МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

Государственное образовательное учреждение
высшего профессионального образования
«Оренбургский государственный университет»

Кафедра финансов

Ю.И. БУЛАТОВА

ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
ДЛЯ ПОДГОТОВКИ К СЕМИНАРСКИМ ЗАНЯТИЯМ

Рекомендовано к изданию Редакционно-издательским советом
государственного образовательного учреждения
высшего профессионального образования
«Оренбургский государственный университет»

Оренбург 2009

УДК 346.548(076.5)
ББК 65-983я73
Б 90

Рецензент
канд. экономических наук, доцент кафедры финансов Л.Б. Мохнаткина

Булатова, Ю.И.
Б 90 **Информационно-аналитическое обеспечение экономической безопасности: методические рекомендации для подготовки к семинарским занятиям / Ю.И. Булатова. - Оренбург: ГОУ ОГУ, 2009. – 40 с.**

Методические рекомендации включают в себя содержание основных вопросов по теме занятия; вопросы для зачета по дисциплине; литературу, рекомендуемую для изучения тем, а также по каждой теме семинарского занятия имеются вопросы для дискуссионного обсуждения, задания для индивидуальной работы.

Методические рекомендации предназначены для подготовки к семинарским занятиям по дисциплине «Информационно-аналитическое обеспечение экономической безопасности» студентов специальности 080105 «Финансы и кредит» специализации «Экономическая и информационная безопасность в финансово - кредитной сфере».

ББК 65-983я73

© Булатова Ю.И., 2009
© ГОУ ОГУ, 2009

Содержание

Введение ……..... 4
1 Сущность информации и информатизация общества..... 6
2 Информационная безопасность
и проблемы защиты информации …..…… 8
3 Информационное обеспечение аналитической
деятельности…..……... 12
4 Основные положения экономической безопасности …… 17
5 Обеспечение экономической безопасности
хозяйствующих субъектов…….. 22
6 Информационно-аналитическое обеспечение
в системе экономической безопасности……..... 26
7 Использование специализированных программных
продуктов и аналитических систем для диагностики,
оценки и мониторинга финансового состояния предприятия ……. 29
8 Литература, рекомендуемая для изучения дисциплины……... 33
9 Вопросы для зачета……..……..... 34
Приложение А Классификация угроз
экономической безопасности…..... 36
Приложение Б Модель системы обеспечения
экономической безопасности……... 37
Приложение В Механизм обеспечения
экономической безопасности…..... 38
Приложение Г Мониторинг экономической безопасности……. 39
Приложение Д Индикаторы экономической безопасности…… 40

Введение

Проблема безопасности ведения бизнеса в современной России является одной из самых значимых. Важнейшее место в решении этой проблемы принадлежит информационно-аналитической деятельности по обеспечению экономической безопасности. Вместе с тем, достижение высоких экономических и социальных результатов, обеспечение экономической безопасности невозможны без использования информационных аналитических систем и соответствующих технологий во всех сферах хозяйственной деятельности. В настоящее время трудно назвать область человеческой деятельности, в которой не использовались бы информационные системы. Особенно это относится к сфере управления различными экономическими объектами, где основными являются процессы принятия решений на основе получаемой информации.

Для подготовки выпускников на современном уровне недостаточно только теоретических знаний о современных методах финансового анализа и финансового менеджмента, экономико-математических методах принятия решений. Выпускников необходимо научить правильному использованию информационных систем, дать возможность опробовать полученные теоретические знания на практике и самостоятельно убедиться в справедливости и целесообразности реализуемых теоретических концепций.

Основная цель курса для студентов специальности «Финансы и кредит» состоит в формировании знаний, умений и навыков в области информационно-аналитической деятельности по обеспечению экономической безопасности, применению информационно-аналитических систем и методов для обеспечения экономической безопасности предприятий, организаций, фирм и других структур.

Методические рекомендации разработаны в соответствии с рабочей программой дисциплины.

В результате изучения дисциплины «Информационно-аналитическое обеспечение экономической безопасности» студент:

1) будет иметь представление об основных открытых источниках информации и поставщиках консалтинговых услуг в области экономической безопасности в России и за рубежом;

2) будет знать:

– современное состояние, тенденции развития и совершенствования системы обеспечения экономической безопасности в экономике;

– сущность и значение информационно-аналитической деятельности в системе обеспечения экономической безопасности;

– принципы, методы, формы и способы ведения конкурентной разведки и контрразведки;

– теоретические и организационно-правовые основы информационно-аналитической деятельности по обеспечению экономической безопасности;

– современные информационные технологии и информационные системы информационно-аналитической деятельности по обеспечению экономической безопасности организации;

3) будет уметь:

– организовывать информационно-аналитическую работу по обеспечению экономической безопасности предприятия (организации);

– использовать информационные технологии и информационные системы информационно-аналитической деятельности по обеспечению экономической безопасности организации;

– проводить изучение деловых партнеров и конкурентов, поиск, подбор и проверку потенциальных партнеров;

– выполнять информационно-аналитическую работу с материалами средств массовой информации и ресурсами Интернет.

1 Сущность информации и информатизация общества

План занятия

1 Понятие информации и ее свойства.
2 Информационные ресурсы.
3 Виды информации в предпринимательской деятельности.
4 Сущность, цели и задачи информатизации.

Термин информация происходит от латинского слова informatio, что означает «сведения, разъяснения, изложение».

Следует отметить, что информация – сведения об окружающем мире (объектах, явлениях, событиях, процессах и т. д.), которые уменьшают имеющуюся степень неопределенности, неполноты знаний, отчужденные от их создателя и ставшие сообщениями (выраженными на определенном языке в виде знаков, в том числе и записанными на материальном носителе), которые можно воспроизводить путем передачи людям устным, письменным или другим способом (с помощью условных сигналов, технических средств, вычислительных средств и т. д.).

С точки зрения принятия решений можно считать, что информацией являются данные, оказывающие влияние на поведение системы, используемые в процессе принятия решений или в связи с осуществлением тех или иных действий.

Студент должен знать, что в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», информация - один из видов объектов гражданских прав; сведения о людях, предметах, фактах, событиях и процессах, независимо от формы их представления.

Выделяют следующие свойства, характеризующие качество информации:

– объективность – независимость от чьего-либо мнения или сознания, а также от методов получения;

– полнота – информацию можно считать полной, когда она содержит минимальный, но достаточный для принятия правильного решения набор показателей;

– достоверность – свойство информации быть правильно воспринятой;

– адекватность – степень соответствия реальному объективному состоянию дела;

– доступность – мера возможности получить ту или иную информацию;

– актуальность – это степень соответствия информации текущему моменту времени.

В XXI веке невозможно найти такую область человеческой деятельности, где бы не существовали информационные потоки. Можно сказать, что это время теории и практики информации, в котором информация

подчас становится более важным ресурсом, чем материальные или энергетические.

Информационные ресурсы можно определить:

– в широком смысле – совокупность данных, организованных для эффективного получения достоверной информации;

– по законодательству РФ – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах: библиотеках, архивах, фондах, банках данных, других видах информационных систем.

Студент должен понимать, что информация как ресурс характеризуется:

– количеством – измеряется по-разному, но для человека – степень изменения его знаний в результате ее получения;

– качеством – определяется полезностью обретенных данных;

– себестоимостью – затраты на производство, документирование, хранение, обеспечение сохранности, обработку и передачу по каналам связи;

– ценой – сумма себестоимости и прибыли от реализации информации.

Предпринимательская деятельность тесно взаимосвязана с получением, накоплением, хранением, обработкой и использованием разнообразных информационных потоков, так как информация позволяет хозяйствующим субъектам:

– определять стратегические, тактические и оперативные цели и задачи организации;

– осуществлять контроль за текущим состоянием организации, ее подразделений и процессов в них;

– принимать обоснованные и своевременные решения;

– координировать действия подразделений в достижении целей.

Совокупность всех сведений, циркулирующих в предпринимательской деятельности, можно сгруппировать по следующим направлениям:

1) предпринимательская (коммерческая) информационная система (сведения о состоянии экономической системы, факторах, положительно или отрицательно влияющих на ту сферу хозяйствования и коммерции, в которой действует предприниматель);

2) правовая информационная система (сведения о действующем законодательстве, регулирующем и охраняющем деятельность предпринимательских структур);

3) специально-оперативная информационная система (сведения о способах, силах и средствах обеспечения безопасности предпринимательской информации от доступа третьих лиц).

Студент должен понимать, что важность информации для предприятий ведет к необходимости информатизации.

Термин «информатизация» может пониматься как:

– комплекс мер, направленных на обеспечение оперативного доступа к информационным ресурсам;

– организационный социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов.

Целью информатизации является обеспечение эффективной информационной поддержки решения вопросов деятельности хозяйствующих субъектов.

Вопросы для дискуссионного обсуждения

1 Дайте определение информации с «идейной» и «материальной» точек зрения.

2 Дайте характеристику основным свойствам информации.

3 Что такое информационный ресурс?

4 Какими свойствами обладает информация как ресурс?

5 Что собой представляет «информационное обеспечение деятельности организации»?

6 Какие виды информации встречаются в предпринимательской деятельности?

7 Что такое информатизация?

8 Какие основные задачи информатизации можно выделить?

9 Охарактеризуйте основные виды информации в предпринимательской деятельности.

10 Как подразделяется информация государственных режимных предприятий?

11 Назовите виды предпринимательской информации, циркулирующей в рыночно-конкурентной сфере деятельности.

Задания для индивидуальной работы

1 Проанализируйте различные подходы к определению понятий «информация» и «информатизация».

2 Сравните информацию как ресурс с другими видами ресурсов. Результаты оформите в виде таблицы.

2 Информационная безопасность и проблемы защиты информации

План занятия

1 Понятие информационной безопасности и правовое обеспечение защиты информации.

2 Виды и источники угроз информационной безопасности.

3 Направления защиты информации.

4 Методы противодействия угрозам.

Значимость информационных ресурсов диктует необходимость обеспечения безопасности информации.

Под информационной безопасностью понимают – защищенность жизненно важных интересов личности, общества и государства от преднамеренных или непреднамеренных воздействий в той или иной форме (информационная блокада, информационная интервенция, информационная война, дезинформация и др.), предназначенная для обеспечения сохранности информационных ресурсов государства и законных прав личности и общества в сфере информации.

В качестве стандартной модели безопасности часто приводят модель из трёх категорий:

– конфиденциальность – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право;

– целостность – избежание несанкционированной модификации информации;

– доступность – избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа.

Следовательно, защита информации – совокупность методов и средств, обеспечивающих целостность, конфиденциальность, достоверность, аутентичность и доступность информации в условиях воздействия на нее угроз естественного или искусственного характера.

Как известно, эффективное функционирование любой организационной и организационно-технической системы, в том числе информационной среды, обеспечивается комплексом социальных норм, регулирующих поведение коллективных (юридических) и индивидуальных (физических) субъектов управления. Такими регуляторами являются нормы права, которые обеспечивают относительную стабильность системы и ее развитие. Особая роль при этом принадлежит сфере государственного управления, одной из главных задач которой является обеспечение действий субъектов в соответствии с нормами права.

Информационное законодательство – это совокупность норм права, регулирующих общественные отношения в информационной сфере.

Предметом правового регулирования в информационной сфере являются:

– создание и распространение информации;

– формирование информационных ресурсов;

– реализация права на поиск, получение, передачу и потребление информации;

– создание и применение информационных систем и технологий;

– создание и применение средств информационной безопасности.

В основе информационного законодательства находится свобода информации и запретительный принцип права

В настоящее время в стране действуют следующие нормативные акты, регулирующие отношения в информационной сфере: Конституция РФ;

Федеральные законы; Гражданский кодекс РФ; Уголовный кодекс РФ; Кодекс РФ об административных правонарушениях; Закон «Об информации, информатизации и защите информации» и др.; Указы и Распоряжения Президента РФ; Постановления Правительства РФ; другие подзаконные акты: местные, ведомственные и внутриорганизационные.

Совокупность вышеперечисленных документов составляет правовую базу, обеспечивающую нормативное регулирование процессов информационного обмена, в том числе и защиту информации.

Необходимо отметить, что информационное законодательство в настоящее время в нашей стране находится еще в стадии формирования, а, следовательно, нашим законодателям предстоит еще большая работа по устранению имеющихся пробелов и недостатков.

Студенту следует понимать, что защите подлежит не вся информация, а только та, которая представляет ценность для предпринимателя, при определении которой необходимо руководствоваться ее свойствами.

Угрозы информационной безопасности – потенциальные или реально возможные действия по отношению к информационной сфере, приводящие к несанкционированным изменениям свойств информации (конфиденциальность, доступность, достоверность, целостность).

Источники информационных угроз делятся по территориальному признаку и по признаку принадлежности к объекту информационной защиты на внутренние и внешние, причем соотношение внешних и внутренних угроз на усредненном уровне можно охарактеризовать как 1 к 4.

Студент должен помнить, что информационные угрозы имеют векторный характер, т.е. всегда преследуют определенные цели и направлены на конкретные объекты.

К наиболее важным объектам обеспечения информационной безопасности относятся:

– информационные ресурсы, содержащие специальные сведения и оперативные данные служебного характера;

– информационно-вычислительные центры, их информационное, техническое, программное и нормативное обеспечение;

– информационная инфраструктура (информационно-вычислительные сети, пункты управления, узлы и линии связи).

Выделяют следующие виды угроз информационной безопасности:

– информационные – нарушения регламента информационного обмена; незаконные сбор и использование информации; несанкционированный доступ к информационным ресурсам; манипулирование информацией (дезинформация, сокрытие или искажение информации); незаконное копирование данных в информационных системах; хищение информации из баз и банков данных;

– программно-математическое – внедрение программ-вирусов, аппаратных и программных закладок; уничтожение или модификация данных в информационных системах.

– радиоэлектронные – перехват информации в сетях передачи данных и линиях связи; воздействие на парольно-ключевые системы; радиоэлектронное подавление линий связи и систем управления;

– физические – разрушение средств обработки информации и связи, а также машинных носителей информации; хищение аппаратных или программных парольных ключей; воздействие на персонал с целью реализации физических, программно-математических или информационных угроз; хищение носителей.

Угрозы информации по их конечному проявлению можно также классифицировать как:

– ознакомление – может проходить различными путями и способами, при этом существенным, является отсутствие изменений самой информации;

– модификация – направлена на изменение таких свойств как конфиденциальность, достоверность, целостность, при этом подразумевается изменение состава и содержания сведений. Модификация информации не подразумевает ее полное уничтожение;

– уничтожение – направлено, как правило, на целостность информации и приводит к ее полному разрушению;

– блокирование – приводит к потере доступа к ней, т.е. она по-прежнему существует, но воспользоваться ею нельзя.

С учетом сложившейся практики обеспечения информационной безопасности выделяют следующие направления защиты информации:

1 Правовая защита – специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе.

2 Организационная защита – регламентация деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и проявление внутренних и внешних угроз.

3 Инженерно-техническая защита – совокупность специальных органов, технических средств и мероприятий по их использованию в интересах защиты конфиденциальной информации.

Студент должен знать, что предприятие для обеспечения информационной безопасности может использовать систему мер, направленных:

– на предупреждение угроз – превентивные меры по обеспечению информационной безопасности в интересах упреждения возможности их возникновения;

– на выявление угроз – выражается в систематическом анализе и контроле возможности появления реальных или потенциальных угроз и своевременных мерах по их предупреждению;

– на обнаружение угроз – определение реальных угроз и конкретных преступных действий;

– на локализацию преступных действий и принятие мер по ликвидации угрозы или конкретных преступных действий;

– на ликвидацию последствий угроз и преступных действий.

Вопросы для дискуссионного обсуждения

1 Что такое информационная безопасность?

2 Факторы, влияющие на состояние информационной безопасности.

3 Охарактеризуйте объекты информационной безопасности.

4 Что такое «информационное оружие»?

5 Назовите отличительные свойства информационного оружия.

6 Охарактеризуйте источники информационных угроз.

7 Какие требования предъявляются к защите информации?

8 Какие виды угроз можете назвать?

9 Какие методы противодействия угрозам может использовать предприятие?

10 Законодательная база в области информационной безопасности.

11 Правовое обеспечение защиты государственной и коммерческой тайны.

Задания для индивидуальной работы

1 Проанализируйте основные положения и противоречия Доктрины информационной безопасности РФ.

2 Дайте характеристику правовому обеспечению защиты информации в Российской Федерации. Сравните его с зарубежной практикой.

3 Информационное обеспечение аналитической деятельности

План занятия

1 Сведения, составляющие коммерческую тайну.

2 Цели и задачи конкурентной разведки.

3 Цикл конкурентной разведки.

4 Контрразведка.

К коммерческой тайне относят преднамеренно скрываемые по коммерческим соображениям экономические интересы и сведения о различных сторонах и сферах производственно-хозяйственной, управленческой, финансовой деятельности фирмы, охрана которых обусловлена интересами и возможными угрозами экономической безопасности. Перечень сведений, составляющих коммерческую тайну, утверждается приказом директора.

Студенту следует знать следующие принципы:

– при засекречивании информации надо исходить из экономической выгоды и безопасности фирмы. Важно, что бы соблюдался принцип «золотой

середины». Чрезмерное засекречивание деятельности фирмы может обернуться потерей прибылей, так как условия рынка требуют широкой рекламы производимой продукции и услуг. Пренебрежительное отношение к коммерческой тайне также ведет к большим потерям;

– информация типа «ноу-хау», безусловно, должна быть отнесена коммерческой тайне, причем ее надо охранять и от собственного персонала (сотрудник может уволится и устроится на работу в конкурирующую форму);

– к коммерческой тайне необходимо отнести информацию о рационализаторском предложении или изобретении, находящемся на стадии разработки;

– особое внимание следует уделить охране договоров, заключаемых предприятием. Причем в определенных случаях охране подлежит не только текст договора, но и сам факт его заключения. Руководитель фирмы должен установить строгий порядок хранения договорных документов и работы с ними. При подписании договора рекомендуется, чтобы представители сторон ставили подписи не только в конце договора, но и каждом листе во избежание замены одного текста другим.

Студенту следует знать, что к коммерческой тайне относят следующие три группы сведений:

1 Деловая информация:

– финансовые сведения;

– данные о цене (стоимости) продукции и услуг, технологии;

– деловые планы и планы производства новой продукции;

– списки клиентов и продавцов, контракты, преференции (льготные пошлины ввоза) и планы;

– информация о маркетинге;

– соглашения, предложения, квоты;

– списки персонала, организационные схемы и информация о сотрудниках (их характеристики).

2 Техническая информация:

– научно-исследовательские проекты;

– конструкторские разработки по производству какой-либо продукции и ее технические параметры;

– заявки на патенты;

– дизайн, эффективность и возможности производственных методов, оборудования и систем;

– информационный процесс;

– программное обеспечение ЭВМ.

3 Информация о клиентах и конкурентах

Студент должен понимать, что существует три основных направления сбора информации:

1) информация о рынке;

2) информация о производстве продукции;

3) информация об организационных особенностях и финансах.

Задача аналитических служб при этом заключается в определении ключевой информации, выявлении возможных каналов утечки, поиске путей ее защиты.

Главной особенностью рыночных условий является резкое возрастание потребности управляющих структур в объективной, достоверной и своевременной информации о реальном положении дел в той или иной отрасли, на предприятии или в регионе.

Информация, необходимая для выработки и реализации адекватных управленческих решений индикативного характера, рассредоточена по множеству информационных фондов и баз данных. В частности, она может быть получена из систем правоохранительных министерств и ведомств народнохозяйственного блока, региональных информационных фондов, информационных банков предприятий и организаций различных форм собственности, независимых аналитических центров, информационных агентств и т.д.

Для обеспечения конкурентных преимуществ и как следствие – успешного развития бизнеса, – в компаниях промышленно развитых стран на исходе XX века стали создавать специальные службы «конкурентной разведки». Основными функциями данных служб являются сбор разведывательных сведений о намерениях конкурентов, основных тенденциях развития бизнеса, возможных рисках для бизнеса, новых возможностях бизнеса и т.д., их анализ, подготовка выводов и прогнозов, и, как следствие, их учет при принятии стратегических управленческих решений.

Однако использование разведки в деятельности бизнеса началось отнюдь не в конце XX столетия. Датой появления первой документально подтвержденной конкурентной разведки принято считать конец XIV века. Тогда Дом Фуггеров в германском Аугсбурге впервые в мире стал использовать элементы конкурентной разведки организованно и на постоянной основе.

Конкурентная разведка в её сегодняшнем виде получила сильный импульс развития в середине 1980-х годов. Родоначальником конкурентной разведки современного периода считается компания Ксерокс, столкнувшаяся с конкуренцией со стороны японских производителей.

И если первые шаги конкурентной разведки были неразрывно связаны с промышленным шпионажем, который проводили либо государства, либо частные компании по поручению государства, то сегодняшнее развитие технологий – прежде всего, связи и компьютеров – сделало полноценную разведку технически и финансово доступной для крупных, средних и даже для малых компаний.

К началу 1990-х годов сформировались международные и национальные общества профессионалов конкурентной разведки, которые за счет выпуска периодических изданий, проведения конференций и тренингов позволили организовать обмен опытом между специалистами. Наиболее известны в мире такие общества как SCIP со штаб-квартирой в США и Competia со штаб-

квартирой в Канаде. В России существует российское общество профессионалов конкурентной разведки РОПКР.

Конкурентную разведку можно определить как проводимые на постоянной основе сбор информации и исследования, как рынка, так и всей деловой среды, с целью выявления реальных и потенциальных факторов, которые влияют или могут повлиять на способность фирмы успешно конкурировать на данном рынке. Студенту необходимо понимать, что это не просто информация, а, прежде всего, постоянный анализ и прогноз изменений на рынке, а также, что конкурентная разведка основана на факторе времени и привязана к нему.

В настоящее время правильно организованная конкурентная разведка не ограничивается изучением конкурентов, а проводит работу в отношении всей среды, в которой живёт предприятие. В частности, изучается политическая и законодательная обстановка, кадровые перемещения людей, чья деятельность может оказать влияние на компанию, эксперты, способные проконсультировать по тому или иному специальному вопросу, новые технологии, собственные клиенты и поставщики компании.

А.И. Доронин формулирует следующие цели разведывательной деятельности субъектов предпринимательского бизнеса:

– своевременное обеспечение руководства надежной и всесторонней информацией об окружающей предприятие среде; выявление факторов риска, которые могут затронуть экономические интересы предприятия и помешать его нормальному функционированию;

– организация максимально эффективной информационной работы, исключающей дублирование структурными подразделениями предприятия функций друг друга;

– выработка краткосрочных и долгосрочных прогнозов влияния окружающей среды на хозяйственную деятельность предприятия; разработка рекомендаций по локализации и нейтрализации активизирующихся факторов риска;

– усиление благоприятных и локализация неблагоприятных факторов влияния окружающей среды на хозяйственную деятельность предприятия (управление рисками).

Конкурентная разведка решает следующие задачи:

– информационное обеспечение процесса выработки управленческих решений на стратегическом и тактическом уровне;

– привлечение внимание лиц, принимающих решения, к угрозам, которые потенциально могут причинить ущерб бизнесу;

– выявление благоприятных для бизнеса возможностей;

– выявление попыток конкурентов получить доступ к закрытой информации компании;

– управление рисками с целью обеспечить эффективное реагирование компании на быстрые изменения окружающей среды;

–систематизация имеющихся информационных ресурсов и поиск новых.

В основе системы конкурентной разведки лежит так называемый цикл разведки, в результате которого «сырая информация» превращается в «аналитические материалы». Технологические стадии разведывательного цикла состоят из четырех основных этапов:

– постановка задачи – важнейшей задачей является проблема планирования операций по проведению работы, включая выявление необходимых первоисточников;

– сбор информации – на этом этапе производится сбор «сырой» информации, на основе которой будут готовится аналитические материалы, по оценкам аналитиков не менее 80-90 % используемой информации поступает из открытых источников;

– анализ информации – самый трудный этап в цикле разведки, даже если анализ базируется на логических выводах и абсолютно достоверных данных, аналитику нередко приходится предугадывать ситуацию и представлять обоснованные предположения относительно последствий тех или иных действий компании;

– представление аналитических материалов руководству – на этом этапе созданные аналитические документы передаются тем лицам, для кого они предназначены. При этом сведения должны «успевать за временем».

Практика показывает, что деятельность подразделения конкурентной разведки в соответствии с разведывательным циклом неизменно приводит к хорошему результату.

Разведка осуществляется пассивными (работа с вторичными источниками) и активными методами (работа с первоисточниками, наблюдение, промышленный шпионаж).

Как ответная мера против ведения разведки появилась контрразведка, которая предназначена для защиты и обеспечения безопасности субъекта предпринимательской деятельности, В качестве объектов контрразведки выступают различные факторы группы риска, оказывающие, в той или иной степени, негативное воздействие на субъект защиты, основными из которых являются противоправная деятельность конкурентов, криминальных структур, проявления фактов промышленного (коммерческого) шпионажа, мошенничества и иных действующих рисков.

Контрразведывательный цикл состоит из 5 этапов:

– определение требований защиты;

– оценка конкурентов;

– оценка собственной уязвимости;

– разработка контрмер;

– реализация контрмер.

По изучению темы студент должен четко понимать, что основная задача контрразведки – обеспечение безопасности, другими словами контрразведка – это, прежде всего оборона, а разведка – наступление.

Вопросы для дискуссионного обсуждения

1 Сведения, составляющие коммерческую тайну.

2 Какие принципы необходимо учитывать при защите информации?

3 Направления сбора информации о хозяйствующих субъектах.

4 Назовите основные источники информации в России и за рубежом.

5 В чем отличие конкурентной разведки и контрразведки?

6 Какими методами осуществляется разведывательная деятельность?

7 Охарактеризуйте цикл конкурентной разведки.

8 Какие новые технологии, используемые в конкурентной разведке, Вы можете назвать?

9 Какие задачи решает конкурентная разведка?

10 Расскажите историю становления и развития разведки и контрразведки.

11 Работа с материалами средств массовой информации и ресурсами Интернет

Задания для индивидуальной работы

1 Проведите сравнительный анализ компаний, оказывающих услуги по конкурентной разведке и контрразведке. Какие факторы на Ваш взгляд будут определяющими при выборе компании?

2 Проанализировать формы и методы конкурентной разведки в зарубежных странах и в России.

3 Разработайте этический кодекс конкурентной разведки, который отвечал бы требованиям российской действительности.

4 Основные положения экономической безопасности

План занятия

1 Понятие «экономическая безопасность», ее определение, категории, содержание.

2 Угрозы экономической безопасности.

3 Проблемы измерения, оценки и анализа экономической безопасности.

Экономическая безопасность предприятия складывается из нескольких функциональных составляющих, которые для каждого конкретного предприятия могут иметь различные приоритеты в зависимости от характера существующих угроз. Основным фактором, определяющим состояние экономической безопасности, является обладание предприятием устойчивыми конкурентными преимуществами. Эти преимущества должны соответствовать стратегическим целям предприятия.

Можно дать следующее определение экономической безопасности предприятия – это состояние наиболее эффективного использования ресурсов для предотвращения угроз и обеспечения стабильного функционирования предприятия, обеспечивающееся за счет эффективной (прибыльной)

деятельности, которая достигается путем прогнозирования и нейтрализации внутренних и внешних угроз.

Такое понятие позволяет показать, что предприятие находится под постоянным влиянием внутренних и внешних угроз и за счет их прогнозирования, нейтрализации, адаптации и уменьшения влияния осуществляет свою цель – устойчиво и эффективно работает в настоящем и будущем для достижения основной цели деятельности организации – получение максимальной прибыли.

Главными задачами экономической безопасности предприятия являются:

– стабильность деятельности (регулярность и полнота поставок, ритмичность и загруженность производства) и его прибыльность;

– безопасность персонала – уменьшение частоты и тяжести травм при организации производственного процесса, исключение опасных для жизни криминальных проявлений, сохранение здоровья людей при чрезвычайных ситуациях;

– сохранность материальных средств – снижение величины хищений и потерь по другим причинам непроизводственного характера;

– соблюдение санкционированности доступа к информации, содержащей коммерческую тайну.

Экономическая безопасность предприятия обеспечивается следующими методами:

– выявление угроз со стороны организованной преступности, конкурентов и недобросовестных партнеров;

– предупреждение агентурного и технического проникновения их на фирму;

– выявление подрывной деятельности со стороны отдельных сотрудников фирмы;

– защита коммерческой тайны;

– обеспечение физической и инженерно-технической защиты помещений и зданий фирмы, а также ее имущества;

– поддержание законности, взаимовыгодности, добросовестности сотрудничества, внутренних и внешних связей;

– отработка механизма ликвидации угроз;

– пресечение посягательств на законные интересы фирмы юридическим, экономическим, организационным и другими путями.

Студенту следует обратить внимание, что экономическая безопасность характеризуется совокупностью качественных и количественных показателей, важнейшим среди которых является уровень экономической безопасности.

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

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

Выделяют следующие функциональные составляющие:

– финансовую;
– интеллектуальную и кадровую;
– технико-технологическую;
– политико-правовую;
– экологическую;
– информационную;
– силовую.

Угрозу экономической безопасности целесообразно определить как совокупность условий и факторов, препятствующих реализации экономических интересов хозяйствующего субъекта и создающих возможность нанесения ему ущерба, размер которого определяет степень снижения экономического потенциала хозяйствующего субъекта за определенный промежуток времени.

При оценке угроз экономической безопасности, их обычно классифицируют по источнику возникновения: внутренние и внешние.

Также угрозы можно классифицировать по степени тяжести последствий: с высокой, значительной, средней и низкой тяжестью последствий.

Высокая тяжесть означает, что эти угрозы могут привести к резкому ухудшению всех финансово-экономических показателей деятельности субъекта предпринимательства, что вызывает немедленное прекращение его деятельности либо наносят такой непоправимый вред, который приведет к этим же последствиям позднее. В этом случае происходит ликвидация фирмы.

Значительная степень тяжести последствий реализации угроз предполагает возможность нанесения фирме таких финансовых потерь, которые окажут негативное воздействие на основные финансово-экономические показатели фирмы, на ее деятельность в будущем и преодолеваются в течение длительных сроков времени.

Средняя степень тяжести означает, что преодоление последствий осуществления этих угроз требует затрат (наносит потери), сопоставимые с текущими затратами фирмы и не требует значительного времени.

Последствия реализации угроз с низкой степенью последствий не оказывают какого-либо существенного воздействия ни на стратегические позиции фирмы, ни даже на ее текущую деятельность.

По степени вероятности угрозы могут быть маловероятными и реальными.

Более подробная классификация угроз экономической безопасности представлена в Приложении А.

Понимая важность обеспечения экономической безопасности, возникает необходимость в ее оценке.

Студент должен знать, что источниками информации для анализа и оценки экономической безопасности могут быть: каталог факторов риска и рисковых ситуаций; личный опыт руководителей предприятия и специалистов; прогнозная информация; материалы ревизий, аудита, проверок налоговой службы, лабораторного и врачебно-санитарного контроля, печати, объяснительных и докладных записок, совещаний, переписки, получаемые в результате личных контактов; бухгалтерский учет и отчетность; статистические данные; сведения о конкурентах, партнерах, поставщиках и потребителях; материалы маркетинговых исследований о состоянии рынка; сведения правоохранительных органов о криминальной обстановке; экономическая, политическая, демографическая ситуации в стране и регионе; платежеспособность покупателей и т. п.

Система оценки и анализа экономической безопасности включает в себя совокупность последовательных, взаимосвязанных между собой блоков, этапов деятельности, систематизированных и приспособленных (сориентированных) к этим задачам методик, методов, моделей, дающих возможность выявить, оценить и уменьшить воздействие хозяйственного риска до приемлемого уровня с минимальными затратами корпоративных ресурсов.

Неотъемлемым элементом исследования экономической безопасности предприятия является выбор ее критерия. Под критерием экономической безопасности предприятия понимаются признак или сумма признаков, на основании которых может быть сделан вывод о том, находится ли предприятие в экономической безопасности или нет. Такой критерий должен не просто констатировать наличие экономической безопасности предприятия, а и оценивать ее уровень. Если назначение критерия будет сводиться только к констатации экономической безопасности предприятия, то в этом случае неизбежна субъективность оценки. При этом количественную оценку уровня экономической безопасности желательно было бы получить с помощью тех показателей, которые используются в планировании, учете и анализе деятельности предприятия, что является предпосылкой практического использования этой оценки.

Для этого целесообразно исследовать показатели финансовой устойчивости, безубыточности и ликвидности предприятия.

В экономической литературе представлены следующие подходы к оценке уровня экономической безопасности предприятия:

– индикаторный подход, при котором уровень экономической безопасности определяется с помощью так называемых индикаторов (пороговые значения показателей, характеризующих деятельность предприятия в различных функциональных областях, соответствующие определенному уровню экономической безопасности);

– ресурсно-функциональный подход – оценка осуществляется на основе анализа состояния использования корпоративных ресурсов по специальным критериям, при этом в качестве корпоративных ресурсов рассматриваются

факторы бизнеса, используемые владельцами и менеджерами предприятия для выполнения целей бизнеса;

– подход, отражающий принципы и условия программно-целевого управления и развития, который основывается на интегрировании совокупности показателей, определяющих экономическую безопасность. При этом используется несколько уровней интеграции показателей и такие методы их анализа, как кластерный и многомерный анализ.

Также, в целях оценки состояния экономической безопасности предприятия целесообразно провести анализ и диагностику финансово – экономической деятельности, в основе которых всестороннее изучение технологического уровня производства, качества и конкурентоспособности выпускаемой продукции, обеспеченности материально – техническими, трудовыми и финансовыми ресурсами, факторов повышения экономической эффективности их использования.

Анализ финансово-экономического состояния предприятия отражает все стороны и характеристики производственно-экономической деятельности и финансово-экономические результаты этой деятельности, объединяет ретроспекцию (анализ предшествующего периода, исторические аспекты становления предприятия), диагноз (систематизированная характеристика реального состояния) и прогнозирование перспективного или возможного состояния.

Студент должен запомнить, что при оценке состояния экономической безопасности наряду с такими методами как экспертный, рейтинговый, факторный, статистический целесообразно более широко применить метод мониторинга состояния предприятия, который отличается постоянством, систематизацией, детальным текущим наблюдением за финансово-экономическим состоянием предприятия.

Вопросы для дискуссионного обсуждения

1 Что такое экономическая безопасность предприятия?

2 Чем отличается экономическая безопасность государства и предприятия?

3 Назовите основные цели и задачи экономической безопасности.

4 Что такое угрозы?

5 Почему возникают угрозы экономической безопасности?

6 Дайте характеристику принципы четырех ролей.

7 Что включает принцип шести уровней экономической безопасности?

8 Охарактеризуйте механизм реализации и защиты от угроз.

9 На основании каких критериев можно оценить состояние экономической безопасности?

10 Основные показатели экономической безопасности организации.

11 Методы, используемые при анализе показателей.

Задания для индивидуальной работы

1 Проведите сравнительную характеристику определений «экономической безопасности». Сформулируйте собственное определение.

2 Постройте классификацию угроз экономической безопасности.

3 Рассмотрите основные показатели, используемые при анализе финансово-хозяйственной деятельности. Какие выводы по ним можно сделать о состоянии экономической безопасности предприятия?

4 Сравните значения фактических индикаторов социально-экономического развития России с пороговыми значениями экономической безопасности. Сделайте вывод.

5 Обеспечение экономической безопасности хозяйствующих субъектов

План занятия

1 Понятие обеспечения экономической безопасности.

2 Система и служба экономической безопасности.

3 Механизм обеспечения экономической безопасности.

Обеспечение экономической безопасности важное, сложное направление в деятельности организации, без реализации которого невозможно ее функционирование и эффективное развитие.

Обеспечение экономической безопасности предприятия – это процесс реализации функциональных составляющих экономической безопасности с целью предотвращения возможных ущербов и достижения максимального уровня экономической безопасности в настоящее время и в будущем.

Способы обеспечения экономической безопасности предприятия – это набор мер и система организации их выполнения и контроля, которые позволяют достигать наиболее высоких значений уровня экономической безопасности предприятия.

Для эффективной деятельности предприятия необходимо спрогнозировать возможные угрозы экономической безопасности и принять своевременные меры для ослабления или нейтрализации их воздействия.

Для обеспечения своей экономической безопасности предприятие использует совокупность корпоративных ресурсов.

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

Среди них можно выделить:

а) ресурс капитала. Акционерный капитал предприятия в сочетании с заемными финансовыми ресурсами является кровеносной системой предприятия и позволяет приобретать и поддерживать остальные корпоративные ресурсы, изначально отсутствующие у создателей данного предприятия;

б) ресурс персонала. Менеджеры предприятия, штат инженерного персонала, производственных рабочих и служащих с их знаниями, опытом и навыками являются основным проводящим и связующим звеном, соединяющим воедино все факторы данного бизнеса, обеспечивающим проведение в жизнь идеологии бизнеса, а также достижение целей бизнеса;

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

г) ресурс техники и оборудования. На основе имеющихся финансовых, информационно-технологических и кадровых возможностей предприятие приобретает оборудование, необходимое (по мнению менеджеров предприятия) и доступное (исходя из имеющихся ресурсов);

д) ресурс прав. С развитием цивилизации, истощением природных ресурсов и повышением ценности для бизнеса нематериальных активов резко выросла роль данного ресурса. Этот ресурс включает в себя права на использование патентов, лицензии и квоты на использование природных ресурсов, а также экспортной квоты, права на пользование землей (причем в настоящее время крайне повысилась ценность городских территорий, предназначенных не для земледелия, а для административной застройки). Использование этого ресурса позволяет предприятию приобщиться к передовым технологическим разработкам, не проводя собственных дорогостоящих научных исследований, а также получить доступ к необщедоступным возможностям развития бизнеса.

Студент должен знать, что основной целью системы экономической безопасности является предотвращение ущерба интересам предприятия в результате хищения финансовых и материальных средств, уничтожения имущества и ценностей в результате чрезвычайных ситуаций, разглашения, утраты, искажения, уничтожения информации, а также опасного для жизни воздействия на персонал и членов их семей.

К задачам системы безопасности относятся:

– своевременное выявление угроз безопасности персонала и ресурсов;

– установление причин и условий, способствующих нанесению финансового и материального ущерба;

– отнесение информации к категориям ограниченного доступа, и других ресурсов к различным уровням уязвимости и подлежащих сохранению;

– создание структуры оперативного реагирования на угрозы безопасности и проявление негативных тенденций в функционировании предприятия;

– эффективное пресечение посягательств на ресурсы и угроз персоналу на основе экономических, правовых, организационных и инженерно-технических мер обеспечения безопасности;

– создание условий для максимально возможного возмещения и локализации ущерба, наносимого неправомерными действиями криминальных структур и конкурентов, ослабление негативного влияния последствий чрезвычайных ситуаций.

Система экономической безопасности не может обеспечить требуемый уровень безопасности без надлежащей подготовки персонала и соблюдения им всех установленных правил, направленных на обеспечение безопасности, а также без создания службы безопасности.

Эффективная система экономической безопасности должна быть:

– непрерывной – это требование проистекает из того, что не всегда есть возможность точно установить время начала действия той или иной угрозы;

– плановой – уже говорилось о том, что обеспечение безопасности не может быть одноразовой акцией;

– централизованной – в рамках определенного предприятия должна обеспечиваться функциональная самостоятельность процесса обеспечения безопасности;

– целенаправленной – защищается то, что должно защищаться в интересах конкретной цели, а не все подряд;

– универсальной – меры безопасности должны перекрывать пути угроз независимо от места их возможного воздействия.

Как и любая другая система, система экономической безопасности должна иметь определенные виды собственного обеспечения, которые позволили бы ей осуществлять свою целевую функцию.

При разработке оптимальной структуры системы безопасности необходимо четко знать задачи и цели организации, место и роль основных структурных подразделений, их взаимодействие между собой. Систему безопасности характеризует уровень развития производительных сил и производственных отношении, их интеграция с другими хозяйственными структурами.

Выявление системного характера экономической безопасности позволило предложить общую модель ее обеспечения (Приложение Б).

Согласно модели важное место в данной системе занимают субъекты экономической безопасности – структуры, занимающиеся непосредственно обеспечением экономической безопасности (сотрудники, подразделения, службы).

Студент должен знать, что действие системы экономической безопасности осуществляется с помощью механизма.

Механизм можно обозначить как систему, устройство, определяющее порядок какого-нибудь вида деятельности.

Как один из элементов системы он служит инструментом реализации практических действий по обеспечению экономической безопасности, которые

включают диагностику экономической безопасности объекта, выработку мер по повышению уровня безопасности, оценку их эффективности и осуществление избранных мер через реализацию политики на предприятии.

Механизм обеспечения экономической безопасности организации уникален для каждой организации, потому что зависит от структуры, деятельности организации, эффективности ее работы и множества других факторов. Кроме того он представляет собой обоснование последовательности реальных событий по обеспечению экономической безопасности.

Функционирование механизма осуществляется через практические действия, которые включают прежде всего, уточнение интересов предприятия, определение приоритетов в хозяйственной деятельности, прогнозирование возможных угроз, а затем разработку на базе этого основных направлений стратегии обеспечения экономической безопасности предприятия. При этом механизм экономической безопасности не должен тормозить развитие организации и должен быть направлен на достижение целей организации.

Действия механизма должно быть направлено на повышение самостоятельности и устойчивости организации, повышение ее независимости от поставщиков и покупателей. Все составные части механизма обеспечения экономической безопасности тесно связаны между собой, и для бесперебойного функционирования требуется их финансирование в полном объеме.

В Приложении В представлен алгоритм действия механизма обеспечения безопасности организации в общем виде.

Данный алгоритм экономической безопасности состоит из блоков, которые при четком выполнении возложенных на них задач обеспечивают экономическую безопасность организации.

На первоначальном этапе руководство организации определяет цели и задачи обеспечения экономической безопасности, в соответствии с которыми вырабатываются принципы обеспечения экономической безопасности, и формируется стратегия обеспечения экономической безопасности.

На следующем этапе механизма происходит постоянный мониторинг экономической безопасности, в результате которого прогнозируются и выявляются внутренние и внешние угрозы экономической безопасности. При этом, как правило, почти все внутренние угрозы экономической безопасности организации можно устранить своими силами, а внешние угрозы экономической безопасности, как отображено в данном алгоритме механизма, иногда требуют структурной перестройки организации и обращения за помощью к другим организационным структурам. Имеются в виду правоохранительные органы, органы государственной власти, которые должны на уровне вмененных им полномочий оказывать необходимую помощь организациям, защищая их от части внешних угроз.

Студент после изучения темы должен понять, что достижение целей обеспечения экономической безопасности возможно при эффективном построении системы экономической безопасности и ее постоянном совершенствовании, а это невозможно без поддержки государства.

Вопросы для дискуссионного обсуждения

1 Что подразумевает обеспечение экономической безопасности?

2 Охарактеризуйте основные способы обеспечения экономической безопасности.

3 Какие корпоративные ресурсы можно выделить?

4 Что такое система обеспечения экономической безопасности?

5 Какую систему можно назвать эффективной?

6 Опишите механизм обеспечения экономической безопасности.

7 Роль службы безопасности в механизме обеспечения экономической безопасности.

8 Общие принципы построения системы безопасности предприятий.

9 Деятельность службы безопасности в правовом и организационном аспекте.

10 Взаимодействие службы безопасности и подразделений предприятия.

Задания для индивидуальной работы

1 Разработайте механизм обеспечения экономической безопасности для анализируемого предприятия.

2 Предложите рекомендации по совершенствованию деятельности службы безопасности хозяйствующего субъекта.

6 Информационно-аналитическое обеспечение в системе экономической безопасности

План занятия

1 Общие требования к информационно-аналитической работе.

2 Организация информационно-аналитической деятельности.

3 Принципы информационно-аналитической работы.

Студенту следует понимать, что отдельно в системе обеспечения экономической безопасности можно выделить информационно-аналитическую составляющую, которая приобретает реальную ценность не за счет сбора данных, а благодаря осмыслению полученного материала.

При решении поставленных задач, аналитикам необходимо:

– изучить всю собранную информацию, дав ей оценку по достоверности и надежности;

– построить модель проблемы или ситуации и с учетом собранной информации предсказать ход событий;

– дать обоснованные рекомендации руководству о том, какие управляющие воздействия необходимо предпринять с учетом возможностей конкурента, своих ресурсов и временных ограничений.

Студент должен помнить, что аналитик практически никогда не располагает всей информацией, и ему приходиться восстанавливать картину событий по отдельным фрагментам, с помощью анализа. Анализ – это процесс обработки информации, часто фрагментарной, и превращения ее в разведывательные сведения. Поэтому роль анализа является определяющей в информационно-аналитической деятельности.

При проведении информационно-аналитической работы распространение получили два подхода:

1) аналитики «старой школы» – считают, что аналитики должны эмпирически описывать тенденции развития процессов, событий, основываясь на исторических аналогах, юридических прецедентах, реальных событиях, с привлечением данных из различных источников информации. Основной принцип – не допускать привнесения в отчетные документы собственных взглядов и суждений;

2) аналитики «новой школы» – в своей работе основываются на принципе глубокого всестороннего исследования фактов и событий, опираясь на научные методы обработки информации, анализа, прогнозирования, выработки доказательных оценок и выявления возможных альтернативных вариантов в изучаемых проблемах.

Общие подходы и некоторые требования к информационно-аналитической работе аналитиков «новой школы»:

1 Ориентация анализа на следующие альтернативные возможности:

– оценки тенденций должны показывать возможности проведения той или иной политики предприятия;

– давать рекомендации руководителю по применению наиболее целесообразных средств воздействия на конкурента или среду для достижения своих целей;

– фокусирование внимания на стратегических процессах.

2 Аналитиков не нужно делать участниками процесса принятия решений, им следует ставить четкие задания по выявлению возможностей и предсказанию вероятных результатов определенного курса действия, исходя из интересов предприятия.

3 Четкое понимание специфики конкурента и конкурентной среды.

4 Аналитики должны исходить из условий неполной информации и дезинформации со стороны конкурентов, а поэтому необходима система проверки поступающей информации.

5 Осознание предела своих знаний:

– четкое осознание пределов и ограниченности возможностей аналитических методов;

– информированность потребителей продукции относительно используемых моделей, теорий, методов.

Студенту следует помнить, что в условиях ограниченности возможностей получения информации, велика роль информационно-

аналитичесих методов. Они позволяют получить необходимые сведения при минимальных затратах.

Аналитическую информацию можно определить как осмысленные сведения, полученные из оцененных, истолкованных и соотнесенных фактов, изложенных таким образом, что ясно видно их значение для решения конкретной текущей задачи.

Основная аксиома информационно-аналитической работы – почти всегда можно найти факты, в какой-то степени относящиеся к исследуемому вопросу. Работа включает в себя 3 самостоятельных аспекта:

1) изучение существующего положения дел;

2) изучение возможностей объекта анализа;

3) изучение намерений.

По результатам проведенного анализа составляются следующие информационные документы: прогноз, аналитическая оценка и отчет, информационная справка, обзор, отчет и т.д.

Можно выделить следующие принципы организации информационно-аналитической работы:

– постановка цели;

– определение понятий;

– использование всех возможных источников;

– раскрытие значений фактов или повышение их полезности;

– установление причинно-следственных связей;

– определение тенденций развития;

– определение степени достоверности полученных данных;

– формирование выводов.

Таким образом, можно сделать вывод, что в понятие информационно аналитической работы включается весь процесс создания аналитической информации, состоящий из нескольких этапов: организации сбора и первичной обработки материалов, собственно анализ и избирательного распространения информации.

Студент после изучения темы должен понять, что в информационно-аналитической работе главное, не допускать произвольных выводов и указывать временной интервал полезности информации.

Вопросы для дискуссионного обсуждения

1 Направления информационно-аналитической деятельности по обеспечению безопасности.

2 Сущность и содержание информационно-аналитической деятельности.

3 Организация и направления информационно-аналитической работы.

4 Формы информационных документов.

5 Какие требования предъявляют к аналитической работе?

6 В чем основное отличие принципов деятельности аналитиков «старой» и «новой» школ?

7 На что следует обращать внимание при составлении информационно-аналитических документов?

8 Какие методы анализа применяются в информационно-аналитической работе?

9 Представление результатов заказчику: основные принципы и требования.

Задания для индивидуальной работы

1 Определите каким требования должен отвечать хороший аналитик. Как осуществляется подбор специалистов для информационно-аналитической работы?

2 Проанализируйте правовую основу и регламентацию информационно-аналитической деятельности.

7 Использование специализированных программных продуктов и аналитических систем для диагностики, оценки и мониторинга финансового состояния предприятия

План занятия

1 Необходимость использования специализированных программных продуктов.

2 Программа Project Expert: назначение и задачи; основные функциональные особенности.

3 Компьютерная программа Audit Expert: основные функции, обмен данными, инструменты.

Начиная с середины 90-х годов предприятия разной отраслевой принадлежности, банки, страховые компании и государственные органы проявляют значительный интерес к применению программ финансового анализа. В настоящий момент на рынке представлено немало разработок подобного рода, однако выбрать наиболее подходящий программный продукт достаточно сложно. Дело в том, что, выбирая конкретный продукт, потенциальному пользователю требуется сопоставлять множество далеко не равнозначных характеристик этих программ и предоставляемых ими возможностей. Поэтому создание и использование формализованных методик сопоставления различных программ финансового анализа, позволяющих уменьшить субъективный фактор в оценке их возможностей применительно к потребностям конкретных групп пользователей, представляет сегодня особый интерес.

В настоящее время программные системы независимо от их назначения развиваются по общим правилам: расширяется их функциональность, совершенствуются средства пользовательского интерфейса, повышается гибкость настройки в целях обеспечения соответствия требованиям конкретных

групп пользователей, развиваются механизмы взаимодействия с системами автоматизации, применяемыми в смежных и иных сферах деятельности. Не являются исключением и системы автоматизации финансового анализа.

Студенту следует учитывать, что рыночная судьба любого тиражируемого программного продукта зависит от числа категорий его пользователей, а также от того, насколько полно с его помощью решаются их задачи. Целевая аудитория программ финансового анализа – предприятия, крупные корпоративные структуры, банки, аудиторские компании и государственные органы. Цели анализа у них различаются, и каждая группа пользователей применяет разные методики анализа. Это побуждает разработчиков таких продуктов делать их более универсальными, в частности расширять их методическое наполнение.

Пользователями программных продуктов, разработанных в России, часто являются предприятия и организации других стран – участниц СНГ. Если говорить о российских программах финансового анализа, то их применение пользователями в этих странах может сдерживаться тем, что каждая страна имеет свои особенности ведения бухгалтерий и формы бухгалтерской отчетности. Следовательно, отличается и входная, информация, используемая для анализа.

Рассмотрим наиболее популярные программы Project Expert и Audit Expert подробнее.

Project Expert – это система стратегического планирования и управления – инструмент, позволяющий руководству предприятий, специалистам, привлекающим финансовые средства для предприятия, экспертам, занятым анализом инвестиционных проектов, менеджерам, управляющим группой проектов, и инвесторам, выбирающим направление вложения средств, успешно решать стоящие перед ними задачи. При этом от пользователя требуется только одно – хорошо знать свой бизнес.

Основные функции, заключаются в том, что программа позволяет пользователям, не имеющим специальной подготовки в области финансового анализа, в короткий срок решить следующие задачи:

– детально описать и спроектировать деятельность любого предприятия с учетом изменения параметров внешней среды (инфляция, налоги, курсы валют);

– разработать план развития предприятия или реализации инвестиционного проекта, стратегию маркетинга и стратегию производства, обеспечивающую рациональное использование материальных, людских и финансовых ресурсов;

– определить схему финансирования предприятия;

– апробировать различные сценарии развития предприятия, варьируя значения факторов, способных повлиять на его финансовые результаты;

– подготовить финансовые отчеты (отчет о движении денежных средств, Баланс, отчет о прибылях и убытках, отчет об использовании прибыли) и

бизнес-план инвестиционного проекта, полностью соответствующие международным требованиям, на русском и английском языках;

– провести всесторонний анализ предприятия (проекта), в том числе анализ общей эффективности, анализ чувствительности, анализ денежных потоков для каждого участника проекта, анализ финансового состояния и доходности предприятия с помощью трех десятков автоматически исчисляемых показателей.

Помимо стандартных таблиц, Project Expert позволяет конструировать любые пользовательские таблицы и графики, при этом шаблон пользовательских таблиц и графиков может быть сохранен для использования в других проектах. Генератор отчетов программы обладает развитыми средствами редактирования отчетных форм (шрифты, выделения, вставка текста из других файлов) и позволяет распечатывать их напрямую из программы или передавать в Microsoft Word .

Audit Expert является эффективным инструментом комплексного анализа финансового состояния и результатов деятельности предприятия.

Приведение финансовой отчетности к международному стандарту позволяет данной программе преобразовать данные финансовой отчетности предприятий за разные годы (Баланс и отчет о финансовых результатах) в аналитические таблицы, соответствующие требованиям Международных стандартов бухгалтерского учета. Такой подход делает результаты анализа понятными как для российских, так и для иностранных экспертов. Отчеты формируются как на русском, так и на английском языке.

Благодаря имеющимся в программе утилитам, пользователь может легко расширить эти возможности.

Стандартизированные аналитические таблицы, полученные при помощи данной программы, позволяют провести детальный анализ предыдущей деятельности и текущего состояния предприятия:

– рассчитать наиболее применяемые показатели ликвидности, устойчивости, рентабельности и деловой активности предприятия;

– оценить структуру баланса по методике Федерального управления по делам о несостоятельности (банкротстве) предприятий;

– проанализировать динамику изменения структуры баланса с различным шагом, как в абсолютных величинах, так и в процентах.

В общей сложности более 70 рассчитываемых параметров помогут оценить все стороны финансового состояния предприятия. Этот список может быть легко дополнен неограниченным количеством финансовых показателей и таблиц, создаваемых пользователем.

Данная программа – единственная система, которая может не только анализировать представленную бухгалтерскую отчетность, но и провести предварительную переоценку баланса по данным детального описания структуры активов и пассивов компании. Это значительно повышает достоверность результатов, а в некоторых случаях вообще является единственным приемлемым подходом к анализу финансовых отчетов.

Ввод данных в программу Audit Expert осуществляется как в ручном (заполнение исходных таблиц), так и в автоматических режимах. Автоматический режим обмена подразумевает прямой импорт данных текстового формата из других систем.

По любым данным, представленным в таблицах Audit Expert , можно тут же построить графики или диаграммы. Наборы графиков могут сохраняться в шаблонах представления результатов и использоваться для дальнейшего анализа.

Audit Expert обладает развитыми средствами подготовки и редактирования отчетных форм. Уникальный генератор отчетов позволяет выводить подготовленный отчет на печать или сохранять как документ MS Word. В ближайшее время появится также и возможность создания HTML – документов.

По результатам изучения темы, студент должен знать, что наряду с использованием общераспространенных средств MS Office для расчета показателей экономической безопасности, широко применяются специализированнъые программные продукты, позволяющие получить наиболее полный и достоверный анализ.

Вопросы для дискуссионного обсуждения

1 Какие специализированные программные продукты и аналитические системы для диагностики, оценки и мониторинга финансового состояния предприятия используются в российской практике?

2 Задачи, которые позволяет решить программа Project Expert.

3 Опишите интерфейс программы Project Expert.

4 Задачи, которые позволяет решить программа Audit Expert.

5 Опишите интерфейс программы Audit Expert.

6 Основные этапы работы в среде Audit Expert.

7 Преимущества и недостатки использования специализированных программных продуктов.

Задания для индивидуальной работы

1 Рассмотрите какие программные продукты используют предприятия для анализа финансово-хозяйственной деятельности.

2 Проведите сравнительный анализ основных существующих специализированных программных продуктов и аналитических систем для диагностики, оценки и мониторинга финансового состояния предприятия. Выявите недостатки и преимущества каждой программы. Результат оформите в виде таблицы.

8 Литература, рекомендуемая для изучения дисциплины

8.1 Основная литература

8.1.1 **Сенчагов, В.К.** Экономическая безопасность России: Общий курс: учебник / под ред. В.К. Сенчагова. – 2-е изд. – М. : Дело, 2005. – 896 с. – ISBN 5-7749-0391-5.

8.1.2 **Олейников, Е.А.** Экономическая и национальная безопасность: учебник / под ред. Е.А. Олейникова. – М. : Издательство «Экзамен», 2004. – 768 с. – ISBN 5-94692-783-3.

8.1.3 **Гапоненко, В.Ф.** Экономическая безопасность предприятий. Подходы и принципы / В.Ф. Гапоненко, А.А. Беспальо, А.С. Власков. – М. : Издательство «Ось-89», 2007. – 208 с. – ISBN 978-5-98534-670-1.

8.1.4 **Баяндин, Н.И.** Технологии безопасности бизнеса: введение в конкурентную разведку: учебно-практич. пособие / Н.И. Баяндин. – М. : Юристъ, 2002. – 320 с. – ISBN 5-7975-0482-0.

8.2 Дополнительная литература

8.2.1 **Завгородний, В.И.** Комплексная защита информации в компьютерных системах: учеб. пособие для вузов / В.И. Завгородний. – М. : Логос, 2001. – 264 с. : ил. – (Учеб. 21 в.). – Библиогр. : с. 260-263. – ISBN 5-94010-088-0.

8.2.2 **Гаценко, О.Ю.** Защита информации: Основы организационного управления / О.Ю. Гаценко. – СПб. : Изд. дом «Сентябрь», 2001. – 228 с. – ISBN 5-94234-015-3.

8.2.3 **Боган, К.** Бизнес-разведка. Внедрение передовых технологий = Benchmarking for Best Practices / К. Боган, М. Инглиш: пер. с англ. – М. ; СПб. : Вершина, 2006. – 368 с. – ISBN 5-9626-0122-X.

8.2.4 **Корнеев, И.К.** Защита информации в офисе: учебник / И.К. Корнеев, Е.А. Степанов. – М. : Проспект, 2008. – 336 с. – ISBN 978-5-482-01976-4.

8.2.5 **Меньшаков, Ю.К.** Защита объектов и информации от технических средств разведки : учеб. пособие / Ю.К. Меньшаков. – М. : Рос. гос. гуманитарный ун-т, 2002. – 399 с. – ISBN 5-7281-0487-8.

8.2.6 **Малюк, А.А.** Информационная безопасность: концептуальные и методологические основы защиты информации: учеб. пособие для вузов / А.А. Малюк. – М. : Горячая линия – Телеком, 2004. – 280 с. – ISBN 5-93517-197-X.

8.2.7 **Одинцов, А.А.** Экономическая и информационная безопасность предпринимательства: учеб. пособие для вузов / А.А. Одинцов. – М. : Академия, 2006. – 336 с. – ISBN 5-7695-2283-6.

8.2.8 **Садердинов, А.А.** Информационная безопасность предприятия: учеб. пособие для вузов / А.А. Садердинов, В.А. Трайнев, А.А. Федулов. – 2-е изд. – М. : Дашков и К, 2005. – 336 с. – ISBN 5-94798-558-6.

9 Вопросы для зачета

1 Цели и задачи дисциплины ИАОЭБ.
2 Понятие информационной безопасности.
3 Объекты информационной безопасности.
4 Информация, информационные ресурсы и информатизация.
5 Факторы, влияющие на состояние информационной безопасности РФ.
6 Деструктивные факторы для экономической безопасности: вызовы, опасности, угрозы.
7 Отличительные свойства информационного оружия.
8 Виды информационного оружия.
9 Виды и источники угроз информационной безопасности.
10 Способы воздействия угроз на объекты информационной безопасности.
11 Методы противодействия угрозам информационной безопасности.
12 Проведение единой политики в области защиты информации.
13 Основные положения доктрины информационной безопасности РФ.
14 Противоречия доктрины информационной безопасности РФ.
15 Принципы обеспечения безопасности информационных систем.
16 Базовые принципы управления системы информационной безопасности организации.
17 Требования к информационной безопасности организации.
18 Риски нарушения политики информационной безопасности организации.
19 Основные источники открытой информации в сфере экономической безопасности в России и за рубежом.
20 Безопасность автоматизированных систем обработки информации. Факторы, влияющие на безопасность предпринимательской деятельности в России.
21 Информационные события, процессы и информационная деятельность.
22 Виды информации в предпринимательской деятельности.
23 Понятие риска. Идентификация рисков.
24 Оценка рисков.
25 Управление рисками.
26 Основные показатели экономической безопасности организации.
27 Цели, задачи и цикл конкурентной разведки.
28 Конкурентная контрразведка.
29 Правовое обеспечение защиты информации в Российской Федерации.
30 Механизм обеспечения экономической безопасности.
31 Система и служба экономической безопасности.
32 Организация и принципы информационно-аналитической деятельности.
33 Назначение и задачи программы Audit Expert.

34 Компоненты системы Audit Expert.

35 Ограничения по применению коэффициентов финансового состояния предприятия.

36 Назначение и задачи программы Project Expert.

37 Компоненты системы Project Expert.

38 Необходимость использования специализированных программных продуктов.

Приложение А
(обязательное)
Классификация угроз экономической безопасности

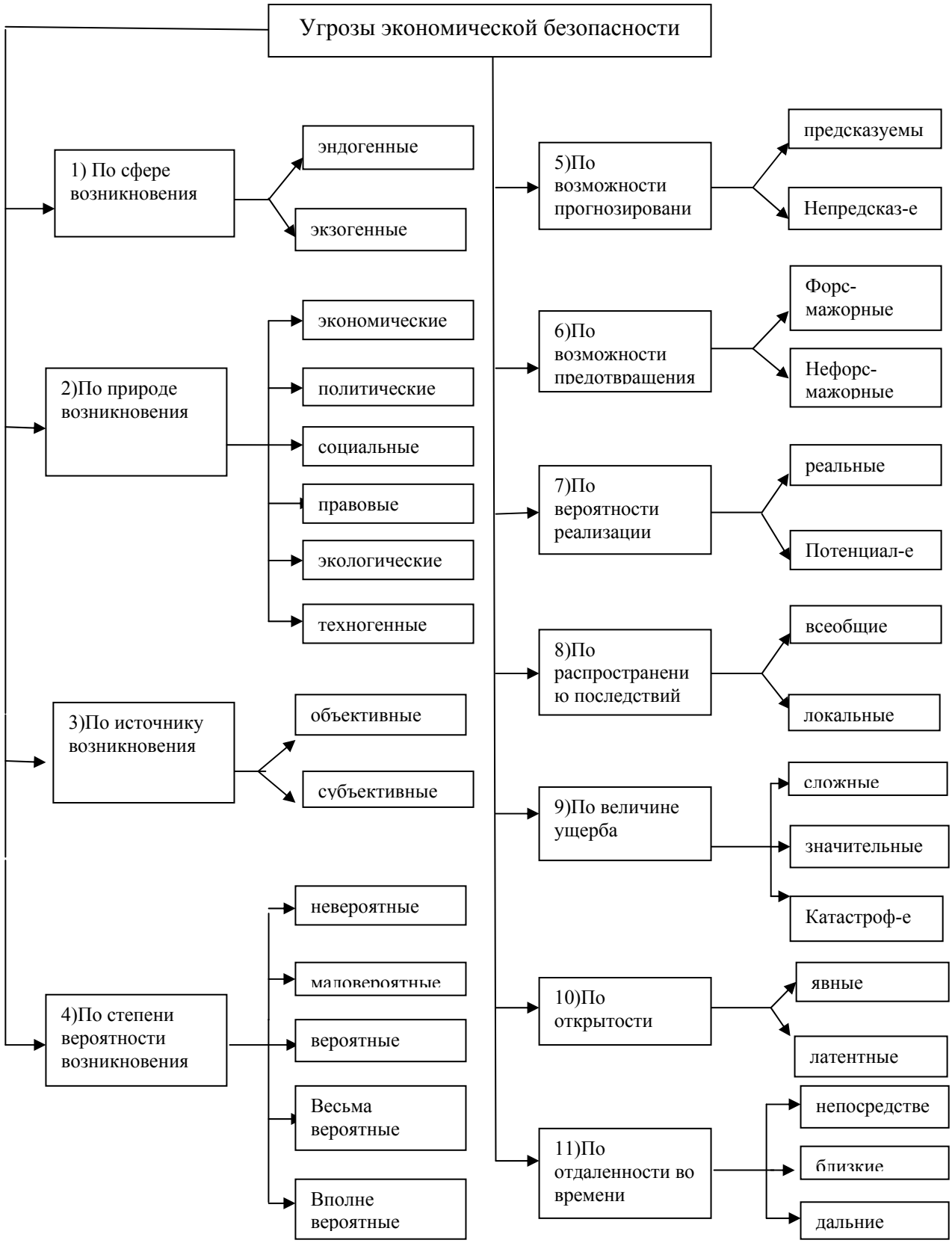

Рисунок А.1 – Классификация угроз экономической безопасности

Приложение Б
(справочное)
Модель системы обеспечения экономической безопасности

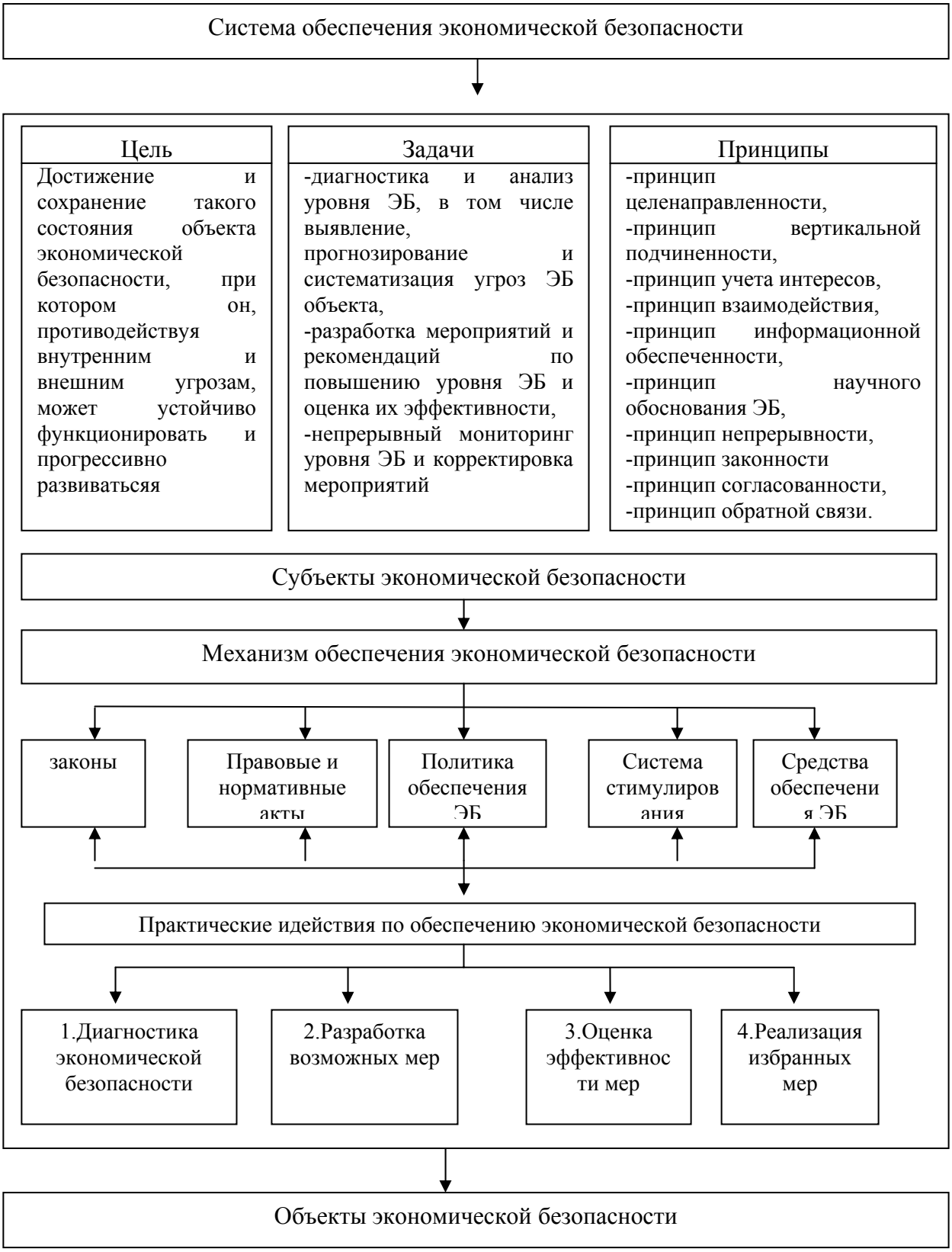

Рисунок Б.1 – Модель системы обеспечения экономической безопасности

Приложение В
(справочное)
Механизм обеспечения экономической безопасности

Рисунок В.1 – Механизм обеспечения безопасности организации

Приложение Г
(справочное)
Мониторинг экономической безопасности

Рисунок Г.1 – Мониторинг экономической безопасности организации

Приложение Д
(справочное)
Индикаторы экономической безопасности

Таблица Д.1 – Показатели индикаторов производства, финансовых индикаторов, социальных индикаторов

Индикаторы производства (характеризуют тенденции развития производства организации и эффективность использования ресурсов и производственного потенциала)	– динамика производства (рост, спад, стабильное состояние, темп изменения)
	– реальный уровень загрузки производственных мощностей
	– темп обновления основных производственных фондов (реновации)
	– стабильность производственного процесса (ритмичность, уровень загруженности в течение определенного времени)
	– удельный вес производства в ВВП (для особо крупных предприятий - монополистов)
	– оценка конкурентоспособности выпускаемой продукции
Финансовые индикаторы (характеризуют тенденции развития экономики организации)	– объем «портфеля» заказов (общий объем предполагаемых продаж)
	– фактический и необходимый объем инвестиции (для поддержания и развития имеющегося потенциала)
	– уровень инновационной активности (объем инвестиций в нововведения)
	– уровень рентабельности производства
	– фондоотдача (капиталоемкость) производства
	– просроченная задолженность (дебиторская и кредиторская)
	– доля обеспеченности собственными источниками финансирования оборотных средств
Социальные индикаторы (отражают уровень социального развития организации)	– уровень оплаты труда по отношению к среднему показателю в отрасли
	– уровень задолженности по зарплате
	– потери рабочего времени
	– структура кадрового потенциала (возрастная, квалификацинная)