Недостаточная правовая защита инвесторов и выполнение законодательства;
6. Кризис финансово-денежной и кредитной системы;

7. Нестабильность экономики, высокая инфляция;
8. Процветание монополизма и коррупции;
9. Неэффективность механизмов формирования и контроля экономической, финансовой и банковской политики государства.

Необходимо осуществлять комплексный мониторинг финансовой устойчивости и безопасности фирмы, так как они взаимосвязаны. Для достижения финансовой устойчивости фирмы важно обеспечить ее финансовую безопасность. Поэтому создание эффективной структуры контроля за обеспечением финансовой устойчивости и безопасности фирмы имеет первостепенное значение для снижения влияния угроз.

Аналитическая служба фирмы является органом, который должен проводить мониторинг финансовой устойчивости и безопасности фирмы в оперативном режиме, оперативно реагировать на изменение ситуации, регулярно подготавливать документы для директора и совета директоров, чтобы принимать решения по проблемам, а также контролировать их выполнение.

Для создания эффективной системы финансовой устойчивости фирмы требуется разработать соответствующую документацию. В этой документации должны быть определены внутренние и внешние угрозы, а также критерии, по которым можно определить, что финансовая устойчивость и безопасность фирмы нарушены.

Другими словами, необходимо определить критерии, которые позволят оценить соблюдение требований финансовой устойчивости и безопасности фирмы. Аналитическая служба будет оценивать соблюдение этих критериев и информировать топ-менеджмент фирмы. Также нужно разработать принципы требований к должникам, чтобы они соответствовали требованиям финансовой устойчивости и безопасности фирмы. При этом аналитическая служба должна выражать свою точку зрения на значимость представляемой отчетности для оценки обеспечения финансовой устойчивости и безопасности фирмы, а также для контроля за финансовыми интересами предприятия. Для всестороннего и объективного мониторинга финансовой устойчивости и

безопасности фирмы необходимо создать информационную систему, которая позволит выявлять и прогнозировать внутренние и внешние угрозы. На основе полученной информации должен быть разработан комплекс оперативных и долгосрочных мер по противодействию негативным факторам, а также по предупреждению возможных нежелательных угроз и их последствий.

С точки зрения теории и практики можно с уверенностью сказать, что для достижения финансовой устойчивости фирмы необходимо и достаточно обеспечить ее финансовую безопасность. В свою очередь, достижение финансовой безопасности возможно только при обеспечении финансовой устойчивости фирмы.

## Тема 6. Показатели финансовой безопасности хозяйствующего субъекта

В предыдущей теме было сказано, что аналитическая служба фирмы является органом, который должен проводить мониторинг финансовой устойчивости и финансовой безопасности фирмы в оперативном режиме. Для этого аналитическая служба должна иметь эффективный механизм мониторинга. Этот механизм формируется из системы финансовых показателей, совокупность которых представляется индикаторами финансовой безопасности предприятия. В экономической литературе представлены наиболее популярные группы финансовых показателей, которые отображают состояние финансовой безопасности предприятия.

Состояние финансовой безопасности предприятия определяется большим количеством финансово-экономических показателей.

Попробуем выделить два их направления.

Первое направление определения финансовой безопасности предприятия – показатели финансовой безопасности.

Второе направление определения финансовой безопасности предприятия – показатели ликвидности активов.

Первое направление - показатели финансовой безопасности можно классифицировать и объединить в следующие четыре группы, исходя из их назначения. Это группа показателей платежеспособности, группа показателей финансовой устойчивости, показатели деловой активности и показатели рентабельности производства.

Детально разберем эти группы финансовых показателей, совокупность которых оценивает финансовую безопасность предприятия.

Первая группа: показатели платежеспособности:

- коэффициент обеспеченности собственными средствами;
- коэффициент восстановления платежеспособности;
- коэффициент утраты платежеспособности;
- коэффициент автономии;

- коэффициент маневренности собственного капитала.

Вторая группа: показатели финансовой устойчивости:

- коэффициент собственности (независимости);
- доля заемных средств;
- соотношение заемных и собственных средств.

Третья группа: показатели деловой активности:

- общий коэффициент оборачиваемости;
- скорость оборота;
- оборачиваемость собственных средств.

Четвертая группа: показатели рентабельности:

- имущество предприятия;
- собственные средства;
- производственные фонды;
- долгосрочные и краткосрочные финансовые вложения;
- собственные и долгосрочные заемные средства;
- норма балансовой прибыли;
- чистая норма прибыли.

Исходные данные для первичного анализа финансовой составляющей экономической безопасности предприятия представляются бухгалтерским балансом и формой №2. Этот анализ необходим не только для оценки текущего финансового состояния предприятия, но и для эффективного управления с целью обеспечения его финансово-хозяйственной устойчивости.

#### 1. Показатели платежной способности.

Показатели платежной способности отражают способность предприятия в течение финансового года погасить все краткосрочные долговые обязательства. Устойчивое финансовое развитие предприятия является одним из показателей его кредитоспособности. Коэффициенты платежной способности предприятия и их динамика позволяют определить наличие собственных средств предприятия и источников их формирования для покрытия кредитных обязательств в

будущем периоде.

1) коэффициент обеспеченности собственными средствами характеризует наличие у предприятия собственных оборотных средств, необходимых для обеспечения его финансовой устойчивости. Рекомендуемое значение для этого показателя составляет больше 1.

$$K_{оск} = \frac{СК - ВА}{ОА},$$

где СК – собственный капитал; ВА – внеоборотные активы; ОА – оборотные активы;

2) коэффициент восстановления платежеспособности отражает возможность предприятия восстановить свою платежеспособность в течение установленного срока.

$$K_{впл} = \frac{К_{тл} + 6 / T(К_{тл} - 2)}{2},$$

где  $K_{тл}$  - коэффициент текущей ликвидности;  $T$  - период времени (обычно 12 месяцев).

3) коэффициент утраты платежеспособности отражает возможность предприятия утратить свою платежеспособность в течение установленного срока.

$$K_{уп} = \frac{К_{тл} + 3 / T(К_{тл} - 2)}{2},$$

где  $K_{тл}$  - коэффициент текущей ликвидности;  $T$  - период времени (обычно 12 месяцев).

4) коэффициент автономии или коэффициент концентрации собственного капитала отражает долю владельцев (собственников) предприятия в общей сумме средств, используемых в финансово-хозяйственной деятельности. Чем выше значение коэффициента, тем более устойчиво и независимо от внешних кредиторов является предприятие. Формула расчета коэффициента автономии или коэффициента концентрации собственного капитала:

$$K_{кск} = \frac{СК}{ВБ},$$

где СК - собственный капитал; ВБ - валюта баланса, то есть сумма всех активов и пассивов на балансе предприятия.

5) Коэффициент маневренности собственного капитала отражает, какая

часть собственного капитала используется для финансирования текущей деятельности, а какая часть капитализирована. Формула расчета коэффициента маневренности собственного капитала:

$$K_{мск} = СОС / СК,$$

где СОС - собственные оборотные средства, то есть средства, вложенные в текущую операционную деятельность; СК - собственный капитал.

2. Показатели финансовой устойчивости отражают степень защищенности привлеченного капитала. Они включают в себя:

1) коэффициент собственности (независимости) ( $F_p$ ), который показывает долю собственных средств в общей стоимости основных средств:

$$F_p = RP / Rf,$$

где  $RP$  - собственные средства,  $Rf$  - стоимость основных средств.

2) коэффициент заемных средств ( $F_{rI}$ ) и

3) коэффициент заемных и собственных средств ( $F_{rIp}$ ). Оба показателя рассчитываются аналогично: в числителе указывается сумма заемных средств или сумма заемных и собственных средств, а в знаменателе – стоимость основных средств.

В странах с развитой рыночной экономикой для этих показателей установлены предельные значения:  $F_p > 0,7$ ;  $F_{rI} < 0,3$ ;  $F_{rIp} < 1$ .

3. Показатели деловой активности включают в себя

1) общий коэффициент оборачиваемости ( $F_{tkq}$ ),

2) скорость оборота

3) оборачиваемость собственных средств.

$$F_{tkq} = Grp / Cp$$

где  $Grp$  - выручка от реализации продукции,  $Cp$  - стоимость имущества (итог баланса).

Для оценки деловой активности предприятия используются и другие показатели. В странах с развитой рыночной экономикой устанавливаются нормативы для наиболее важных показателей деловой активности в целом и по отраслям.

Обычно такие нормативы отражают средние фактические значения этих коэффициентов. Например, в большинстве стран существуют следующие нормативы:

- норматив оборачиваемости запасов - три оборота, что соответствует 120  $Ftkq$  - 122 дням;
- норматив оборачиваемости дебиторской задолженности - 4,9, что соответствует примерно 74 дням.

Для расчета средней стоимости активов и пассивов за определенный период используется средняя хронологическая по месячным данным. Если финансовому аналитику доступен только годовой баланс, то для расчета используется упрощенный метод: среднее значение между данными на начало и конец периода.

4. Показатели оценки рентабельности включают в себя имущество предприятия, собственные средства, производственные фонды, долгосрочные и краткосрочные финансовые вложения, собственные и долгосрочные заемные средства, а также норму балансовой прибыли.

Формула расчета рентабельности имущества:

$$R_p = P_c / A \times 100\%$$

где  $R_p$  – рентабельность имущества,  $P_c$  - чистая прибыль,  $A$  - средняя стоимость имущества (активов).

Для постоянного контроля за экономической безопасностью предприятия руководству необходимы индикаторы, позволяющие быстро оценивать изменения. В практике наиболее информативными являются квартальные, ежемесячные или даже ежедневные промежуточные отчеты, которые оцениваются по тем же методикам, что и ежегодные. При достаточной плотности и взаимосвязи краткосрочные анализы могут быстро выявить сильные и слабые стороны положения предприятия и дать необходимые рекомендации для корректирующих мер. Информацию для анализа следует брать из открытых годовых и итоговых отчетов, включая:

- параметры деятельности предприятия, которые предшествовали

- банкротству или обеспечивали его интенсивное развитие;
- наличие возможности восстановить (или потерять) платежеспособность в течение определенного периода;
- причины финансовой неустойчивости, приведшие к неплатежеспособности предприятия;
- состояние ликвидности активов и их структуры.

Финансовое равновесие означает своевременное выполнение платежных обязательств перед бюджетом, сотрудниками и поставщиками материальных ресурсов, а также удержание факторов, которые могут дестабилизировать ситуацию.

Для обеспечения дальнейшего развития и совершенствования, особенно в современном динамично развивающемся мире, необходимо модернизировать производство, повышать профессиональный, образовательный и культурный уровень работников, расширять производство, диверсифицировать направления деятельности и вкладывать внутренние инвестиции. Это становится обязательным условием для обеспечения устойчивости и стабильности функционирования предприятия.

Второе направление определения финансовой безопасности предприятия – показатели ликвидности активов.

Для получения дополнительной информации о финансовой безопасности и устойчивости предприятия рассчитываются коэффициенты ликвидности активов, которые позволяют оценить способность компании погасить свои долговые обязательства в короткие сроки. Основными коэффициентами являются:

1. Коэффициент быстрой (промежуточной) ликвидности (Кбл) показывает, насколько компания может погасить свои краткосрочные обязательства за счет своих оборотных активов. Коэффициент рассчитывается по формуле:

$$\text{Кбл} = \text{ОА} - \text{З} / \text{КО},$$

где ОА - оборотные активы; З - запасы; КО - краткосрочные обязательства.

Рекомендуемое значение коэффициента быстрой (промежуточной) ликвидности составляет от 0,7 до 1,5.

2. Коэффициент текущей ликвидности (Ктл) показывает, достаточно ли у предприятия средств для покрытия краткосрочных обязательств в течение года. Он рассчитывается по формуле:

$$\text{Ктл} = \text{ОА} / \text{КО}$$

где где ОА – оборотные активы; КО – краткосрочные обязательства

Рекомендуемое значение коэффициента текущей ликвидности составляет от 1 до 2, что говорит о том, что у предприятия достаточно средств для покрытия своих текущих обязательств в течение года.

3. Коэффициент абсолютной ликвидности (Кабл) измеряет долю кредиторской задолженности, которую компания может выплатить немедленно.

$$\text{Кабл} = (\text{ДС} + \text{КФВ}) / \text{КО},$$

Где ДС - денежные средства; КФВ - краткосрочные финансовые вложения. Рекомендуемое значение Кабл составляет более 0,2.

## **Тема 7. Интеллектуальная и кадровая безопасность предприятия.**

Интеллектуальный потенциал современного предприятия открывает возможности для освоения и генерации инноваций. В общем, интеллектуальный потенциал представляет собой интеллектуальный капитал предприятия, который включает ресурсы, объединенные интеллектуальной природой.

Согласно исследованиям, человеческий капитал является наибольшей ценностью для предприятия в современных условиях хозяйствования. Он включает образование, знания, практические навыки, творческие и мыслительные способности, мотивацию, культурный уровень и моральные ценности, которые используются в процессе функционирования предприятия для получения прибыли.

Стремительный технический прогресс вместе с внедрением информационных технологий приводит к росту требований к качеству человеческого потенциала. Опыт демонстрирует, что для обеспечения конкурентоспособности предприятия все большее значение имеют не права собственности на материальные ценности, а факторы, способствующие инновационному развитию, повышению уровня интеллектуального потенциала. Интеллектуальный и кадровый потенциал не только являются движущей силой, способствующей эффективному функционированию предприятия, но могут также представлять угрозу для экономической безопасности организации.

В современных условиях развития экономики около 80% ущерба материальным активам предприятий наносится их же персоналом. Эта статистика учитывает только умышленный ущерб, но значительные убытки могут быть вызваны ошибками, неграмотным использованием ресурсов, недостаточной компетентностью и бездействием как руководителей, так и низшего звена, а также другими причинами.

Кадровая безопасность предприятия является сложным понятием, которое используется в различных значениях в экономической науке. Для использования в качестве базового понятия безопасности целесообразно раскрыть со-

держание этой категории через сочетание различных научных подходов отраслевой направленности.

Кадровая безопасность предприятия заключается в устранении рисков, вызванных с недобросовестной работой персонала, снижением уровня развития их интеллектуального потенциала и организацией трудовых отношений в целом. Важно отметить, что кадровая безопасность должна иметь приоритетное значение по отношению к другим элементам системы обеспечения экономической безопасности предприятия.

Несмотря на то, что в среде экономистов не существует единого определения кадровой безопасности предприятия – следует принять тот факт, что эта категория является производной экономической безопасности, то есть элементом экономической безопасности предприятий. Она достигается при наличии всех этапов организации и управления персоналом, направленных на установление таких трудовых и социокультурных отношений, которые обеспечивают безубыточную деятельность предприятия. Поэтому можно считать кадровую безопасность предприятия совокупностью таких составляющих, как профессиональная безопасность, антиконфликтная безопасность, безопасность жизнедеятельности, социально-мотивационная безопасность. Со своей стороны профессиональная безопасность это безопасность труда, информационная безопасность, интеллектуальная безопасность, пенсионно-страховая безопасность.

Антиконфликтная безопасность состоит из психологической, патриотической и коммуникационной безопасности. Безопасность жизнедеятельности это безопасность здоровья, физическая безопасность. Социально-мотивационная безопасность немного шире. Это финансовая, карьерная, технологическая, административная и эстетическая безопасность.

Кадровая политика предприятия должна основываться на определении потребностей в рабочей силе по количеству и качеству, а также на выборе форм ее привлечения и использования. Это включает повышение квалификации, постоянное развитие персонала, создание условий для стимулирования

высокопроизводительного труда и предотвращение появления неблагонадежных сотрудников. Неблагонадежность является динамическим процессом, который меняется со временем под влиянием внешних и внутренних факторов и отражает готовность индивида принимать действия, которые могут быть расценены как нарушение существующих норм и традиций в его социокультурной среде.

Снижение кадровых рисков связано с высоким уровнем дисциплины, ростом численности квалифицированных кадров, снижением текучести кадров, достижением высокого образовательного уровня и компетентностью руководителей. Эти факторы являются направлениями, обеспечивающими экономическую безопасность предприятия. Поэтому уровень образования персонала на сегодняшний день является одним из показателей экономической безопасности.

Для обеспечения кадровой безопасности предприятия необходимо проводить комплекс мероприятий, направленных на устранение или снижение воздействия внутренних и внешних угроз и рисков.

Внешние угрозы - это та категория угроз, с которой практически невозможно бороться и противопоставить ей чего-либо. Тем не менее, своевременное выявление внешних угроз помогает принимать оперативные решения и минимизировать возможные последствия. Например, если конкурирующее предприятие имеет более эффективную кадровую политику и более высокий уровень мотивации, то ценный сотрудник может уйти на это предприятие, что может привести к большему ущербу, чем просто потеря сотрудника. Кроме того, могут возникать угрозы коммерческой тайны и целенаправленного переманивания сотрудников предприятием-конкурентом. Инфляционные процессы также являются внешней угрозой, которую необходимо учитывать при определении уровня заработной платы и прогнозировании ее уровня в будущем.

Среди наиболее распространенных внутренних угроз кадровой безопасности предприятия можно выделить: слабую организацию системы обучения, несоответствие уровня квалификации сотрудников требованиям, низкий уровень

контроля за новыми сотрудниками и неэффективную корпоративную политику предприятия.

Раздельно или совместно внутренние и внешние угрозы могут нанести предприятию серьезный материальный ущерб. Обеспечение кадровой безопасности на предприятии является одним из приоритетов для достижения стабильности и процветания не только отдельного предприятия или группы предприятий, но и экономической системы государства. В настоящее время предприятия различных форм собственности сталкиваются с ростом угроз со стороны собственного персонала, что ухудшает их экономическую безопасность вследствие увеличения рисков в управлении персоналом. Эти риски могут привести к финансовым потерям предприятия, а также к полной потере владельцами собственности.

Систематизация факторов, которые могут привести к угрозе кадровой безопасности предприятия, показала, что к внешним угрозам можно отнести:

- лучшие условия мотивации у конкурентов;
- попытки конкурента «переманить» сотрудников;
- внешнее давление на сотрудников и вовлечение их в различные зависимости;
- инфляционные процессы, которые также следует учитывать при расчете заработной платы.

Внутренние угрозы кадровой безопасности предприятия могут включать в себя:

- несоответствие квалификации сотрудников занимаемой должности;
- недостаточную квалификацию работников;
- отсутствие системы оценки персонала;
- слабую организацию системы обучения;
- неэффективную систему мотивации;
- ошибки в планировании ресурсов персонала;
- отсутствие творческих элементов в работе;
- нецелевое использование квалифицированных сотрудников.

Эффективная кадровая работа на предприятии создает предпосылки кадровой безопасности, что является залогом успешной работы всех производственных звеньев. Главная задача состоит в том, чтобы свести к минимуму человеческий фактор, нейтрализовать риск негативного воздействия персонала на эффективность работы предприятия. Для этого необходимо на предприятии создать механизм поддержания кадровой безопасности, включающий следующие положения:

- сочетание материального вознаграждения с моральным поощрением;
- создание достойных условий труда и отдыха работников;
- обеспечение карьерного роста персонала;
- осуществление и контролирование стратегического планирование кадрового и интеллектуального потенциала предприятия;
- обеспечении заинтересованности персонала в высоких конечных результатах деятельности предприятия;
- согласовывать рыночные условия развития бизнеса и интересы сотрудников предприятия;
- установление зависимости размера оплаты труда от производственных инноваций, результатов НИОКР и ноу-хау на предприятии.

## **Тема 8. Индикаторы интеллектуальной и кадровой безопасности предприятия**

Интеллектуальный и профессиональный уровень кадров оказывает значительное влияние на достижение надлежащего уровня экономической безопасности предприятия. Кадровая служба и главный инженер отвечают за интеллектуальную составляющую экономической безопасности на предприятии.

Для обсуждения критериев кадровой безопасности важно рассмотреть некоторые количественные параметры экономической безопасности компании.

Реализация концепции и стратегии экономической безопасности предусматривает разработку системы мер и механизмов на основе анализа результатов мониторинга качественных и количественных критериев. Иногда устанавливаются сигнальные показатели с пороговыми значениями, которые помогают предотвратить негативные тенденции в экономической и кадровой безопасности. Эти сигнальные показатели называются индикаторами.

Индикатор - это количественная или качественная оценка состояние какого-либо объекта, с помощью которой определяется объект. Индикаторы экономической безопасности предприятия - это показатели, которые помогают оценить уровень экономической безопасности предприятия и выявить его проблемные зоны. Они также позволяют определить пути и способы повышения эффективности предприятия.

Показатели-индикаторы уровня экономической безопасности предпринимательства должны количественно отражать уровень угрозы и обладать значительной чувствительностью для предупреждения возможной опасности. Целесообразно использовать систему индикаторов вместо отдельных показателей. Это позволит определить уровень внутренних и внешних угроз объекта с наибольшей точностью и вероятностью.

Надежность применения индикаторов при оценке системы экономической безопасности предприятия достигается широким охватом индикаторами исследуемой тематики. Накопление числовых параметров такой совокупности

показателей необходимо для мониторинга и прогнозирования экономической безопасности предпринимательской деятельности, оценки значимости тех или иных конкретных угроз.

Критические значения исходных показателей определяются на основе минимально допустимого уровня безопасности, так как превышение этого уровня может привести к переходу в экономически опасную зону.

В отношении интеллектуальной и кадровой составляющей обеспечения экономической безопасности предприятия рекомендуется выделить основные группы индикаторов, которые оказывают прямое влияние на эффективность функционирования предприятия. Это:

1. Группы индикаторов качества мотивационной системы предприятия (показатели оплаты труда, уровень льгот сотрудникам, стоимость затрат на обучение персонала и т.д.),
2. Группа индикаторов состояния интеллектуального потенциала предприятия (показатели образовательного уровня персонала, количество изобретений и рационализаторских предложений на одного работника, количество патентов и т.д.),
3. Группа индикаторов эффективности принимаемых мер по обеспечению экономической безопасности предприятия по ее интеллектуальной и кадровой составляющей (показатель, рассчитываемый на основе карты расчета эффективности принимаемых мер по методике оценки ущербов).

При анализе различных групп индикаторов, используемых для определения влияния интеллектуальной и кадровой составляющей на экономическую безопасность предприятия, необходимо учитывать не только значения показателей, но и их динамику. Если наблюдается негативная тенденция, то необходимо определить ключевые факторы, которые оказывают наибольшее влияние на изменение показателей. Это позволит разработать комплекс мероприятий для устранения недостатков и нивелирования негативного влияния конкретных факторов.

Учитывая различия в потребностях анализа для предприятий разных видов деятельности, связанных с отраслевыми особенностями, спектр возможных индикаторов интеллектуальной и кадровой безопасности предприятия может быть изменен.

Повышение кадровой безопасности предприятия предусматривает ряд важных мероприятий, включающих:

- привлечение талантливой молодежи на предприятие;
- проведение ежегодных конкурсов среди выпускников вузов на занятие перспективных должностей;
- разработку механизма закрепления перспективных сотрудников;
- организацию института наставничества;
- управление карьерой сотрудников;
- рост числа функциональных руководителей;
- приведение уровня оплаты труда в соответствие с вкладом каждого работника в повышение эффективности предприятия;
- внедрение системы мотивации перспективных сотрудников и другие меры.

Если значения показателей превышают пороговые значения, то это является сигналом к действию по предотвращению угрозы, снижению ущерба или прекращению вредоносных атак. Для достижения максимальной степени безопасности необходимо, чтобы все показатели находились в пределах допустимых границ своих пороговых значений. Основными группами критериев, относящимися к кадровой безопасности, являются:

- численный состав персонала и его динамика;
- квалификация и интеллектуальный потенциал сотрудников;
- эффективность использования персонала;
- качество мотивационной системы.

Для обеспечения кадровой безопасности служба персонала, после установления критериев и определения их параметров, должна:

- 1) разрабатывать текущие и плановые значения показателей кадровой

безопасности для стратегического и оперативного планирования;

2) постоянно отслеживать установленные показатели в своей области ответственности;

3) предоставлять отчетность о состоянии своих критериев с разной периодичностью и в определенном объеме данных;

4) незамедлительно извещать соответствующие службы об отрицательных отклонениях значений показателей от нормативных величин;

5) участвовать в разработке и реализации мероприятий по стабилизации параметров и сценариев.

Мониторинг необходим для выявления и прогнозирования неблагоприятных воздействий на объекты экономической безопасности. Негативные явления и процессы могут проявляться в:

- отклонениях контрольных показателей от пороговых значений в отрицательную сторону;

- увеличении динамики установленных показателей сверх допустимых значений;

- необъяснимых финансовых, технологических и информационных явлениях и процессах;

- возникновении форс-мажорных обстоятельств;

- негативном поведении отдельных сотрудников и групп;

- конфликтных ситуациях между внутренними и внешними субъектами бизнеса;

- подозрительном интересе со стороны внешних субъектов к деятельности компании, ее персонала, руководства, информации, материальных и денежных средств;

- фактах хищений, повреждений имущества, пропажи денег и документов, других неправомерных действиях;

- попытках незаконного доступа и использования корпоративной информации;

- возникновении проблем безопасности руководства и сотрудников

предприятия.

Важно отметить, что все должностные лица и сотрудники обязаны незамедлительно информировать службу безопасности о выявленных отклонениях, а в некоторых случаях, указанных во внутренних документах, - сообщать непосредственно руководству. Отсутствие принятых соответствующих мер может повлечь за собой определенную ответственность.

Обеспечение интеллектуальной и кадровой безопасности предприятия включает несколько взаимосвязанных, но одновременно самостоятельных направлений деятельности.

Первое направление нацелено на работу с персоналом фирмы и на повышение эффективности его деятельности.

Второе направление нацелено на сохранение и развитие интеллектуального потенциала (права на интеллектуальную собственность, знания и профессиональный опыт работников).

Следует рассматривать следующие основные объекты интеллектуальной собственности:

1. Изобретения;
2. Технические и организационные новации;
3. Know-how;
4. Дизайн и товарные знаки;
5. Методики;
6. Аудио и видео продукция;
7. Компьютерные программы;
8. Другие разработки и объекты интеллектуальной собственности.

Из-за сильного сходства деятельности по сохранению и развитию интеллектуального потенциала предприятия и обеспечению информационной составляющей экономической безопасности компании, планирование и реализация мер по защите этих аспектов экономической безопасности должны проводиться в тесном контакте и сотрудничестве всех работников предприятия.

Кадровая безопасность означает защиту интересов организации, направленных на развитие и улучшение ее человеческого капитала, обеспечение эффективной системы управления персоналом и снижение рисков, связанных с кадровой составляющей компании. Кадровая безопасность определяется как состояние организации в ее социальном и индивидуальном аспектах, при котором воздействие природной, экономической и социальной среды, а также внутренней среды человека не может нанести вреда.

В настоящее время для оценки интеллектуальной и кадровой безопасности также широко применяется индикаторный метод, который отличается простотой использования и позволяет получать наглядные результаты. Это дает возможность принимать правильные управленческие решения. Индикатор представляет собой характеристику или признак объекта, который может быть выражен в количественной форме и используется для его оценки.

Суть индикаторного метода оценки кадровой безопасности заключается в определении индикаторов состояния кадровой безопасности предприятия и установлении их максимально допустимых значений. Отклонение от этих норм может привести к нарушению функционирования системы кадровой безопасности.

Наивысший уровень безопасности достигается, если все показатели находятся в пределах своих пороговых значений, определяемых как допустимые границы.

Качество оценки уровня кадровой безопасности сильно зависит от правильного определения пороговых значений индикаторов, выбранных для оценки. Пороговое значение представляет собой максимально допустимую величину индикатора, превышение которой свидетельствует о нарушении процесса обеспечения кадровой безопасности. Пороговое значение является нормативом, а величина отклонения от этого норматива отражает уровень угроз КБ.

В научном сообществе до сих пор нет единого мнения о том, каким должен быть состав и уровень пороговых значений кадровой безопасности, так

как используются разные методы для их нормирования. Один из наиболее распространенных методов - метод нормирования пороговых значений, который основывается на понятии неприемлемого ущерба. Однако, главная проблема при использовании этого подхода заключается в сложности оценки возможных экономических потерь, связанных с превышением допустимых пороговых значений, определенных индикаторами кадровой безопасности.

Пороговые значения индикаторов могут быть определены с использованием нескольких методов. Это

1. метод функциональных взаимосвязей,
2. метод аналогий,
3. задающий метод,
4. экспертный метод.

Метод функциональных взаимосвязей устанавливает более жесткие нормы. Методом аналогий, пороговые значения на конкретном предприятии определяются на основе анализа значений, полученных от отечественных и зарубежных предприятий, работающих в данной отрасли, за предыдущие годы. Задающий метод предполагает определение пороговых значений в зависимости от целей, которые стоят перед предприятием. В экспертном методе нормативные значения определяются на основании мнения экспертов.

Применение методов определения пороговых значений кадровой безопасности сопряжено с трудностями, поскольку не все индикаторы могут быть вычислены с помощью четких математических методов. Кроме того, различные индикаторы отличаются своим содержанием и характером, что требует использования множества методов для расчета их пороговых значений.

Существует несколько факторов, которые влияют на формирование пороговых значений кадровой безопасности, включая:

- Финансовую стабильность предприятия.
- Качественный и количественный состав трудовых ресурсов.
- Показатели движения персонала, такие как коэффициенты текучести кадров и постоянства.

- Кадровую политику, включая оптимизацию численности персонала, подсистемы развития, адаптации и мотивации.

- Уровень профессиональной подготовки руководителей.

- Состояние регионального рынка труда.

- Уровень развития научно-технического прогресса и информационных технологий.

- Нормативно-правовую базу в сфере трудового, административного и уголовного права.

При определении пороговых значений индикаторов кадровой безопасности (КБ) необходимо учитывать состояние экономики государства в каждый конкретный момент времени. Проблемы безопасности становятся более острыми в периоды кризисов и структурных преобразований, поэтому предельно допустимые показатели могут изменяться.

Следовательно, создание унифицированных пороговых значений, которые бы объективно отражали уровень кадровой безопасности, не является целесообразным.

Предельные значения, которые характеризуют высокий уровень кадровой безопасности на одном предприятии, могут быть относительно низкими и не отвечать надлежащему уровню кадровой безопасности на другом предприятии. Несмотря на возможные различия в пороговых значениях индикаторов кадровой безопасности, алгоритм их определения будет идентичным для всех предприятий.

Для определения пороговых значений индикаторов кадровой безопасности применяется следующий алгоритм:

1. Оценка внешней среды предприятия и возможных угроз.
2. Анализ внутренней среды предприятия и возможных угроз.
3. Сбор статистических данных о фактических значениях показателей безопасности.
4. Определение косвенных оценок и промежуточных показателей.
5. Построение динамических рядов.

6. Оценка показателей одним из вышеописанных методов и выявление закономерностей.

7. Установление пороговых значений индикаторов кадровой безопасности.

Установление пороговых значений индикаторов кадровой безопасности может осуществляться двумя подходами:

1. определение минимально возможного значения и
2. установление максимально возможного значения.

В первом случае вектор оптимизации значения индикатора будет направлен вверх, а во втором случае - вниз. Однако на практике для обеспечения достаточности и необходимости индикаторов оценки лучше всего использовать оба подхода.

Базовые индикаторы кадровой безопасности и рекомендуемые пороговые значения следующие:

1. Показатели состава и движения персонала

Индикаторы:

- Коэффициент текучести кадров,
- Образовательный состав персонала

Направление оптимизации – min

Рекомендуемый порог - 10%

2. Показатели инвестирования в персонал

Индикатор:

Издержки на обучение в общем объеме издержек на персонал

Направление оптимизации- max

Рекомендуемый порог - 100%

3. Показатели мотивации персонала

Индикаторы:

- Степень удовлетворенности оплатой труда,
- Удельный вес оплаты труда в общем объеме издержек организации

Направление оптимизации – min, max

Рекомендуемый порог – 10%, 100%.

#### 4. Показатели условий труда

Индикаторы:

- Наличие профзаболеваний
- Уровень автоматизации труда

Направление оптимизации – min, max

Рекомендуемый порог – 3%, 70%.

#### 5. Личностные показатели

Индикаторы:

- Доля персонала, не имеющего нарушений трудовой дисциплины
- Вероятность сохранения коммерческой тайны

Направление оптимизации – max, max

Рекомендуемый порог –100%, 100%.

Оценка кадровой безопасности предприятия должна проводиться регулярно, и необходимо отслеживать динамику фактических значений индикаторов во времени. При проведении анализа кадровой безопасности предприятия важно помнить, что большинство показателей должны находиться в пределах допустимых границ, только в этом случае можно говорить о стабильном уровне кадровой безопасности.

Если один или несколько показателей приближаются к своему предельно допустимому значению, это указывает на нарастание угроз кадровой безопасности, а если пороговое значение превышено, то предприятие вступает в зону повышенного риска.

Если предприятие превысит пороговые значения, оно потеряет способность нормально функционировать, динамично развиваться и противостоять конкурентам.

Также необходима регулярная корректировка как самих индикаторов кадровой безопасности, так и их пороговых значений, учитывая влияние различных факторов внутренней и внешней среды на функционирование предприятия.

На основе результатов оценки кадровой безопасности разрабатывается

стратегия кадровой безопасности предприятия, которая включает в себя приоритетные цели и управленческие подходы, обеспечивающие защиту организации от всех угроз, связанных с кадровым направлением ее деятельности.

Эта стратегия кадровой безопасности является важной частью организационной стратегии экономической безопасности и должна учитываться при формировании кадровой политики предприятия.

## **Тема 9. Экологическая безопасность предприятия**

В свете экологических проблем в настоящее время остро встает вопрос выживаемости человечества на земле. Эта проблема затрагивает не только политиков, но и экономистов, социологов, правоведов. Имея много граней проблема экологии сводится к решению задачи сохранения окружающей среды хотя бы в том виде, что мы имеем и не увеличивать нанесения вреда природе в результате деятельности человека. В условиях экологического кризиса, охвативший весь земной шар, достижение поставленной цели является сложной задачей. В этой связи в обиход плавно и естественно вошло понятие экологическая безопасность. Она стала главной среди множества видов безопасности, хотя бы потому, что на кону поставлена сохранение жизни на земле.

Многие экологи и специалисты смежных профилей определяют экологическую безопасность как процесс согласование взаимодействия человека и окружающей среды. Важным компонентом такого согласования выступает условие включения в деятельность человека природоохранных компонентов и создание оптимальной для жизни человека среды обитания. И хотя данное определение экологической безопасности оставляет нераскрытыми множество аспектов проблемы - с большими допусками можно согласиться с выше-приведенным определением экологической безопасности.

Принимая общее определение экологической безопасности, как процесс согласование взаимодействия человека и окружающей среды, можно экологическую безопасность предприятия сформулировать как соответствие его (предприятия) природоохранной деятельности определенным нормативным требованиям. В свете растущей экологической ответственности, экологическая безопасность предприятия имеет большое значение для окружающей среды и населения и является важным фактором конкурентоспособности предприятия.

Экологическая безопасность тесно связана с контролем в области охраны окружающей среды, или экологический контроль, который представ-

ляет собой систему мер, направленных на предотвращение, выявление и пресечение нарушений законодательства в области охраны окружающей среды, а также на обеспечение соблюдения субъектами хозяйственной и иной деятельности требований, включая нормативы и нормативные документы в области охраны окружающей среды.

В настоящее время экологическая безопасность, являясь самостоятельным и очень важным видом безопасности играет значительную роль в обеспечении экономической безопасности предприятий. Повсеместное ухудшение экологической обстановки представляет серьезную проблему для человечества, которую можно решить путем перехода к инновационным (безотходной или малоотходной) технологиям производства. Совместно с внедрением новых технологий в хозяйственную и другую деятельность увеличивается ущерб, наносимый окружающей среде. Это всем известное загрязнение атмосферы, эрозия и загрязнение почв, вырубка лесов, разрушение озонового слоя, гибель и вымирание многих видов животных, нарушение экологии мирового океана, гибель крупных водоемов и других катастроф.

Эти и многие другие последствия деструктивной деятельности людей в отношении природы представляют реальные угрозы для существования не только человеческой расы, но всего живого на земле.

Основными источниками загрязнения окружающей среды являются:

- промышленные компании, которые выделяют загрязненные отходы в процессе производства;
- испытания различных видов оружия;
- государственные программы технологического развития, которые недостаточно учитывают негативные побочные эффекты в экологическом аспекте.

Проблему экологической безопасности можно рассмотреть на уровне национальной экономики и на уровне деятельности предприятий. Решение проблемы экологической безопасности на обоих уровнях требует разработки общемировых правил и стандартов сохранения окружающей среды. Требуется

выработка единых норм содержания вредных веществ и отходов производства, а также экологических параметров производимой продукции, вместо индивидуальных, региональных или национальных систем. Это связано с тем, что возможно ослабление контроля за соблюдением экологических норм вредных выбросов и чистоты производимой продукции под влиянием промышленных лобби. Поэтому необходима обязательная интернационализация норм минимального содержания вредных веществ.

Подтверждением целесообразности введения и применения мировых стандартов является тот факт, что квалификационный уровень специалистов в этой области на международном уровне значительно выше, чем на национальном уровне.

Нарушение экологических норм одной или нескольких стран может причинить вред экологии соседних стран.

Практика показывает, что предприятия не желают добровольно вводить меры для обеспечения экологического контроля за производственным процессом и производимой продукцией. Такое поведение компаний объясняется тем, что соблюдение экологических норм требует дополнительных затрат, связанных, например, с установкой очистных сооружений или переориентацией технологии на производство экологически чистой продукции.

Поскольку коммерческие интересы обычно преобладают в деятельности предприятий, большинство стран использует системы штрафов за нарушение национального экологического законодательства, чтобы обеспечить соблюдение экологических норм.

Стоит отметить, что нормы содержания вредных веществ, действующие для отечественных предприятий в Узбекистане менее строгие по сравнению со странами-членами Европейского союза. Это объясняется наличием объективных и субъективных обстоятельств. К объективным причинам относятся то, что на производствах республики до сих пор функционируют физически и морально устаревшие оборудования, которые являются энергозатратными и

малоэффективными. Очевидно, что промышленные предприятия с таким техническим потенциалом не в состоянии обеспечивать выполнения высоких экологических норм по содержанию вредных веществ в отходах производства. Кроме того обеспечение экологической безопасности возможна при наличии высококвалифицированных специалистов экологов.

Назрела необходимость подготовки отечественных высококвалифицированных экономистов-менеджеров в области природопользования и включения должности экономиста-менеджера в области природопользования в штатное расписание предприятий. Это важно, если вспомнить, что функционирование предприятия и ведение природоохранной деятельности в соответствии с нормативными требованиями сопровождается ростом конкурентоспособности предприятия.

Экологическая экспертиза играет важную роль в обеспечении экологической безопасности предприятий. Это означает, что проводится оценка соответствия экологическим требованиям предполагаемой хозяйственной и другой деятельности и определяется допустимость дальнейшего функционирования данного предприятия.

Перечислим основные требования экологической экспертизы. Они базируются на следующих правилах:

- Предполагается, что любая хозяйственная или другая деятельность представляет потенциальную экологическую опасность;
- Принятие решения о реализации объекта должно предшествовать проведению государственной экологической экспертизы;
- Осуществляется комплексная оценка воздействия хозяйственной и другой деятельности на окружающую среду и ее последствий;
- Требования экологической безопасности учитываются при проведении экологической экспертизы;
- Информация, представляемая на экологическую экспертизу, должна быть достоверной и полной;
- Эксперты экологической экспертизы должны быть независимыми при

осуществлении своих полномочий;

- Заключение экологической экспертизы должны быть научно обоснованными, объективными и законными;

- Общественные организации и объединения должны иметь возможность участвовать в экологической экспертизе;

- Участники экологической экспертизы и заинтересованные лица должны нести ответственность за организацию, проведение и качество экологической экспертизы.

В целях объективности и непредвзятости целесообразно осуществления двух видов экологической экспертизы - государственной и общественной.

Экологический менеджмент применяется для управления производственной деятельностью промышленных предприятий с целью защиты окружающей среды от загрязнения и обеспечения оптимального природопользования.

Экологический менеджмент является неотъемлемой частью системы регулирования охраны природы и является важным условием для успешной и быстрой санации окружающей среды. Он включает в себя государственное, общественное и рыночное экологическое регулирование на всех уровнях управления, включая предприятия, регионы, страны и мировое сообщество.

Экологический менеджмент на предприятии выполняется в три этапа:

- 1 этап - определение состояние и оценка влияния производственной деятельности на окружающую среду;

- 2 этап - разработка стратегии и программы по защите окружающей среды на предприятии;

- 3 этап - определение целей, способов и сроков реализации программы (например, сокращение выбросов вредных веществ, улучшение использования ресурсов, внедрение малоотходных и безотходных технологий и т.д.).

Внедрение механизма экологического менеджмента позволит предприятию в процессе уменьшения вредных выбросов в окружающую среду, выявить резервы экономии сырья, энергии, воды, утилизации отходов, снижения

себестоимости продукции и, как неоднократно указывалось, поднять конкурентоспособность предприятия.

Опыт добровольного участия предприятий в системе экологического менеджмента подтверждает экономическую выгодность такого участия. Экологический менеджмент на предприятии играет важную роль в решении глобальных экологических проблем. Требования, предъявляемые Европейским союзом к предприятиям, принимающим участие в системе, распространяются на их партнеров и поставщиков, независимо от страны происхождения, что позволяет привлечь широкий круг предприятий в систему экологического менеджмента и, следовательно, улучшить состояние окружающей среды.

Для контроля за экологическим состоянием окружающей среды на предприятии используется экологический аудит.

Экологический аудит (экоаудит) является неотъемлемой частью системы экологического менеджмента и представляет собой объективную, систематическую, документированную и периодически проводимую проверку состояния окружающей среды на предприятии. Он основывается на сравнении результатов, достигнутых предприятием в области экологии. Экологический аудит, как правило, включает независимые исследования технологий производства.

Участие в экологическом аудите подразумевает организацию охраны окружающей среды на всех уровнях функционирования предприятия, охватывая:

- энергетические расходы;
- использование сырья;
- технологические процессы производства;
- производство и выпуск продукции;
- поставки и сбыт;
- транспортировку;
- управление отходами всех типов.

Концепция проведения экологического аудита на предприятии была

предложена впервые в США в середине 1970-х годов. Однако практическое внедрение этой идеи началось в Европейском союзе в июле 1993 года. Процесс экологического аудита на предприятии включает несколько этапов:

1 этап – проведение регулярных проверок состояния окружающей среды и сопоставление результатов с программой предприятия по охране окружающей среды;

2 этап- установление соответствия состояния окружающей среды требованиям экологического законодательства, общественности и поставленным целям.

3 этап- доведение до общественности результаты проверки публикуемой в экологической декларации;

4 этап- проведение независимым эоаудитом проверки всей системы экологического менеджмента;

5 этап- выдача предприятию сертификат участника системы экологического менеджмента при условии положительного результата проверки эоаудита. Сертификат способствует росту репутации предприятия, позволяет получить ряд льгот и преференций (доступ к выгодным кредитам, лучшие условия страхования, повышает конкурентоспособность на рынке).

## **Тема 10. Оценка эффективности экологической безопасности предприятия**

Предприятие, функционирующее в условиях рыночной экономики оценивается множеством параметров социально-экономического характера. Это делается с целью выявления картины современного состояния и обоснованной перспективы развития предприятия. Экологические аспекты предприятия, являясь важной составной частью ее деятельности, должны также оцениваться системой показателей, что позволяет определять эффективность работ по природоохранной деятельности предприятия. Для оценки экологической безопасности предприятия необходим комплексный подход, который требует пересмотра принципов построения системы показателей. Основная цель системы показателей - преобразовать различные виды информации (нормативной, плановой, финансовой, юридической, учетной) в такие критерии, которые позволяют понять суть процесса и оценить масштаб изменений, происходящих в нем.

Для создания эффективной системы оценочных инструментов экологической безопасности предприятия показатели и критерии, входящие в эту систему, должны удовлетворять трем условиям:

Первое условие. Показатели должны быть пригодными для использования, т.е. простыми, понятными, иметь физический смысл и быть выражены в количественной форме или через логическую характеристику.

Второе условие. Показатели должны быть эффективными, т.е. польза от показателя должна превышать затраты на его получение. Некоторые критерии, основанные на статистических данных, могут быть теоретически правильными, но требуют сложных расчетов и длительных экспериментов, что делает их непрактичными.

Третье условие. Показатели должны быть доступными для получения, т.е. их можно будет получить из конкретных форм отчетности, внутренней информации и доступной внешней информации, чтобы обеспечить возможность проведения анализа.

Экологический менеджмент направлен на обеспечение безопасности деятельности предприятия и снижение негативного воздействия на окружающую среду. На первом этапе оценки экологической безопасности предприятия рекомендуется дать общую количественную оценку воздействия предприятия на окружающую среду. Этому может служить выявление:

1. степени экологичности производства,
2. степени экологичности продукции.

Для определения степени экологичности производства можно использовать коэффициент экологичности производства, который вычисляется по формуле:

$$K_{\text{эк.пр.}} = Z_{\text{охр}} / Z_{\text{общ}},$$

где:

*K<sub>эк. пр.</sub>* – коэффициент экологичности производства;

*Z<sub>охр</sub>* - это затраты компании на природоохранную деятельность (охрану атмосферного воздуха, водных ресурсов, земельных угодий);

*Z<sub>общ</sub>* - это общие затраты за определенный период времени.

Для определения степени экологичности продукции можно использовать коэффициент экологичности продукции, который вычисляется по формуле:

$$K_{\text{эк.прод}} = P_{\text{серт}} / P_{\text{общ}},$$

где:

*K<sub>эк. прод.</sub>* – коэффициент экологичности продукции;

*P<sub>серт</sub>* - это объем продукции, сертифицированной на экологичность и безопасность;

*P<sub>общ</sub>* - это общий объем выпущенной продукции.

Если продукция, производимая предприятием, будет более экологичной, то это даст ему преимущество в конкурентной борьбе за покупателей и клиентов.

Сегодня западные корпорации считают в соответствии с «концепцией устойчивого развития», что состояние окружающей среды в начале и конце

отчетного периода должно быть одинаковым, то есть не ухудшаться. Впервые термин "экоэффективность" был введен Всемирным экономическим форумом по устойчивому развитию. Экоэффективный режим работы предприятия позволяет снизить воздействие на окружающую среду и, в то же время, повысить его рентабельность.

Экоэффективность может быть точно измерена с помощью экологического учета и анализа, который предоставляет точную информацию о природоохранных расходах, сбережениях и воздействии хозяйственной деятельности на окружающую среду.

Экоэффективность измеряется коэффициентом экологической эффективности формуле:

$$\text{Кэк.эф.} = \text{Фин.рез} / \text{Экол.р.},$$

где :

Кэк. эф. – коэффициент экологической эффективности;

Фин.рез. - это финансовый результат, достигнутый в производственной деятельности, т.е. прибыль от продажи (или производственный результат - выручка от продажи продукции);

Экол.р. - это экологический результат, полученный от данного производственного процесса (количество затраченной энергии, выброшенных в атмосферу газов, потребленной воды и т.д.).

Экоэффективность представляет собой эффективность, которая одинаково учитывает экологические и экономические аспекты, отражая производительность природных ресурсов. Концепция экоэффективности означает удельное воздействие предприятия на окружающую среду в расчете на прибыль или произведенную продукцию, такие как потребление энергии на единицу продукции или величина прибыли на тонну выброшенного в атмосферу углекислого газа. Экоэффективность является относительной комплексной величиной, которая отражает соотношение между экологической и финансовой эффективностью. Принцип экоэффективности заключается в том, что предприятие стре-

мится достичь экономической выгоды путем снижения воздействия на окружающую среду и уменьшения использования природных ресурсов.

При оценки экологических аспектов деятельности организации необходимо учитывать как финансовые, так и экологические параметры. Оценка финансовых параметров природозащитной деятельности достигается следующими количественными критериями:

1. Текущие затраты на охрану окружающей среды,
2. Экологические платежи,
3. Затраты, направленные на повышение экологической эффективности внедряемых производственных и технологических решений,
4. Преимущества, получаемые от экологических улучшений.

Текущие затраты на охрану окружающей среды это затраты на охрану и рациональное использование водных ресурсов, атмосферного воздуха, окружающей среды от отходов производства и потребления, рекультивацию земель, а также затраты на капитальный ремонт основных фондов по охране окружающей среды. Экологические платежи включают плату за допустимые и сверхнормативные выбросы загрязняющих веществ, а также средства и штрафы, взысканные в возмещение ущерба, причиненного нарушением природоохранного законодательства.

Экологические параметры могут быть описаны качественными критериями, включающими:

- Здоровье и безопасность людей;
- Потенциальные экологические риски;
- Экологические происшествия;
- Нагрузку на окружающую среду (выбросы, утечки, отходы), а также тенденции изменения этих показателей со временем;
- Соответствие экологическим требованиям законодательных и нормативных актов;
- Рациональное использование материальных ресурсов.

Если требуется провести детальную оценку экологической безопасности предприятия, можно использовать подход, при котором используются показатели эффективности информации о экологической безопасности предприятия и показатели эффективности управления обеспечения информации о действиях, предпринимаемых руководством для воздействия на экологическую безопасность предприятия.

При оценке экологической эффективности функционирования и управления предприятием выделяются важные аспекты, которые зависят от конкретной ситуации. Это позволяет составить список индикативных показателей окружающей среды. Номенклатура таких показателей должна быть технически обоснована и отражать технологический процесс.

Для описания конкретного состояния окружающей среды необходимо использовать абсолютные, удельные, относительные и агрегированные значения. При выборе таких показателей следует учитывать тот факт, что они должны показывать изменения в короткие временные промежутки, показывать тенденции ухудшения состояния окружающей среды и показывать направленность на достижение конкретных целей.

Для более детальной оценки экологической безопасности предприятия можно использовать множество показателей в соответствии с возможностями, интересами и потребностями предприятия. Для этого потребуются определить производственные факторы, которые оказывают негативное воздействие на окружающую среду. Перечень этих факторов следующий:

1. *Фактор эксплуатация природных ресурсов,*
2. *Фактор использование земель,*
3. *Фактор использование атмосферы,*
4. *Фактор использование водных ресурсов,*
5. *Фактор размещение отходов,*
6. *Фактор лимитов техногенной нагрузки на ландшафтные сообщества,*
7. *Фактор воздействия на человека,*
8. *Фактор эстетического характера,*

## *9. Фактор условий сохранения животного мира.*

Список производственных факторов, которые оказывают негативное воздействие на окружающую среду определяется для каждого предприятия индивидуально. Здесь принимается во внимание возможности, интересы и потребности предприятия, масштабы и типы производства, используемыми материалы и энергоносители, наличие выбросов в окружающую среду, степень экологического риска, вероятность аварийных ситуаций и требования обязательных законодательных и нормативных актов прочие условия.

В заключении следует отметить, что система информационного обеспечения управления экологической безопасностью предприятия является сложным механизмом. Она включает нормативные, плановые и прогнозные данные, справочную и информационный базу, базу учетной системы. Эффективное функционирование информационной системы немислимо без автоматизации этих процессов и использовании на практике соответствующих компьютерных программ. Процессы получения данных, расчет количественных показателей и обработки качественных критериев используются предприятиями в автоматизированной режиме. Во многих современных предприятиях мира произведена цифровизация всех этих процессов и работа осуществляется дистанционно. Для сбора и обработки информации по трудоемким участкам используется выборочный метод с экстраполяцией результатов на весь исследуемый объект.

Использование системы показателей экологической безопасности позволит выявлять и устранять экологические проблемы предприятия. Регулярный анализ обеспечит оперативный мониторинг ключевых аспектов экологической безопасности. Это позволит оперативно управлять экологической политикой предприятия в целях предотвращения нанесения ущерба окружающей среде.

## **Тема 11. Организация службы безопасности предприятия**

Сохранение материальных ценностей и информации, в том числе коммерческой тайны, является важной задачей для хозяйствующих субъектов. Кража интеллектуальной собственности стала массовым явлением, происходят целенаправленные действия по завладению секретами конкурентов, включая подкуп и сманивание их сотрудников. Непреднамеренные организационные каналы утечки и несанкционированного доступа к информации, разглашение информации персоналом, разглашение информации при проведении совещаний или приеме посетителей, рекламной и выставочной деятельности усугубляют проблему. Защиту от этих действий можно обеспечить путем создания и организации структур служб безопасности на предприятии.

Служба безопасности предприятия представляет собой комплекс мер, осуществляемых на организационно-правовой основе с целью защиты предпринимательской и производственной деятельности от реальных или потенциальных действий физических или юридических лиц, которые могут привести к значительным экономическим потерям в результате нарушения информационной безопасности фирмы. Меры безопасности включают в себя использование сил и средств, направленных на предотвращение возможных угроз и рисков для предприятия.

Самостоятельная организационная единица, подчиняющаяся непосредственно руководителю предприятия, должна представляться как служба безопасности (СБ). Такая структура управления системой безопасности, имеющая четкую вертикаль, характерная для области обеспечения безопасности, где требуется определенность, четкие границы и регламентация отношений на всех уровнях - от рядового сотрудника до менеджеров высшего звена. Из практики следует, что только предприятия, где проблемы безопасности находятся под постоянным контролем руководителя, могут достичь наиболее высоких результатов в обеспечении безопасности.

Начальник службы безопасности (СБ) должен занимать должность заместителя руководителя предприятия по безопасности. При этом руководитель СБ

должен иметь максимально возможный круг полномочий, чтобы воздействовать на другие подразделения и различные области деятельности предприятия, если это необходимо для обеспечения безопасности.

Не существует единой методики формирования структуры службы безопасности, однако можно представить алгоритм ее построения. Это:

Первый шаг – выбор точки отсчета,

Второй шаг – выявление угроз безопасности,

Третий шаг – анализ рисков,

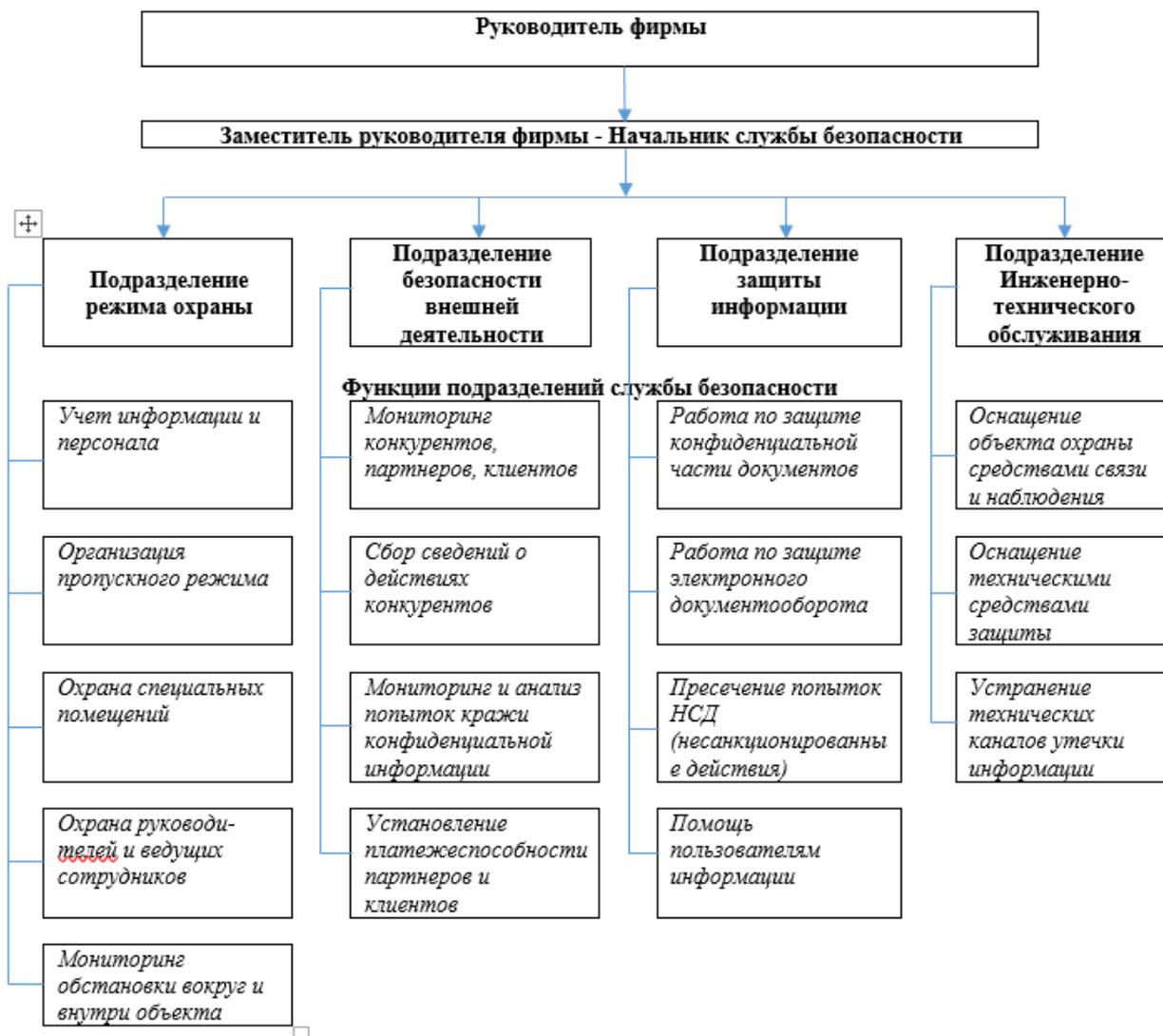
Четвертый шаг – планирование мер по локализации угроз,

Пятый шаг – создание службы безопасности,

Шестой шаг - поддержание функционирования системы безопасности.

Структура и численность службы безопасности зависят от различных факторов, таких как форма собственности предприятия, вид его производственной деятельности, место на рынке товаров и услуг, численность сотрудников, наличие крупных материальных ценностей, взрыво- и пожароопасность производства, информации, составляющей коммерческую тайну, а также активности конкурентов и криминальных структур. Из-за этого невозможно представить универсальную структуру службы безопасности, однако можно выделить основные структурные подразделения, которые должны присутствовать в большинстве случаев при создании службы безопасности (СБ) на крупных промышленных государственных, акционерных предприятиях, в промышленно-финансовых группах, холдингах и т.д.

## Предполагаемая структура службы безопасности



Структура службы безопасности, представленная выше, не может быть универсальной и должна быть адаптирована под конкретную организацию. Новые отделы, такие как отдел пожарной безопасности, группа управления персоналом или группа сопровождения грузов, могут быть введены в нее по мере необходимости. В большинстве случаев формирование или реформирование структуры СБ осуществляется после проведения аналитических исследований степени защищенности объекта и понимания задач, которые должны ею решаться на текущий момент. Однако необходимо помнить, что создание службы безопасности является только первым шагом в создании защиты любого объекта, и от того, насколько тщательно проводится этот процесс, зависит эффективность последующих мер по обеспечению безопасности.

Важный пункт - это организация защиты коммерческой тайны. Коммерческая тайна в общем понимании означает конфиденциальные данные, которые имеют особую тактическую или потенциальную важность.

Информация, которая является коммерческой тайной, включает в себя сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют реальную или потенциальную коммерческую ценность из-за их неизвестности третьим лицам, к которым у третьих лиц нет законного доступа, и в отношении которых обладателем таких сведений установлен режим коммерческой тайны.

Коммерческая тайна - это конфиденциальные данные, не являющиеся государственной тайной, которые представляют определенную ценность для субъекта предпринимательства и разглашение которых может причинить ущерб фирме.

К мерам установления режима тайны коммерческого характера, относятся:

1. Определение перечня информации, которая составляет коммерческую тайну;
2. Ограничение доступа к такой информации путем установления индивидуального порядка ее использования и контроля за соблюдением этого режима;
3. Ведение журнала лиц, которым был предоставлен доступ к конфиденциальной информации;
4. Определение важности коммерческой информации для организации;
5. Обязательное подписание соглашения о неразглашении коммерческой информации при приеме сотрудника в организацию;
6. Все носители информации должны быть помечены грифом "Коммерческая тайна" и указанием владельца такой информации.

Раскрытие информации, которая составляет коммерческую тайну, может привести к финансовым потерям и даже банкротству фирмы. Сегодня, когда угрозой являются не только действия конкурентов, но и хакерские атаки и вирусные заражения, защита коммерческой тайны является ключевым условием для успешного ведения бизнеса. Целью защиты коммерческой тайны является предотвращение несанкционированного доступа к конфиденциальной информации и минимизация рисков утечки такой информации, которая может нанести ущерб бизнесу.

Комплекс мер по защите коммерческой информации выполняет несколько задач одновременно:

1. Помощь в укреплении позиции в конкурентной борьбе, сохранении сегмента рынка и клиентов.
2. Защита стратегически важной информации на протяжении определенного времени.
3. Проверка возможных каналов утечки информации.
4. Предотвращение рисков, связанных с ротацией кадров.

Для того чтобы система защиты конфиденциальной коммерческой информации работала эффективно, необходимо соблюдать несколько условий. Прежде всего, внутри компании необходимо достичь согласия по финансовым, производственным, операционным и коммерческим аспектам деятельности. Обеспечение информационной безопасности также требует взаимодействия между всеми структурными подразделениями компании. Основой успешной защиты является объективная оценка информации и объектов, которые нуждаются в защите, а также разработка и согласование мер по их защите еще до введения этих мер. Личная материальная ответственность руководителей структурных подразделений и сотрудников, которые работают с конфиденциальной информацией, может усилить защиту. Документальная закреплённость санкций за нарушение условий конфиденциальности и сохранности информации, которая является коммерческой тайной.

Перед внедрением средств защиты конфиденциальных данных важно

определить объект и предмет защиты. Как правило объектом защиты является информация, связанная с деятельностью компании и представляющая финансовый и стратегический интерес для конкурентов, то есть коммерческая тайна. Предметом защиты являются носители информации, на которых содержатся данные, являющиеся частью коммерческой тайны, включая бумажные и электронные документы, внешние накопители информации, а также другие устройства для хранения и передачи данных.

Для качественной защиты коммерческой тайны необходимы меры, разных направлений. Если не использовать комплексный подход, возможно нарушение конфиденциальности стратегически важной информации путем кражи, хищения, утечки, фальсификации, несанкционированного распространения сведений, которые являются конкурентной информацией для других компаний.

Конфиденциальность финансовой информации и защита коммерческой тайны фирмы достигается на основе использования на практике:

- Защиты правового характера;
- Организационных инструментов;
- Социально-психологических методов.

Принятие внутренних нормативных документов и соблюдение законодательства, касающегося защиты информации, которая является коммерческой ценностью, являются мерами юридического характера.

Законодательные основы защиты коммерческой тайны закрепляются в уставах, приказах, правилах внутреннего трудового распорядка, контрактах и трудовых договорах. Обязанность сотрудника соблюдать правила сохранности информации, полученной во время работы, может быть отдельно оговорена в коллективном договоре или трудовом соглашении.

Фактически, правовая защита информации осуществляется посредством, выбранных фирмой, методов, которые зависят от деятельности фирмы.

Административно-организационные меры защиты коммерческой тайны предполагают использования двух основных составляющих:

1. Присутствие специального структурного подразделения, которое занимается обеспечением информационной безопасности, и
2. Наличие пунктов пропуска и постов охраны на объектах предприятия, требующих повышенной защиты.

Служба охраны отвечает за контроль посещений и оформление пропусков, а также за фиксацию времени пребывания на территории организации. С другой стороны, задачи службы информационной безопасности включают установление порядка рассекречивания и уничтожения информации, которая находилась под защитой, контроль публикуемой информации, обеспечение техническими средствами безопасности офисных помещений и оборудования для работы с информацией, формирование системы защиты электронных носителей информации и использование технических средств для контроля пользовательских рабочих станций, а также принятие превентивных мер против несанкционированного доступа к закрытой информации.

Кадровая служба играет важную роль в обеспечении безопасности коммерческой тайны. Вместе с ИБ-специалистами (информационная безопасность), специалисты по работе с персоналом проводят инструктаж по соблюдению мер безопасности при работе с информацией, которая является коммерческой тайной.

Для обеспечения безопасности коммерческой тайны используются не только правовые и организационные меры, но и социально-психологические меры. Работа с персоналом проводится по двум направлениям:

- Тщательный подбор кандидатов при приеме на работу, основанный на профессиональных и моральных качествах, и оценка соискателей.
- Материальное стимулирование сотрудников, систематически соблюдающих правила работы с конфиденциальной информацией.

До 80% успешной защиты коммерческой тайны обеспечивают грамотный подбор кадров, а также своевременная и справедливая мотивация персонала.

В настоящее время не все руководители предприятий осознают необхо-

димось создания надежной системы экономической безопасности. У большинства руководителей все еще существуют стереотипы, связанные с тем, что безопасность фирмы должно обеспечить государство. Хозяин фирмы должен сам защищать свои интересы и обеспечить безопасность бизнеса. Одним из способов обеспечения безопасности предприятия является создание собственной службы безопасности на базе компании.

Перед тем как создать службу безопасности следует изучить цели, структуру и функции. Важно также определить, какие объекты требуют защиты на предприятии. Объектами, требующими защиты на предприятии, являются:

- Объекты и
- Особые объекты.

Объекты это:

1. территория предприятия;
2. объекты, расположенные на территории (здания, сооружения);
3. носители конфиденциальной информации (документы, изделия);
4. материальные ценности (грузы).

Особые объекты включают:

1. руководство предприятия;
2. персонал, который имеет доступ к конфиденциальной информации.

Охранные мероприятия для защиты руководства и персонала на предприятии регулируются специальным положением (инструкцией), которое утверждает руководитель предприятия. В случае необходимости, это положение согласовывается с территориальными органами внутренних дел и органами безопасности.

Основные цели охраны руководства и персонала на предприятии заключаются в обеспечении их личной безопасности в повседневных условиях и в случае возникновения чрезвычайных ситуаций. Также необходимо предотвра-

щать возможные попытки злоумышленников завладеть защищаемой информацией, используя физическое или другое насильственное воздействие на этих людей, и разрабатывать рекомендации для охраняемых лиц по правильному поведению в различных ситуациях.

В зависимости от размеров и мощности предприятия, задачи по обеспечению безопасности и защите информации могут быть решены с помощью услуг специализированных центров безопасности, которые предоставляют абонентское обслуживание, или с помощью полноценной службы безопасности, созданной самой компанией с развитой штатной численностью.

Важнейшими целями службы безопасности являются:

- предотвращение попыток несанкционированного проникновения злоумышленников на территорию предприятия;
- оперативное обнаружение и задержание лиц, пытающихся проникнуть на охраняемую территорию;
- обеспечение сохранности находящихся на охраняемой территории носителей конфиденциальной информации и материальных ценностей;
- предупреждение происшествий на охраняемом объекте и устранение их последствий.

Среди задач охраны объектов предприятия можно выделить следующие:

- осуществление контроля за объектом и охраняемой территорией, в том числе территории с особым режимом пропуска, с целью обнаружения и предотвращения попыток несанкционированного проникновения на них посторонних лиц;
- обеспечение конфиденциальности и сохранения в тайне фактов проведения закрытых мероприятий на предприятии (его объектах), а также обсуждаемых или рассматриваемых вопросов;
- сопровождение и охрана носителей конфиденциальной информации, в том числе служебных документов предприятия, материальных ценностей и грузов при их транспортировке и перевозке (доставке);

- защита объектов и территорий с особым режимом пропуска от насильственных действий и вооруженных нападений, которые могут нанести ущерб предприятию;
- выполнение специальных задач по обеспечению личной охраны руководства предприятия и персонала, который имеет доступ к конфиденциальной информации;
- участие в обеспечении пропускного режима для посетителей, транспортных средств и грузов на охраняемой территории (объектах предприятия) с целью установления личности и учета посетителей, контроля за ввозом, вывозом носителей конфиденциальной информации, грузов, материальных ценностей, предотвращения их несанкционированного перемещения, а также обнаружения попыток хищения иного имущества предприятия;
- систематический анализ эффективности системы охраны, принимаемых должностными лицами мер по охране объектов предприятия и обеспечению сохранности носителей конфиденциальной информации, материальных ценностей и грузов, и выработка предложений по совершенствованию системы охраны.

Для достижения основных целей и задач по охране предприятия (его объектов) создается система охраны, которая включает в себя:

1. персонал подразделений охраны (караулов);
2. технические средства охраны;
3. места, где находится персонал, выполняющий задачи охраны, и где используются технические средства;
4. методы охраны объектов.

Локация персонала охраны может включать в себя один из элементов системы контроля доступа - контрольно-пропускные пункты.

Средства технической охраны, используемые при охране предприятий, можно разделить на две группы:

- средства обнаружения (такие как пожарная и охранная сигнализация, "тревожное" оповещение, охранное телевидение, охранное освещение, аппаратура

проверки почтовой корреспонденции, радиосвязь, прямая внутренняя связь, прямая телефонная связь с милицией и другие);

- средства обнаружения и устранения (например, средства пожаротушения, индивидуальные средства защиты, газовые ловушки, автотранспорт, оружие, инженерно-технические средства и другие).

Если компания создает свои собственные штатные подразделения охраны, то они могут быть объединены в службу охраны. Служба охраны включает в себя посты охраны, группы сотрудников охраны (включая подразделение личной охраны руководства и персонала), группу охраны и сопровождения материальных ценностей и грузов, группу быстрого реагирования («тревожную» группу) и, при необходимости, подразделения сторожевых собак. Служба охраны как правило становится самостоятельной организационной единицей, подчиняющейся руководителю предприятия. Начальником службы безопасности является заместитель руководителя предприятия по безопасности.

Для оптимальной организации службы безопасности необходимо включить следующие структурные единицы:

1. Отдел режима и охраны, который состоит из сектора режима и сектора охраны.
2. Отдел защиты информации.
3. Инженерно-техническая группа.
4. Группа по обеспечению безопасности внешней деятельности.

Структура службы безопасности, представленная выше, не является универсальной и должна быть адаптирована под конкретную организацию. В ней могут быть введены новые отделы, такие как отдел пожарной безопасности, группа управления персоналом или группа сопровождения грузов. Как правило, формирование или реформирование структуры собственной безопасности осуществляется по мере осознания задач, которые должны быть решены на текущий момент.

Основные функции службы безопасности включают в себя:

1. Выявление случаев недобросовестной конкуренции со стороны других предприятий.
2. Получение информации об уголовных делах.
3. Исследование случаев раскрытия конфиденциальной информации о деятельности предприятия.
4. Получение информации о людях, заключивших сделки с предприятием.
5. Организация поиска пропавшего имущества предприятия и расследование случаев незаконного использования товарных (фирменных) знаков данного предприятия.
6. Исследование случаев незаконного использования товарных (фирменных) знаков, принадлежащих предприятию.
7. Поиск пропавших без вести сотрудников.
8. Определение неплатежеспособных партнеров.
9. Определение ненадежных деловых партнеров.
10. Сбор информации по гражданским делам.
11. Сбор информации для подготовки к деловым переговорам.
12. Обеспечение безопасности жизни и здоровья персонала от незаконных действий.
13. Защита собственности предприятия.
14. Обеспечение безопасности и порядка на мероприятиях, проводимых предприятием, включая представительские, конфиденциальные и массовые.
15. Предоставление советов и рекомендаций руководству и персоналу предприятия по вопросам обеспечения безопасности,

## **Тема 12. Система организации экономической безопасности государств**

Обеспечение экономической безопасности является необходимым условием для достижения стабильного социально-экономического развития и процветания нации любого государства. Мировой опыт свидетельствует, что не существует единого подхода к определению экономической безопасности государств. Эксперты считают, что это понятие находится где-то между экономической наукой и теорией международных отношений. Кроме того, данное понятие является относительно новым как для западных, так и для постсоветских стран, что также может служить причиной отсутствия единого определения. Поэтому важнейшей задачей является анализ мирового опыта в исследовании проблемы обеспечения экономической безопасности государства и практики ее реализации в международном сообществе. Целью является разработка предложений по усовершенствованию механизмов обеспечения экономической безопасности.

До появления термина «экономическая безопасность» в мировой практике использовалось понятие «национальная экономическая безопасность», которое стало широко распространенным в западной литературе в середине 1980-х годов. Исследования показывают, что термин «национальная экономическая безопасность» был впервые использован в США в период экономического кризиса в 1970 году, когда страна выразила стремление стать мировым экономическим лидером.

В рамках обеспечения экономической безопасности, США выделяют такие приоритетные направления политики, как: повышение конкурентоспособности местных товаров, развитие сотрудничества в торгово-экономических отношениях и сокращение объема иностранных займов. Первой программой в США, направленной на обеспечение экономической безопасности, можно

считать Меморандум 1990 года. Этот документ был создан для защиты лидирующих позиций США в технологических отраслях и поддержания экономического развития страны на мировой арене.

Для разработки скоординированной политики экономической безопасности, США создали Межведомственную рабочую группу, которая разработала основной механизм управления системой экономической безопасности. В результате ее работы были приняты новые нормативно-правовые акты, а также проведена переподготовка кадров. Рабочая группа определила основные угрозы экономической безопасности страны и разработала «Каталог угроз экономической безопасности и их оценку».

Исследование японской модели национальной безопасности показывает, что она связана с американской моделью из-за послевоенной оккупации, которая привела к формированию союзных отношений между Японией и США.

Основными документами Японии, касающимися обеспечения национальной безопасности, являются доктрина Ёсида (Ёсида - Премьер-министр в 1946-1954 гг. и лидер Либеральной партии Японии) и доктрина Комплексного обеспечения национальной безопасности, которые были приняты в середине XX века и основаны на политике обеспечения национальной безопасности после Второй мировой войны. Эти доктрины направлены на динамичное развитие экономики. В связи с ограниченными природными ресурсами Японии было решено установить научно-техническое и торговое сотрудничество с другими странами.

Доктрина послужила основой для политики национальной безопасности Японии в то время, когда страна благодаря ее реализации уже в 1968 году вошла в двадцатку лучших стран мира по объему промышленного производства.

Ситуация в Европейском союзе (ЕС) несколько отличается, в том числе, потому что понятие экономической безопасности в ЕС имеет два определения.

Первое определение исходит из того, что ЕС видит себя в мировой экономической системе как объединение стран Европы для обеспечения конкурентоспособности на международном рынке. Решение о создании ЕС было принято, поскольку у отдельных стран Европы были проблемы с природными и трудовыми ресурсами в сравнении с другими развитыми странами мира и США.

Второе определение декларирует обеспечение экономического равенства и солидарности между европейскими странами. ЕС и Европейский банк развития выделяют всем странам Европы значительные бюджетные средства на развитие экономики, инфраструктуры, ликвидацию последствий стихийных бедствий. Основной целью ЕС является интеграция европейских стран с одинаковым экономическим потенциалом и одинаковым уровнем жизни.

Для обзора экономической безопасности ЕС рассмотрим программы, доктрины и концепции экономической безопасности отдельных стран членов ЕС.

Во Франции обеспечение экономической безопасности началось в 1964 году после принятия Закона о национальной безопасности. До употребления категории экономической безопасности во Франции употреблялся термин «национальная экономическая безопасность», так как упор делался на развитие экономики страны путем улучшения уровня жизни населения. В Законе о национальной безопасности в качестве основных критерий использовались следующие послылы:

- минимизация внешних рисков;
- ликвидация барьеров для субъектов предпринимательства;
- ликвидация зависимости приоритетных отраслей экономики от внешних факторов.

В отличие от Франции, в Германии не существует специального документа, который регламентировал бы экономическую безопасность страны. То есть в стране отсутствуют законы, концепции или доктрины непосредственно

посвященные экономической безопасности страны. Проблемами экономической безопасности занимается министерства обороны страны, на которых обращен часть законодательных актов министерства. В них описаны приоритетные направления, обеспечивающие, развитие конкуренции, ограничение монополий, стабильность национального валютного курса и другие.

В Великобритании экономическая безопасность является частью национальной системы и воспринимается как защита общих интересов населения страны. В стране отсутствуют НПА (нормативно-правовые акты) по экономической безопасности. Основными характеристиками экономической безопасности являются поддержка предпринимательства, организация связи между правительством и бизнесом, а также прогнозирование угроз и защита экономической безопасности государства.

Важнейшей основой Концепции экономической безопасности Испании, принятой в стране в отличие от других стран ЕС, является:

- сильная нормативно-правовая база;
- оперативная структура ответственных государственных органов;
- организация и эффективное функционирование контрольных органов государства.

Концепции экономической безопасности позволяет правильно распределять права между государственными органами, ответственными за развитие экономической сферы, а также механизмы контроля за исполнением решений правительства. Основными мерами обеспечения экономической безопасности являются мониторинг инвестиционной и валютной политики, развитие промышленного производства и создание нормативно-правовой базы для бизнеса. Государственное управление Италии не имеет регулирующего документа, но при этом позволяет защищать отечественных производителей на международном рынке. Правительство отдает предпочтение международному сотрудничеству и внешнеторговой деятельности, внедрению кооперативов в промышленном производстве и защите интересов отечественных бизнесменов.

Проведенный анализ показал, что ведущие страны Экономического Союза, такие как Франция, Германия, Великобритания, Испания и Италия, не смотря на отличающую друг от друга экономическую политику, сумели сформировать эффективную экономическую систему, способную поддерживать, улучшать и обеспечивать экономическую безопасность государства и ее граждан.

В период между XX и XXI веками, в условиях трансформации политических и экономических систем, экономика стран была подвержена не только внутренним преобразованиям, но и влиянию других государств и мировой экономики в целом. В этой ситуации национальная, и особенно экономическая, безопасность стран стала приобретать особую значимость.

Стратегия обеспечения экономической безопасности России основывается на официально принятых нормативных актах, включая Конституцию Российской Федерации, Закон РФ «О безопасности» от 5 марта 1992 г. № 2446-1, Государственную стратегию экономической безопасности РФ и Стратегию национальной безопасности России до 2020 года. В указанных документах экономическая безопасность рассматривается как неотъемлемый элемент национальной безопасности, которая в свою очередь является системой, включающей внешние и внутренние факторы, важные интересы личности, общества и государства, а также реальные и потенциальные угрозы их безопасности, институты и субъекты, обеспечивающих безопасность.

На долгосрочную перспективу главными стратегическими рисками и угрозами национальной безопасности России в экономической сфере являются сохранение экспортно-сырьевой модели развития национальной экономики, снижение конкурентоспособности и высокая зависимость от внешнеэкономической конъюнктуры важнейших сфер, потеря контроля над национальными ресурсами, ухудшение состояния сырьевой базы промышленности и энергетики, неравномерное развитие регионов, низкая устойчивость и защищенность национальной финансовой системы, сохранение условий для коррупции и

криминализации хозяйственно-финансовых отношений, а также незаконной миграции.

В целях достижения национальной безопасности через экономический рост Российская Федерация сосредоточивает свои усилия на развитии науки, технологий и образования, а также повышения уровня безопасности в оборонной, военной и международной сферах. Усиливается функциональность национальных инвестиционных и финансовых институтов.

В перспективе Россия считает важным развивать конкурентоспособные отрасли экономики, расширять рынки сбыта продукции, повышать эффективность топливно-энергетического комплекса и использовать преимущества государственно-частного партнерства. Также необходимо завершить формирование транспортной, энергетической, информационной и военной инфраструктуры в Арктической зоне, Восточной Сибири и на Дальнем Востоке.

Как и многие другие страны на постсоветском пространстве, Республика Узбекистан унаследовала энергозатратную экономику и материалоемкое производство с физически и морально устаревшим оборудованием и технологией, загрязняющей окружающую среду. В условиях перехода от административно-командной экономики к рыночной, важным явилась внедрение макроэкономического планирования с учетом охраны окружающей среды и на этой основе обеспечения экономической безопасности страны и населения. В этой связи правительством были приняты ряд нормативно-правовых документов. Исходя из существующих условий, в новом независимом государстве - Узбекистане был разработан курс преобразований всех сфер жизни. Главной особенностью этого курса стала разработка собственной стратегии перехода к рыночной экономике, отказ от применения "шоковой терапии" в экономике и взятие уверенного курса на кардинальные и планомерные преобразования.

Модель перехода Узбекистана к рынку не была простым копированием чужого опыта, а основывалась на менталитете народа, многовековых традициях и уникальных условиях, которые существовали на момент начала реформ. При этом использовался положительный зарубежный опыт в различных

областях, но адаптированный именно к существующим условиям в Узбекистане на каждом этапе преобразований. В начальный период реформирования в основе стратегии лежали пять принципов, сформулированных Президентом Узбекистана И. А. Каримовым.

Первый принцип заключается в приоритете экономики перед политикой, а также в деидеологизации внутренних и внешних экономических отношений.

Второй принцип заключается в том, что государство выступает в роли главного реформатора и последовательного инициатора преобразований, проводимых в республике на переходном этапе.

Третий принцип заключается в обеспечении законности и верховенства права во всех сферах общественной жизни.

Четвертый принцип заключается в том, что сильная социальная политика обеспечивает социальную защиту и поддержку уязвимых слоев населения в переходный период.

Пятый принцип заключается в том, что постепенный эволюционный переход к рыночным отношениям и отказ от шоковой терапии осуществляются последовательно и поэтапно.

Эти и другие мероприятия явились основой национальной политики экономической безопасности, проведенной первой администрацией Республики Узбекистан.

В настоящее время в Республике Узбекистан не существует специального отдельного документа, посвященного стратегии экономической безопасности. Однако это не означает, что в стране не уделяют должного внимания внутренним и внешним угрозам и обеспечению экономической безопасности государства, общества и граждан. В "Стратегии развития нового Узбекистана на 2022-2026 годы", утвержденной Указом Президента Республики Узбекистан от 28 января 2021 года № УП-60 весь документ посвящен защите различных аспектов экономической безопасности Республики Узбекистан.

Среди 100 целей, которые содержатся в стратегии, каждая решает задачу обеспечения экономической безопасности страны.

Глава VII посвящена укреплению безопасности и оборонного потенциала страны, а также ведению открытой, прагматичной и активной внешней политики. В ней декларируется:

- дальнейшее усиление оборонной способности государства,
- усиление готовности к бою, боеспособности и потенциала Вооруженных Сил,
- создание эффективной системы предотвращения и реагирования на чрезвычайные ситуации,
- развитие тесного сотрудничества в области безопасности, торгово-экономических, водных, энергетических, транспортных и культурно-гуманитарных взаимоотношений в Центральной Азии на высокий уровень;
- укрепление присутствия Узбекистана в органах и институтах Организации Объединенных Наций, а также в глобальных и региональных экономических, финансовых и гуманитарных организациях.
- дальнейшее развитие отношений Узбекистана с традиционными партнерами, уделяя приоритетное значение расширению географии нашего внешнего взаимодействия и усилению экономической дипломатии.
- присоединение к Всемирной торговой организации и углублению процессов интеграции с Евразийским экономическим союзом.
- увеличение эффективности распространения информации, направленной на улучшение репутации нашей страны, среди аудитории мирового сообщества.
- улучшение нормативно-правовой базы внешней политики и внешнеэкономической деятельности, а также договорных основ международного сотрудничества.
- улучшение системы предоставления гражданам Узбекистана услуг за рубежом через дипломатические представительства и консульские учреждения Республики Узбекистан в других странах.

В то время как глава VII направлена на развитие политической безопасности, в других разделах стратегии можно увидеть цели, связанные с развитием экономической безопасности в разных отраслях экономики. Например:

Цель 80 предусматривает защиту экологии и окружающей среды, улучшение экологической обстановки в городах и районах, а также реализацию национального проекта «Зеленый край».

Цель 24 заключается в обеспечении бесперебойного энергоснабжения экономики, активном внедрении "зеленых" технологий во все сферы и увеличении энергоэффективности экономики на 20 процентов.

Цель 22 заключается в продолжении реализации промышленной политики, направленной на обеспечение стабильности национальной экономики, повышение доли промышленности в валовом внутреннем продукте и увеличение объема производства промышленной продукции в 1,4 раза.

Цель 21 заключается в увеличении объема валового внутреннего продукта на душу населения в 1,6 раза в ближайшие пять лет путем обеспечения стабильно высоких темпов роста в различных отраслях экономики. К 2030 году размер ВВП на душу населения должен достигнуть 4 тысяч долларов США и создать предпосылки для вхождения Узбекистана в категорию «государств с доходом выше среднего».

Цель 13 заключается в обеспечении надежной защиты имущественных прав и ограничении незаконного вмешательства государственных органов в имущественные отношения.

Цель 14 заключается в обеспечении верховенства закона и конституционной законности, а также в установлении чести и достоинства человека как основного критерия этого процесса.

Несмотря на то, что весь документ "Стратегия развития нового Узбекистана на 2022-2026 годы" посвящен экономической безопасности, очевидно, что отдельные вопросы, связанные с внешними и особенно внутренними угрозами экономики, не нашли отражения. В этой связи представляется необходи-

мым создания специального документа – «Стратегия экономической безопасности Республики Узбекистан», в котором можно было бы найти ответы на все выше обозначенные вопросы обеспечения экономической безопасности Республики Узбекистан.

## Глоссарий

**Администратор безопасности** – полномочный представитель (лицо или группа лиц), ответственный за обеспечение безопасности в автоматизированных системах и сетях.

**Административная ответственность** – вид юридической ответственности за проступки и правонарушения, не являющиеся уголовно наказуемыми.

**Административное право (АП)** – отрасль права, регулирующая общественные отношения в сфере государственного управления. Нормы АП определяют порядок организации и деятельности управленческого аппарата, права и обязанности должностных лиц и граждан. Юридическими источниками АП являются конституция, а также содержащие административно-правовые нормы законы, указы, положения, уставы, постановления, распоряжения, приказы и инструкции различных органов управления.

**Адресование документа** – разрешение на доступ к конкретному документу в виде резолюции на самом документе или специальном клапане, с указанием конкретных лиц, которым дается разрешение на ознакомление (исполнение) документа.

**Анализ риска** – процесс определения угроз безопасности системы и отдельным ее компонентам, определения их характеристик и потенциального ущерба, а также разработка мер защиты.

**Аппаратные средства защиты** – механические, электромеханические, электронные, оптические, лазерные, радио-, радиотехнические, радиолокационные и другие устройства, системы и сооружения, предназначенные для защиты информации от НСД, копирования, кражи или модификации.

**Аутентификация информации** – установление подлинности информации исключительно на основе внутренней.

**«Враждебное поглощение»** – это получение контроля над финансово-хозяйственной деятельностью или активами компании-цели в условиях сопротивления со стороны руководства или ключевых участников компании-цели.

**Государственное право** – отрасль права, представляющая собой совокупность юридических норм, закрепляющих общественное и государственное устройство, систему, принципы организации и деятельности государственных органов, основные права и обязанности граждан.

**Государственная тайна** – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности государства.

**Гриф конфиденциальности** – специальная отметка на носителе информации либо в сопроводительных документах на него, свидетельствующая о том, что носитель содержит конфиденциальную информацию.

**Гриф секретности** – реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставленные на самом носителе и/или в сопроводительной документации на него. Установлено три степени секретности сведений, составляющих гостайну, и соответствующие грифы секретности: «особой важности», «совершенно секретно» и «секретно».

**Доступ к конфиденциальной информации** – санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную или коммерческую тайну.

**Закрытые данные** – данные, доступные ограниченному кругу пользователей. Как правило, ограничение доступа осуществляется системой разграничения с помощью определенных правил (паролей).

**Идентификация** – отождествление предметов или лиц по их характеристикам, или по документам, или путем опознавания по приметам и определение полномочий, связанных с доступом к конфиденциальной информации.

**Информационная безопасность** – это состояние защищенности информационных ресурсов и потоков информации компании.

**Информация секретная** – информация, сведения, составляющие государственную тайну.

**Коммерческая тайна** – не являющиеся государственными секретами сведения, связанные с производством, технологической информацией, управлением, финансами и другой деятельностью предприятия, разглашение или утечка которых может нанести ущерб его интересам. Не могут составлять коммерческую тайну учредительные документы и устав; документы, дающие право заниматься предпринимательской деятельностью; сведения по установленным формам отчетности о финансово-хозяйственной деятельности; документы о платежеспособности; сведения о численности, составе работающих, их заработной плате и условиях труда, а также о наличии свободных мест; документы об уплате налогов и обязательных платежей; сведения о загрязнении окружающей среды; сведения об участии должностных лиц предприятий в кооперативах, малых предприятиях, товариществах и т. д.

**Компьютерный шпионаж** – подключение к компьютерам (или их прослушивание) без согласия владельцев с целью съема или повреждения содержащихся в них секретных данных.

**Контрразведка** – деятельность специальных органов государства (компаний) в целях борьбы против разведок других государств (компаний).

**Криптография** – тайнопись, система изменения информации (текста, речи) с целью сделать ее непонятной для непосвященных лиц.

**Многоуровневая защита** – защита, обеспечивающая разграничение доступа субъектов с различными правами доступа к объектам различных уровней конфиденциальности.

**Мошенничество** – это преступление, в результате которого его жертва добровольно передает часть своих материальных средств в какой-либо форме мошеннику.

**Объект промышленного шпионажа** – любые материальные и нематериальные объекты, содержащие коммерческую тайну предприятия и представляющие какой-либо интерес для заказчика: документы, чертежи, образцы продукции, неоформленные патенты, технические проекты, информация о ценах, контрактах, поставщиках и т. д.

**Оператор персональных данных** – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных (т. е. каждый работодатель в отношении своих работников является оператором т. к. ведет личные дела).

**Персональные данные** – любая информация, относящаяся к определенному на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

**Полиграф (детектор лжи)** – прибор, который непрерывно измеряет значения кровяного давления, частоты пульса, влажности кожи, частоту дыхания и другие физиологические переменные.

**Полномочия** – право пользователя или уполномоченного им субъекта осуществлять определенные процедуры над охраняемыми сведениями.

**Правовая защита информации** – специальные правовые акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе.

**Правонарушение** – противоправное, виновное (умышленное или неосторожное) действие или бездействие, за которое законодательством предусмотрена административная ответственность.

**Разграничение доступа** – система мероприятий, обеспечивающих предоставление пользователям только той информации, которая необходима им для выполнения работы.

**Санкционированный доступ к информации** – доступ к информации, не нарушающий правил разграничения доступа.

**Служба безопасности (СБ)** – система штатных органов управления и организационных формирований, предназначенных для обеспечения безопасности деятельности компании.

**Управление безопасностью** – система регулярных защитных мероприятий,

направленных на обеспечение безопасности в соответствии с изменяющимися условиями внутренней и внешней среды.

**Шпионаж** – передача, похищение, добывание или собирание с целью корыстного использования или передачи иностранному государству или его агентуре сведений, составляющих конфиденциальную тайну (государственную, военную, экономическую, промышленную, коммерческую и т. п.).

**Экономическая безопасность** – состояние наиболее эффективного использования всех видов ресурсов в целях предотвращения (нейтрализации, ликвидации) угроз и обеспечения стабильного функционирования компании в условиях рыночной экономики.

**Экономическая разведка (в бизнесе)** – информационно-аналитическая работа (добывание, обработка, получение выводной информации) по экономическим проблемам.

## Вопросы для самопроверки по темам

### По теме 1.

1. Сущность и содержание категорий: безопасность, экономическая безопасность
2. Внутренние и внешние угрозы безопасности
3. Угрозы экономической безопасности предприятия.
4. Внешние и внутренние, субъективные и объективные опасности и угрозы предприятий
5. Функциональные составляющие экономической безопасности предприятия.

### По теме 2.

1. Основные направления и способы обеспечения экономической безопасности предприятия.
2. Этапы организации обеспечения экономической безопасности предприятия.
3. Основные пороговые значения экономической безопасности предприятия (организации).
4. Понятие и типы стратегий экономической безопасности предприятия.

### По теме 3.

1. Сущность технико-технологической составляющей экономической безопасности предприятия
2. Основные индикаторы состояния технико-технологической составляющей экономической безопасности предприятия
3. Частный функциональный критерий технико-технологической составляющей.
4. Способы обеспечения технико-технологической безопасности предприятия.

#### **По теме 4.**

1. Концепция информации и информационной безопасности
2. Направления обеспечения информационной безопасности бизнеса
3. Цели защиты информации
4. Угрозы и риски информационной безопасности
5. Организационные аспекты информационной безопасности.

#### **По теме 5.**

1. Сущность финансовой безопасности государства
2. Сущность финансовой безопасности предприятия
3. Обеспечения финансовой безопасности и финансовой устойчивости
4. Внутренние и внешние угрозы финансовой безопасности.

#### **По теме 6.**

1. Приведите показатели финансовой безопасности:
  - Показатели платежеспособности
  - Показатели финансовой устойчивости
  - Показатели деловой активности
  - Показатели рентабельности
2. Приведите показатели ликвидности активов:
  - Коэффициент быстрой (промежуточной) ликвидности
  - Коэффициент текущей ликвидности
  - Коэффициент абсолютной ликвидности.

### **По теме 7.**

1. Сущность интеллектуального потенциала современного предприятия
2. Кадровая составляющая экономической безопасности предприятия.
3. Внешние и внутренние угрозы интеллектуальной и кадровой безопасности предприятия
4. Обеспечение эффективного функционирования механизма кадровой безопасности и ее укрепление.

### **По теме 8.**

1. Сущность экономических индикаторов, их роль и значение
2. Индикаторы состояния интеллектуальной и кадровой составляющей экономической безопасности предприятия
3. Мероприятия по повышению кадровой безопасности предприятия
4. Преодоление пороговых значений
5. Объекты интеллектуальной собственности
6. Сущность индикаторного метода оценки кадровой безопасности предприятия
7. Пороговые значения индикаторов
8. Методы определения пороговых значений кадровой безопасности предприятия
9. Факторы, оказывающие влияние на формирование пороговых значений кадровой безопасности
10. Алгоритм определения пороговых значениях индикаторов кадровой безопасности

11. Базовые индикаторы кадровой безопасности и рекомендуемые пороговые значения.

**По теме 9.**

1. Сущность экологической составляющей экономической безопасности предприятия
2. Способы обеспечения экологической составляющей экономической безопасности предприятия
3. Основные индикаторы экологической безопасности предприятия
4. Экологическая экспертиза и ее принципы
5. Экологический менеджмент предприятия
6. Экологический аудит (экоаудит) предприятия.

**По теме 10.**

1. Оценка экологической безопасности предприятия
2. Количественная оценка воздействия предприятия на окружающую среду
3. Экоэффективность предприятия
4. Финансовые и экологические параметры
5. Экологическая безопасность производственной системы
6. Экологическая эффективность менеджмента компании
7. Факторы воздействия на экологию и оценочные показатели состояния окружающей среды.

**По теме 11.**

1. Объекты предприятия, нуждающиеся в защите
2. Организация защиты коммерческой тайны.

3. Цели и задачи охраны предприятия

4. Служба охраны предприятия

5. Структура службы безопасности

6. Функции службы безопасности.

**По теме 12.**

1. Экономическая безопасность государства.

2. Национальная экономическая безопасность

3. Сравнительный анализ мировой практики обеспечения экономической безопасности

4. Экономическая безопасность в Российской Федерации

5. Экономическая безопасность Республики Узбекистан.

## Тесты

### Тесты контроля (1-го модуля)

#### 1. Хакер -

- А) это лицо, которое взламывает интрасеть в познавательных целях;
- Б) это мошенник, рассылающий свои послания, в надежде обмануть наивных и жадных;
- В) это лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов разрушающих ПО;
- Г) так в XIX веке называли плохого игрока в гольф, дилетанта;
- Д) это мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

#### 2. Фракер -

- А) это лицо, которое взламывает интрасеть в познавательных целях;
- Б) это мошенник, рассылающий свои послания, в надежде обмануть наивных и жадных;
- В) это лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов, разрушающих ПО;
- Г) так в XIX веке называли плохих игроков в гольф, дилетантов;
- Д) это мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

#### 3. Фишер -

- А) это лицо, которое взламывает интрасеть в познавательных целях;
- Б) это мошенник, рассылающий свои послания, в надежде обмануть наивных и жадных;

В) это лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов разрушающих ПО;

Г) так в XIX веке называли плохого игрока в гольф, дилетанта;

Д) это мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

#### 4. Скамер –

А) это лицо, которое взламывает интрасеть в познавательных целях;

Б) это мошенник, рассылающий свои послания, в надежде обмануть наивных и жадных;

В) это лицо, изучающее систему с целью ее взлома и реализующее свои криминальные наклонности в похищении информации и написании вирусов разрушающих ПО;

Г) так в XIX веке называли плохого игрока в гольф, дилетанта;

Д) это мошенники, которые обманным путем выманивают у доверчивых пользователей сети конфиденциальную информацию.

#### 5. Финансовая безопасность это:

А) эффективное функционирование финансовой системы;

Б) обеспечение безопасного функционирования всех элементов финансово-экономического механизма страны;

В) стабильный курс национальной валюты.

#### 6. К внутренним угрозам экономической безопасности относятся:

А) структурные изменения экономики;

Б) демографические изменения и проблемы занятости;

В) высокий внешний долг;

Г) высокий внутренний долг.

7. Государственная стратегия экономической безопасности является:

- А) составной частью стратегии национальной безопасности;
- Б) приоритетным направлением экономической политики государства;
- В) доминирующей над государственной стратегией национальной безопасности.

8. Совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства, это:

- А) безопасность;
- Б) жизненно важные интересы;
- В) субъекты экономической безопасности.

9. Что из нижеперечисленного не является способом «утечки» капиталов:

- А) челночная торговля;
- Б) «импорт воздуха»;
- В) завышение контрактных цен на импортные товары по сравнению с фактическими ценами;
- Г) завышение контрактных цен на экспортные товары по сравнению с фактическими ценами.

10. Разрастание какой из сфер российской экономики в период рыночных реформ носило паразитарно-спекулятивный характер:

- А) внешнеторговой;
- Б) энергетической;
- В) добывающей;
- Г) кредитно-финансовой.

11. Постоянное наращивание производственного и научно-технического потенциалов, это интересы:

- А) общества;
- Б) государства;
- В) личности.

12. Усиление протекционизма во внешней политике страны свидетельствует:

- А) о необходимости предотвращения экономических потрясений;
- Б) о полном самообеспечении страны за счет собственных ресурсов;
- В) о том, что резко возросший импорт угрожает национальному производству отдельных товаров.

13. Попытки зарубежных государств устранить продавцов высокотехнологичных товаров и современных услуг с мировых рынков, это:

- А) нормальная практика ВЭД, применяемая всеми странами;
- Б) внешняя угроза внешнеэкономическим интересам России;
- В) внутренняя угроза внешнеэкономическим интересам России.

14. Экономическая безопасность – это способность системы:

- А) сохранять устойчивость по отношению к негативным внешним воздействиям;
- Б) сохранять устойчивость по отношению к негативным внутренним воздействиям;
- В) оставаться неизменной, т. е. не деградировать и не развиваться.

15. Деформация структуры российской экономики обусловлена:

- А) усиление топливно-сырьевой направленности экономики;
- Б) высокая конкурентоспособность продукции большинства отечественных предприятий;

В) рост внешнего долга России и связанное с этим увеличение расходов госбюджета на его погашение.

16. К негативным последствиям проведения приватизации в Российской Федерации относятся:

- А) рост числа негосударственных предприятий;
- Б) переход контроля над значительной частью отечественных предприятий к иностранцам;
- В) рост товарного предложения.

17. Действия системы экспортного контроля направлены:

- А) на недопущение вывоза оружия массового уничтожения;
- Б) на недопущение вывоза товаров народного потребления;
- В) на недопущение вывоза отдельных видов сырья, материалов.

18. К угрозам экономической безопасности во внешнеэкономической сфере относятся:

- А) незаконный вывоз подакцизных товаров;
- Б) долларизация экономики;
- В) рост экспорта.

19. К внутренним угрозам энергетической безопасности относятся:

- А) прохождение некоторых энергосетей по территории страны;
- Б) дефицит капиталовложений;
- В) ослабление негативного воздействия предприятий ТЭК на экологию и социальную сферу.

20. Закрепление хозяйствующих субъектов на мировых рынках товаров и услуг и постепенное усиление их роли на этих рынках является:

- А) жизненно важным интересом внешнеэкономической безопасности;
- Б) потенциальной внутренней угрозой внешнеэкономической безопасности;
- В) критерием обеспечения внешнеэкономической безопасности.

21. К каналам «утечки» за границу сведений о новейших технологиях и результатах НИР относятся:

- А) непродуманность публикаций;
- Б) предоставление зарубежными неправительственными организациями грантов перспективным научным коллективам и отдельным ученым;
- В) контроль со стороны зарубежных ФПП над научно-производственной базой многих российских предприятий;
- Г) все вышеперечисленное.

22. Основной причиной возникновения угроз национальной безопасности страны является кризисное состояние в этой сфере:

- А) военной;
- Б) экономической;
- В) энергетической;
- Г) экологической.

23. Экономическая безопасность- это такое:

- А) состояние экономики, при котором обеспечивается стабильность экономических процессов на государственном уровне, эффективное управление, защита экономических интересов государства на международном уровне;

Б) состояние экономики, при котором обеспечивается устойчивый экономический рост приоритетных отраслей промышленности, достаточное удовлетворение потребностей отдельных социальных слоев населения;

В) состояние экономики, при котором обеспечивается устойчивый экономический рост, достаточное удовлетворение общественных потребностей, эффективное управление, защита экономических интересов на национальном и международном уровнях;

Г) состояние экономики, обеспечивающее достаточный уровень оборонного существования страны, неуязвимость и независимость ее военных интересов по отношению к возможным внешним и внутренним угрозам и воздействиям.

24. К внутренним факторам, представляющим угрозу экономической безопасности, относятся:

А) сырьевая ориентация экспорта;

Б) низкая конкурентоспособность экономики;

В) усиление импортной зависимости;

Г) усиление зависимости от внешних инвестиций.

25. Первый шаг государства по обеспечению экономической безопасности:

А) разработка параметров и критериев экономической безопасности;

Б) разработка концепции экономической безопасности;

В) мониторинг факторов, определяющих угрозы экономической безопасности;

Г) разработка пороговых значений экономической безопасности.

26. Индекс Дали-Кобба:

- А) индекс устойчивого экономического благосостояния, при его расчетах делаются поправки на издержки экологического характера, связанные с нерациональным природопользованием;
- Б) обобщающий показатель уровня экономического развития и уровня обеспечения экономической безопасности;
- В) индекс устойчивого экономического роста;
- Г) обобщающий показатель уровня ВВП и уровня обеспечения экономической безопасности.

27. Раскрытие сущности понятия "экономическая безопасность" связано:

- А) с пониманием угрозы безопасности;
- Б) с пониманием угрозы безопасности, исходящей от источников опасности;
- В) с пониманием источников опасности.

28. Экономическая безопасность подразделяется на следующие уровни:

- А) международная, национальная, локальная и частная;
- Б) глобальная, региональная, фирм и личности;
- В) международная, региональная или отраслевая внутри страны.

29. По размеру и масштабам возможных негативных последствий опасности могут быть:

- А) международные, национальные, локальные;
- Б) глобальные и региональные в смысле регионов мира и частные;
- В) международные, национальные, локальные и частные

30. К объектам экономической безопасности относятся: государство, его экономическая система и все его природные богатства, общество с его институтами, учреждениями, фирмами и личность. Так ли это?

- А) да;

Б) нет.

31. Включает ли стратегия экономической безопасности характеристику, угроз экономической безопасности как совокупность условий и факторов, создающих опасность жизненно важным экономическим интересам личности, общества и государства?

А) да, включая угрозы внутренние и внешние:

Б) да, включая лишь угрозы внутренние:

В) нет.

32. Банки, биржи, фонды и страховые компании являются ли они субъектами экономической безопасности?

А) да;

Б) нет.

33. Представляют ли, в настоящее время, внутренние угрозы наибольшую опасность экономической безопасности предприятия?

А) да;

Б) нет.

34. Усиление и активизация разведывательной деятельности иностранных государственных и межгосударственных специальных служб в экономической сфере являются проявлением:

А) внешней угрозы;

Б) внутренней угрозы.

35. В чем отличие объективных негативных воздействий от субъективных негативных воздействий?

А) объективные негативные воздействия возникают без участия и помимо воли предприятия или его служащих, а субъективные

негативные воздействия возникают как следствие неэффективной работы предприятия или его работников;

Б) объективные негативные воздействия возникают как следствие форс мажорных обстоятельств, а субъективные негативные воздействия возникают как следствие неэффективной работы руководителей и сотрудников предприятия.

36. Экономическая разведка содействует в комплексе и во взаимосвязи специальными силами и средствами:

А) внешнеэкономическому курсу государства;

Б) коммерческой деятельности предприятий;

В) внешнеэкономическому курсу государства и коммерческой деятельности предприятий.

### **Тесты контроля (2-го модуля)**

1. Безопасность - это:

1.1. Минимизация рисков

1.2. Защищенность от угроз

1.3. Компенсация ущерба

2. Угроза - это:

2.1. Вероятность ущерба

2.2. Опасность

2.3. Совокупность неблагоприятных факторов

3. Конфиденциальность - это:

3.1. Условие защиты коммерческой тайны

3.2. Форма проявления коммерческой тайны

3.3. Секретность информации

4. Коммерческая тайна - это:

4.1. Информация, имеющая рыночную стоимость

4.2. Конфиденциальная информация коммерческой организации

4.3. Защищаемая ценная информация коммерческой организации

5. Интеллектуальная собственность - это:

5.1. Нематериальные активы организации

5.2. Исключительное право лица на результаты интеллектуальной деятельности

5.3. Патенты и авторские права

6. Оптимальный размер затрат на охрану коммерческой тайны

6.1. 5% к себестоимости продукции

6.2. 15%

6.3. 25%

7. Допустимые значения коэффициента абсолютной ликвидности

7.1. 0.1-0.2

7.2. 0.2-0.5

7.3. 0.5-0.7

8. Степень риска оценивается с использованием методик

8.1. SWOT – анализа

8.2. Шеррингтона

8.3. Лоренца

9. Для собирания доказательств по факту нарушения хозяйственной деятельности используются приемы:

9.1 . АХД

9.1. Ревизия

9.3. Экспертиза

10. При интеллектуальном подлоге:

10.1 . В подлинный документ вносятся изменения

10.2 . В подлинном документе сведения не соответствуют фактическим

10.3 . Документ заменяется новым

11. Проверка персональной информации при найме на работу в открытые организации:

11.1. Проводится без согласия работника

11.2. Проводится с письменного согласия работника

11.3. Проводится по указанию органов МВД

12. Треугольник мошенничества - это:

12.1. Характеристика субъектов мошенничества

12.2. Перечень признаков мошенничества

12.3. Оценка условий мошенничества

13. Сговор в трудовых отношениях оценивается

как:

13.1. Форма уголовно-наказуемых отношений

13.2 Форма девиантных отношений

13.3. Форма деликвентных отношений

14. Право воздействовать на поведение других людей определяется как:

14.1. Ответственность

14.2. Власть

14.3. Полномочия

15. Характер неформальных отношений в коллективе опреде-

ляют:

15.1. Руководитель

15.2. Работники

15.3. Профсоюз

16. Управление социальными инновациями направлено на:

16.1. Изменение оплаты труда

16.2 . Изменение квалификации работников

16.3 . Изменение отношений в коллективе

17. Оптимальное значение коэффициента текучести:

17.1. 2%

17.2. 5%

17.3. 10%

18. Заявление об увольнении подается за:

18.1. 2 мес.

18.2. 2 недели

18.3. 1 мес.

19. Запись в трудовую книжку делается:

19.1. Немедленно при поступлении на работу

19.2. В течение 1 недели

19.3. По истечении испытательного срока

20. В качестве меры воздействия на работника штраф:

20.1. Разрешен законодательством о труде

20.2. Запрещен

20.3. Установлен условиями трудового договора.

21. Интеллектуальная собственность

21.1. Знания, умения, навыки

21.2. Результаты интеллектуальной деятельности лица

21.3. Нематериальные активы.

22. Секретность

- 22.1. Тайна
- 22.2. Форма выражения тайны
- 23.3. Гриф доступа к документу

## 23. Мошенничество

- 23.1. Противоправное поведение
- 23.2. Завладение имуществом путем обмана
- 23.3. Злоупотребление доверием

## 24. Организационные меры защиты материальных активов

- 24.1. Защита в суде
- 24.2. Учет и охрана
- 24.3. Материальные санкции

## 25. Информационная безопасность

- 25.1. Защита информации
- 25.2. Состояние, обеспечивающее защиту информации
- 25.3. Минимизация информационных рисков

## 26. Критерии экономической безопасности

- 26.1. Значения
- 26.2. Условия
- 26.3. Основания

## 27. Имущественные права

- 27.1. Определяют условия владения имуществом

27.2. Являются элементом вещного права

27.3. Определяют условия распоряжения имуществом

28. Меры по защите имущественных интересов акционеров определяются

28.1. Приказом руководителя

28.2. Уставом акционерного общества

28.3. Решением Совета директоров

29. Финансовая устойчивость предприятия определяется

29.1. Величиной собственных средств

29.2. Долей заемного капитала в валюте баланса

29.3. Платежеспособностью предприятия

30. Материальный подлог

30.1. Замена документа

30.2. Подчистка данных в документе

30.3. Изъятие документа

31. Интеллектуальный подлог

31.1. Несоответствие содержания документа форме документа

31.2. Несоответствие содержания документа факту

31.3. Несоответствие формы документа его содержанию

32. Перечень сведений, составляющих коммерческую тайну

- 32.1. Утверждается правительством государства
  - 32.2. Утверждается руководителем предприятия
  - 32.3. Приводится в соглашении о неразглашении коммерческой тайны
33. Документы, содержащие коммерческую тайну, имеют гриф
- 33.1. Секретно
  - 33.2. Конфиденциально
  - 33.3. Для служебного пользования
34. Персональная информация
- 34.1. Сведения о личности
  - 34.2. Информация, позволяющая идентифицировать личность
  - 34.3. Паспортные данные
35. Проверка персональной информации
- 35.1. Осуществляется с согласия работника
  - 35.2. Не требует согласия работника
  - 35.3. Осуществляется в обязательном порядке
36. Оптимальный уровень затрат на обеспечение экономической безопасности (% в себестоимости)
- 36.1. 5%
  - 36.2. 15%
  - 36.3. 25%

## 37. Гриф секретности

37.1. Условие

37.2. Знак

37.3. Показатель

## 38. Управление риском это

38.1. Избежание риска

38.2. Минимизация риска

38.3. Принятие риска

## 39. Признаки мошенничества предполагают наличие

39.1. Криминальной ситуации

39.2. Треугольника мошенничества

39.3. Ущерба

## 40. Досье это

40.1. Анкета работника

40.2. База данных

40.3. Личное дело

## Темы рефератов

1. Экономическая безопасность: сущность, виды безопасности, их характеристика.
2. Теневой сектор экономики: причины существования и методы оценки.
3. Государственный долг: классификация, допустимые размеры и его роль в обеспечении финансовой безопасности страны.
4. Финансовая безопасность: сущность, показатели оценки.
5. Банковская безопасность: сущность, показатели оценки.
6. Концепция экономической безопасности Российской Федерации.
7. Налоговая безопасность: сущность, показатели оценки.
8. Экономическая безопасность в системе национальной безопасности страны.
9. Безопасность страны: сущность и место экономической безопасности.
10. Стратегия экономической безопасности Российской Федерации.
11. Экономическая безопасность: характеристика и её классификация.
12. Налоговая безопасность: понятие, критерии оценки в федеративном государстве.
13. Теневая экономика в Российской Федерации и её влияние на экономическую безопасность страны.
14. Экономическая безопасность как элемент национальной безопасности страны.
15. Оценка уровня экономической безопасности страны.
16. Методы расчета уровня экономической безопасности региона.
17. Основные направления обеспечения экономической безопасности

предприятий региона.

18. Организационно - экономические особенности управления системой
19. экономической безопасности.
20. Становление современной методологии оценки экономической безопасности социально-экономических систем.
21. Механизм управления экономической безопасностью социально-экономических систем.
22. Объективные предпосылки формирования механизма экономической
23. безопасности социально-экономических систем.
24. Налоги как материальная основа экономической мощи страны (на примерах официальной статистики).
25. Теоретическое обоснование необходимости создания механизма экономической безопасности страны.
26. Зарубежный опыт (опыт отдельных стран: США, Франция, Япония, Германия, Великобритания и др.) по обеспечению экономической безопасности (государства, региона, фирмы, домашнего хозяйства и т.д.).
27. Обоснование критериев и показателей различных уровней экономической безопасности (государство, регион, отрасль, организация, личность).
28. Системы экономической безопасности (мирового сообщества, государства, региона, организации, личности).
29. Виды экономической безопасности (финансовая, производственная, коммерческая, банковская, информационная, инвестиционная, инновационная, кадровая, продовольственная, энергетическая, сырьевая, транспортная, научно-техническая и др.).
30. Теневая экономика как угроза экономической безопасности государства.

31. Методы оценки уровня теневой экономики (государства, региона).
32. Методика диагностики опасностей и угроз экономической безопасности (государства, региона, организации).
33. Концепция экономической безопасности (государства, региона, организации).
34. Конкурентоспособность продукции и ее влияние на экономическую безопасность страны.
35. Энергетическая безопасность как условие обеспечения экономической безопасности страны.
36. Обеспечение экологической безопасности.
37. Институциональные основы системы экономической безопасности.
38. Транспортная безопасность как условие обеспечения экономической безопасности.
39. Ценовой фактор в обеспечении продовольственной безопасности.
40. Инновации и экономическая безопасность страны
41. Экономическая безопасность фирмы: проблемы и перспективы
42. Опыт развитых стран в обеспечении экономической безопасности
43. Организационно-экономические особенности управления системой экономической безопасности государства
44. Налоговый контроль и его влияние на экономическую безопасность страны
45. Зарубежный опыт (опыт отдельных стран: США, Франция, Япония, Германия, Великобритания и др.) по обеспечению экономической безопасности государства

46. Теневая экономика как угроза экономической безопасности государства
47. Теневая экономика как угроза экономической безопасности государства.
48. Теория и методология финансовой безопасности государства.
49. Основы финансовой безопасности домохозяйств.
50. Финансовая безопасность частных и непрофессиональных инвесторов на финансовых рынках.
51. Безопасность платежной и денежно-кредитной систем как часть финансовой безопасности государства.
52. Методы государственного регулирования в сфере финансовой безопасности государства.
53. Система управления кредитными рисками в коммерческом банке.
54. Роль службы внутреннего контроля в управлении рисками в коммерческом банке.
55. Экономическая политика государства.
56. Опыт ЕС в обеспечении продовольственной безопасности.
57. Формирование глобальной продовольственной безопасности.
58. Особенности реализации концепции продовольственной безопасности на региональном уровне.
59. Продовольственная безопасность страны: особенности оценки в Республике Узбекистан.
60. Экономическая безопасность Республики Узбекистан.

## Контрольные вопросы для самостоятельных работ

1. Дайте определение основным понятиям. Экологическая безопасность. Экологические риски. Сертификация. Природоохранные капитальные вложения. Опасность. Стандартизация. Продовольственная безопасность. Государственное регулирование экологии.
2. Дайте определение пороговых значений экономической безопасности предприятия (организации).
3. Должно ли государство регулировать инвестиционную деятельность?
4. Какие индикаторы состояния информационной составляющей экономической безопасности предприятия?
5. Какие способы обеспечения информационной составляющей экономической безопасности предприятия вы знаете?
6. Какова сущность финансовой составляющей экономической безопасности предприятия.
7. Каковы методы расчета инвестиционного риска?
8. Каковы основные индикаторы состояния технико-технологической составляющей экономической безопасности предприятия?
9. Каковы основные направления и способы обеспечения экономической безопасности предприятия?
10. Каковы основные организации обеспечения экономической безопасности предприятия?
11. Когда предприятие прибегает к внешнему кредиту? Где границы его выгоды?
12. Может ли быть произведена защита вычислительной техники?
13. Назовите и охарактеризуйте финансовые риски предприятия.
14. Обоснуйте положение, согласно которому институт несостоятельности (банкротства) является комплексным институтом права.
15. Организация материальной ответственности персонала.
16. Основная сущность экологической составляющей.

17. Основные индикаторы состояния финансовой составляющей экономической безопасности предприятия.
18. Основные индикаторы экологической составляющей экономической безопасности предприятия.
19. Понятие, классификация, особенности кадровых рисков.
20. Раскройте содержание внутренних и внешних угроз экономической безопасности предприятия?
21. Риски найма и продвижения персонала.
22. Создание и организация структур служб безопасности.
23. Способы обеспечения интеллектуальной и кадровой составляющей экономической безопасности предприятия.
24. Способы обеспечения политико-правовой составляющей экономической безопасности предприятия.
25. Сущность политико-правовой составляющей экономической безопасности предприятия.
26. Что необходимо знать, чтобы обеспечить финансовую безопасность?
27. Что представляет собой правовая защита информации?
28. Что такое обязательные платежи?
29. Что такое технико-технологическая составляющая экономической безопасности предприятия?
30. В чем разница между финансовой безопасностью государства и финансовой безопасностью предприятия.

## **Задания для самостоятельных работ (кейсы)**

Задание 1. Организация работает с информацией, составляющей государственную тайну, и информацией, являющейся коммерческой тайной. Дайте сравнительную характеристику государственной и коммерческой тайн. Предложите мероприятия по защите как государственной, так и коммерческой тайн.

Задание 2. Многие российские технологии были вытеснены зарубежными. Доля финансовых средств, направляемых российскими предприятиями на инновационную деятельность, составляет не более 5%, что в 10 - 15 раз ниже, чем в промышленно-развитых странах. Объем России в мировом объеме торговли гражданской наукоемкой продукцией оценивается лишь в 0,3%. Так, например, в КНР этот показатель составляет 6%. Объясните с чем это связано, и как это влияет на экономическую безопасность предприятия?

Задание 3. Почему раскрытие компьютерного преступления часто бывает связано с чистой случайностью? Например, однажды сотрудник вычислительного центра, который обслуживал несколько нефтяных компаний, обратил внимание, что у одного из клиентов перед тем, как загорится световой индикатор записи, всегда долгое время светится индикатор считывания. Проведенное расследование показало, что этот человек занимался промышленным шпионажем и продавал данные компании компаниям-конкурентам.

Задание 4. Наблюдатели отмечают, что по мере научно-технического развития и притока большого количества промышленных инноваций границы прежних представлений о морально правильных действиях и этически правильной жизни будут все чаще нарушаться. Согласны ли вы с этим?

Задание 5. Назначенный собственником финансовый менеджер фирмы неэффективно с позиции собственника управляет финансами. Охарактеризуйте оценочные показатели работы менеджера. Сформулируйте мероприятия, позволяющие взять ситуацию под контроль. Оцените их эффективность.

Задание 6. Охраной отмечены случаи воровства рабочими слесарного инструмента. Руководство цеха не подтверждает случаи хищения. Определите

причины возникшей ситуации. Сформулируйте оценочные показатели диагностики ситуации. Разработайте мероприятия, исключающие возможность повторения ситуации.

Задание 7. «Не будь ни должником, ни кредитором», - советовал Полоний своему сыну в пьесе Уильяма Шекспира. Если бы вы были руководителем предприятия, последовали бы вы этому совету?

Задание 8. Назначенный собственником финансовый менеджер фирмы неэффективно с позиции собственника управляет финансами. Охарактеризуйте оценочные показатели работы менеджера. Сформулируйте мероприятия, позволяющие взять ситуацию под контроль. Оцените их эффективность.

Задание 9. Охраной отмечены случаи воровства рабочими слесарного инструмента. Руководство цеха не подтверждает случаи хищения. Определите причины возникшей ситуации. Сформулируйте оценочные показатели диагностики ситуации. Разработайте мероприятия, исключающие возможность повторения ситуации.

Задание 10. Работник в грубой форме отреагировал на замечание руководителя в связи с опозданием на работу. Свидетелей не было. Оцените ситуацию, назвав причины. Предложите тактику действий руководителя. Сформулируйте мероприятия, исключающие повторение подобных ситуаций.

Задание 11. Вы являетесь руководителем службы управления персоналом и включены в состав комиссии по разработке программы экономической безопасности предприятия. Определите возможные кадровые риски. Оцените вероятность этих рисков. Разработайте мероприятия, снижающие вероятность кадровых рисков.

Задание 12. Руководство фирмы, реализуя стратегию развития, поставило перед Вами - руководителем кадровой службы - задачу минимизировать кадровые риски. Сформулируйте кадровые риски. Предложите показатели и методики, обеспечивающие возможность прогнозирования кадровых рисков.

Задание 13. На предприятии широко используются информационные технологии. Для обеспечения информационной безопасности кадровой

службе предложено разработать комплекс организационных мероприятий. Сформулируйте концепцию. Определите основные задачи. Сформулируйте первоочередные меры.

Задание 14. Для разработки программы экологической безопасности на предприятии необходимо иметь по возможности полную информацию об угрозах, рисках, ущербе. Дайте определения угрозы, риска. Охарактеризуйте основные методики оценки угроз и рисков. Приведите методику оценки ущерба.

Задание 15. Рассматривая влияние водного фактора на состояние здоровья населения, установлено, что неинфекционная заболеваемость, связанная с водой, может быть обусловлена такими моментами, как: - повышенное или пониженное содержание микроэлементов; - наличие токсических и радиоактивных веществ; - зависимость между химическим составом питьевых вод и показателями физического развития, иммунобиологической реактивности, состояния сердечно-сосудистой системы. Что нужно сделать, чтобы снизить или вообще исключить эти негативные моменты?

Задание 16. Часто причину аварии связывают с ошибками действия оператора, нарушившего ту или иную из многочисленных инструкций. Действительно, ошибки и сознательное отсутствие от инструкций стали скорее нормой, чем исключением в работе операторов целых отраслей промышленности. В чем причина этого явления? Неужели только в массовой халатности операторов? Например, при расследовании причин аварии Чернобыльской АЭС среди основных виновников были названы операторы, нарушившие ряд пунктов инструкции по эксплуатации оборудования. Но ни в одной из инструкций не было даже намека на то, что подобные нарушения могут привести к взрыву энергоблока. Более того, в любой литературе по безопасности реакторов, применяемых на станции, указывалось, что взрыв в принципе невозможен. Как бы вы прокомментировали это?

## Вопросы к экзамену

1. Виды безопасности
2. Внешние опасности и угрозы экономической безопасности государства
3. Внешние угрозы экономической безопасности предприятия
4. Внутренние опасности и угрозы экономической безопасности государства
5. Внутренние угрозы экономической безопасности предприятия
6. Глобализация: плюсы и минусы
7. Государственная стратегия экономической безопасности РФ
8. Демографическая безопасность
9. Деструктивные факторы, влияющие на экономическую безопасность
10. Инвестиционная безопасность и институты коллективного инвестирования
11. Инновации и экономическая безопасность
12. Информационная безопасность как составной элемент экономической безопасности бизнеса
13. Источники опасностей экономической безопасности предприятия
14. Классификация и оценка экономической безопасности предприятия
15. Классификация угроз экономической безопасности
16. Конкурентоспособность и экономическая безопасность: определяющие факторы и теории
17. Коррупция как угроза экономической и национальной безопасности
18. Критерии и параметры состояния экономики, отвечающие требованиям экономической безопасности РФ
19. Критерии и показатели экономической безопасности государства
20. Критерии экономической безопасности государства
21. Культура как фактор экономической безопасности
22. Меры и механизмы экономической политики, направленные на обеспечение экономической безопасности

23. Необходимость финансовой безопасности государства. Финансовая безопасность, ее сущность.
24. Объекты безопасности предприятия
25. Объекты государственной стратегии экономической безопасности
26. Опыт зарубежных государств в обеспечении безопасности предпринимательской деятельности
27. Основные меры по укреплению безопасности госбюджета. Безопасность финансово-денежной системы государства и меры по ее обеспечению.
28. Основные угрозы экономической безопасности предприятия
29. Открытость экономики: потенциальные угрозы открытости
30. Показатели национальной экономической безопасности государства
31. Показатели экономической безопасности государства
32. Понятие экономической безопасности
33. Понятие экономической безопасности предприятия
34. Принципы обеспечения безопасности государства
35. Принципы организации системы экономической безопасности предприятия
36. Система финансовой безопасности.
37. Меры по укреплению финансовой безопасности государства.
38. Содержание экономической безопасности
39. Социальная и демографическая безопасность: безопасность личности. Безработица.
40. Субъекты безопасности государства
41. Субъекты безопасности предприятия
42. Сущность внешнеэкономической безопасности.
43. Теневая экономика как угроза экономической безопасности государства
44. Угрозы внешнеэкономической безопасности.
45. Угрозы теневой экономики национальным интересам России
46. Управление экономической безопасностью региона
47. Уровни безопасности

48. Уровни глобализации экономики
49. Функции системы безопасности
50. Цели государственной стратегии экономической безопасности

## Список литературы

### Основная литература:

1. Бочаров В.П. Экономика и организация производства: учеб. пособие / под ред. Ю.И. Трещевского, Ю.В. Вертаковой, Л.П. Пидоймо ; рук. авт. кол. Ю.В. Вертакова. - М.: ИНФРА-М, 2018. - 381 с.: Режим доступа: <http://znanium.com/catalog/product/814430>

2. Бухалков М.И. Производственный менеджмент: организация производства: Учебник / М.И. Бухалков. – 2-е изд. – М.: НИЦ ИНФРА-М, 2018. – 395 с. – Режим доступа: <http://znanium.com/catalog.php?bookinfo=949884>

3. Кормишкина Л.А. Экономическая безопасность организации (предприятия) : учебное пособие / Л.А. Кормишкина, Е.Д. Кормишкин, И.Е. Илякова. — М. : РИОР : ИНФРА-М, 2018. — 293 с. — URL: <http://znanium.com/catalog/product/951723>

4. Экономика, организация и управление промышленным предприятием: учебник / Е.Д. Коршунова, О.В. Попова, И.Н. Дорожкин, О.Е. Зимовец, с.в. Курилова, А.Г. Схиртладзе, А.А. Корниенко. — М.: КУРС: Инфра-м, 2018. — 272 с. – URL: <http://znanium.com/catalog/product/930126>

5. Экономическая безопасность: учеб. пособие / под ред. Н.В. Манохиной. — М.: ИНФРА-М, 2019. — 320 с. — URL: <http://znanium.com/catalog/product/993528>

### *Нормативно-правовые документы:*

1. Закон Республики Узбекистан «О гарантиях свободы предпринимательской деятельности» (Новая редакция). Настоящая редакция утверждена Законом РУз от 02.05.2012 г. № ЗРУ-328 с изменениями в соответствии с Законом РУз от 29.12.2015 № ЗРУ-396. (Народное слово, 3 мая 2012 г.; Собрание законодательства Республики Узбекистан, 2012 г., N 18, ст. 201; Ведомости палат Олий Мажлиса Республики Узбекистан, 2012 г., N 5, ст. 133)

2. Указ Президента Республики Узбекистан № УП-4848 от 05.10.2016 г. «О дополнительных мерах по обеспечению ускоренного развития предпринимательской деятельности, всемерной защите частной собственности и качественному улучшению делового климата» (Собрание законодательства Республики Узбекистан, 2016 г., № 40, ст. 467, 2017 г., № 37, ст. 982; Национальная база данных законодательства, 20.02.2018 г., № 06/18/5347/0788) URL: <http://www.press-service.uz/ru/document/5340/>

3. ISO 9001 - Quality Management Systems – Requirements / The ISO Survey of Management System Standard Certifications (1993-2015) – Режим доступа: [http://www.iso.org/iso/home/standards/management-standards/iso\\_9000.htm](http://www.iso.org/iso/home/standards/management-standards/iso_9000.htm).

Дополнительная литература:

1. Бухалков М. И. Организация и нормирование труда: Учебник для вузов/Бухалков М. И., 4-е изд., испр. и доп. – М.: НИЦ ИНФРА-М, 2016.- 380 с. – Режим доступа: <http://znanium.com/catalog.php?bookinfo=526939>
2. Генкин Б.М. Организация, нормирование и оплата труда на промышленных предприятиях: Учебник для вузов / Б.М. Генкин. - 6-е изд., изм. и доп. – М.: Норма: НИЦ ИНФРА-М, 2014. – 416 с. – Режим доступа: <http://znanium.com/catalog.php?bookinfo=462619>
3. Голов Р.С. и др. Системы управления инновационно-инвестиционной деятельностью промышленных организаций и подготовкой машиностроительного производства [Электронный ресурс] : Монография / Р. С. Голов А. В. Рождественский А. П. Агарков и др.; под ред. д.э.н., проф. Р. С. Голова, д.э.н., проф. А. В. Рождественского. – М.: Издательско-торговая корпорация «Дашков и Ко», 2014. – 448 с. – Режим доступа: <http://znanium.com/catalog.php?bookinfo=512676>
4. Грядов С.И. и др. Организация сельскохозяйственного производства: Учебное пособие / Грядов С.И. и др.; Под ред. М.П. Тушканова, Ф.К. Шакирова. - М.: НИЦ ИНФРА-М, 2014. - 292 с. – Режим доступа: <http://znanium.com/catalog.php?bookinfo=427186>

5. Минько Р.Н. Организация производства на транспорте: Учебное пособие / Р.Н.Минько – М.: Вузовский учебник, НИЦ ИНФРА-М, 2015. –160 с.– Режим доступа: <http://znanium.com/catalog.php?bookinfo=501811>
6. Организация энергосбережения (энергоменеджмент). Решения ЗСМК-НКМК-НТМК-ЕВРАЗ: Учебное пособие / Под ред. Кондратьев В.В. – М.:НИЦ ИНФРА-М, 2017. – 108 с. – Режим доступа: <http://znanium.com/catalog.php?bookinfo=599254>
7. Тушканов М.П. и др. Организация сельскохозяйственного производства : учебник / М.П. Тушканов, С.И. Грядов, А.К. Пастухов [и др.] ; под ред. М.П. Тушканова, Ф.К. Шакирова. – М. : ИНФРА-М, 2017. – 292 с. – Режим доступа: <http://znanium.com/catalog.php?bookinfo=809825>
8. Устойчивая конкурентоспособность компаний высокотехнологичных отраслей: моногр./И.П. Комарова. – М.: Русайнс, 2017. Источник: <https://www.rea.ru/ru/org/managements/biblcentr/Pages/reviews.aspx> © ФГБОУ ВО «РЭУ им. Г.В. Плеханова»
9. Колупаев В.А. Формирование концепции национальной экономической безопасности в зарубежных странах. //Белорусская экономика: анализ, прогноз, регулирование. - Экономический бюллетень НИЭИ Минэкономики РБ. – Минск. - 2002. № 12. -С.2-9.
- 10.Никитенко П.Г., Булавко В.Г. Экономическая безопасность: теория, методология, практика. - Институт экономики НАН Беларуси. – Минск: Право и экономика, 2009.- 483 с.
11. К. Арыстанбеков Государственное обеспечение экономической безопасности в США. // Фемида. - 2002. - №8. - С. 58-60.
12. Арменский А. Е., Гусев В. С., Петров А. Е. Информационная и экономическая безопасность государства. Учебно-методическое пособие для государственных служащих. –Москва: Мобиле, 2003.-С. 153.
13. Прилепский А. И. Формирование механизма обеспечения экономической безопасности в народнохозяйственном комплексе: дис. канд. экон. наук: 08.00.05.– М.,1999.– 222

14. A Strong Britain in an Age of Uncertainty: The National Security Strategy. // Официальный сайт Министерства Обороны Великобритании: <http://www.official-documents.gov.uk>
15. Осереpek Economic Security and the European Dream. // [Электронный ресурс]: Marquette University.

**Перечень ресурсов  
информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля):**

1. Правительственные порталы – <https://www.press-servis.ru>; [www.presser-vice.uz](http://www.presser-vice.uz); <http://government.ru>; <https://www.gov.uz/uz>;
2. Информационно-правовые системы – <http://www.consultant.ru/>; <http://www.garant.ru/>; <http://www.norma.uz/>; <http://www.kodeks.net>;
3. Электронно-библиотечные системы – <http://www.sciencedirect.com/>; <https://www.aeaweb.org/econlit/>; <http://znanium.com>; <http://absopac.rea.ru/>; <http://cyberleninka.ru/>; <http://elibrary.ru>; <http://bibliotekar.ru>;
4. Экономические порталы – <http://www.economicus.ru>; <http://institutiones.com>; <http://www.economyst.org.ua>;
5. Обзорная информация по мировой экономике - [www.ereport.ru](http://www.ereport.ru);
6. Стратегическое управление и планирование – <http://www.stplan.ru>;
7. Справочник для экономистов – <http://www.catback.ru>.

**Перечень информационных технологий,  
используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем**

№ п/п	Перечень информационных технологий, программного обеспечения, информационных справочных систем	Номера тем
1.	ЕКportal.ru – Информационный сайт по экономике	1-12
2.	Электронно библиотечная система/ <a href="http://znanium.com/">http://znanium.com/</a>	1-12
3.	Научная электронная библиотека «Киберленинка» – <a href="http://cyberleninka.ru/">http://cyberleninka.ru/</a>	1-12
4.	Учебники. – <a href="http://economicus.ru/">http://economicus.ru/</a>	1-12