

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ**

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

**(ДГТУ)**

УТВЕРЖДЕНО

на заседании кафедры

Экономической безопасности, учёта и права

«\_\_» \_\_\_\_\_\_\_\_ 2025 г.

**Золотарева И.В.**

### МЕТОДИЧЕСКИЕ УКАЗАНИЯ

для самостоятельной работы студентов по дисциплине

**«Основы информационной безопасности»**

для направления *38.05.01 «Экономическая безопасность»*

специализация «Экономико-правовое обеспечение экономической безопасности»

Ростов-на-Дону

2025

**Золотарева И.В.** Методические указания для самостоятельной работы студентов по дисциплине «Основы информационной безопасности». – Ростов-на-Дону: Донской государственный технический университет, 2025. – 17с.

В методических указаниях излагается содержание практической работы студентов по дисциплине «Основы информационной безопасности». Разработаны исходя из утвержденной программы курса. Рассчитаны на специалистов, обучающихся по направлению *38.05.01 «Экономическая безопасность»* специализация «Экономико-правовое обеспечение экономической безопасности».

Составитель: **Золотарева И.В.,**

к.э.н., доцент кафедры Экономической безопасности, учета и права ДГТУ

Рецензент: **Крохичева Г.Е.,**

д.э.н., профессор, зав. кафедрой Экономической безопасности, учета и права ДГТУ

© Донской государственный

технический университет, 2020

**МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ИЗУЧЕНИЮ ДИСЦИПЛИНЫ**

**«Основы информационной безопасности»**

**ОБЩИЕ МЕТОДИЧЕСКИЕ УКАЗАНИЯ к самостоятельной работе студента**

Самостоятельная работа студента является одной из важнейших составляющих учебного процесса, в ходе которой происходит формирование навыков, умений и знаний, и в дальнейшем обеспечивается усвоение студентом приемов познавательной деятельности, интерес к творческой и научной работе. При этом наибольший эффект достигается тогда, когда имеет место систематичность и равномерная интенсивность работы студента в течение семестра. Цель самостоятельной работы заключается в изучении теории комплексного экономического анализа хозяйственной деятельности и умении применять полученные знания на практике.

Организация самостоятельной работы студентов под руководством преподавателя является одним из наиболее эффективных направлений в учебном процессе, развивающим самостоятельную творческую деятельность, стимулирующую приобретение и закрепление знаний. При этом наиболее актуальной проблемой является поиск путей активизации самостоятельной познавательной деятельности как условия непрерывности и эффективности образования.

Для самостоятельной работы студентам предлагаются такие формы, как работа с первоисточниками, учебниками, сборниками задач, тестов и ситуаций разработка моделей занятий, анализ дополнительной литературы и др.

Чтобы стимулировать и постоянно поддерживать у студентов интерес к получению новых знаний, нужно больше внимания обращать на обучение их системе самообразования. Студенты должны овладеть основными элементами труда преподавателя: работать с научной, методической и учебной литературой; излагать учебный материал, составлять систему дифференцированных упражнений и управлять ею в процессе решения задачи; использовать приемы постановки вопроса, формулировать организующие и управляющие вопросы, а также варианты одного и того же вопроса; быстро и адекватно реагировать на возникшую учебную ситуацию; уметь контролировать и оценивать знания и др.

Методические указания подготовлены в соответствии с программой в целях самостоятельного изучения и закрепления теоретического материала и получения практических навыков по введению в профессиональную деятельность, а также эффективного самоконтроля за ходом изучения отдельных тем курса и непосредствен­ной подготовки к зачету.

Основой изучения дисциплины является самостоятельная работа студента над рекомендуемым учебным материалом по темам, приведенным в УМКД.

**Структура выполнения самостоятельной работы включает в себя:**

**1.** **Усвоение текущего учебного материала**

В процессе лекции студент ведет конспектирование излагаемого преподавателем материала с выделением основных понятий, фактов, формул, правил и т.д. Конспект лекций следует вести аккуратно, выделяя разделы, подразделы, отдельные темы. При последующей самостоятельной внеаудиторной работе студенту необходимо отметить непонятные выражения и положения, закончить (вставить) слова, пропущенные (упущенные) при конспектировании с использованием рекомендуемой к лекции литературы.

Усвоение текущего учебного материалапредусматривает:

- повторение ранее изученного материала;

- изучение текущих тем лекций с использованием основной и дополнительной литературы из рабочей программы;

- выявление наиболее трудного для понимания материала;

- подготовку вопросов по материалу лекции.

В течение семестра преподавателем проводятся консультации по утвержденному графику (но не менее 1 часа в неделю). В период сессии проводятся индивидуальные и групповые консультации, в том числе перед зачетом.

**2. Самостоятельное изучение дополнительных разделов дисциплины**

В процессе изучения дисциплины **«Основы информационной безопасности»** студентам необходимо обратить особое внимание на самостоятельное изучение дополнительных разделов дисциплины и тем лекций, вынесенных на самостоятельную проработку с использованием рекомендованной учебной (а также научной и популярной) литературы, для чего предусмотрена работа в библиотеке и в компьютерном классе по изучению материалов в Интернете.

Самостоятельная работа с учебными пособиями, научной и популярной литературой по материалам периодики и Интернета является наиболее эффективным методом получения знаний по предмету, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала.

При работе с литературой по конкретным темам курса основное внимание следует уделять важнейшим понятиям, терминам, определениям, для скорейшего усвоения которых целесообразно вести краткий конспект.

Самостоятельная работа студентов с литературой не отделена от лекций и семинаров, однако вдумчивое чтение источников, составление тезисов, обобщение прочитанных материалов способствует гораздо более глубокому пониманию изучаемой проблемы. Данная работа также предполагает обращение студентов к справочной литературе для уяснения конкретных терминов и понятий, введенных в курс, что способствует пониманию и закреплению пройденного лекционного материала, и подготовке к практическим (лабораторным) занятиям.

Самостоятельное изучение дополнительных разделов дисциплины должно выполняться, в том числе, на основе технических средств в классах ЭВМ при использовании соответствующих обучающих программ, а также стендов и макетов различных устройств, имеющихся на кафедре.

**3. Подготовку к практическим занятиям**

Подготовка к практическим (лабораторным) занятиям осуществляется на основании тематики, представленной в рабочей программе дисциплины, материалов, представленных в методических указаниях к практическим (лабораторным) занятиям, а также вопросов, предлагаемых для подготовки к занятию преподавателем при изучении предыдущей темы.

Студент перед лабораторной (практической) работой должен изучить основные вопросы, теоретический материал, необходимый для понимания сущности процессов, протекающих при ее выполнении.

**4. Подготовку к зачёту**

Подготовка к зачету представляет собой обобщение всего материала дисциплины на основании конспекта лекций и рекомендованных литературных источников и заключается во всестороннем рассмотрении всех тем с обязательным повторением материала практических занятий.

Вопросы, выносимые на зачет, в соответствии с рабочей программой дисциплины доводятся до студентов на последнем лекционном занятии в семестре.

**ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ**

Для преподавания дисциплины предусмотрены традиционные технологии в рамках аудиторных занятий и самостоятельной работы студентов, в частности: лекции, на которых излагается теоретическое содержание курса; практические занятия, предназначенные для закрепления теоретического курса и приобретения студентами практических навыков в области арбитражного процесса.

Лекции и практические занятия обеспечивают должный уровень теоретической и практической подготовки обучающихся специальности «Экономическая безопасность» в рамках дисциплины «Основы информационной безопасности».

При проведении занятий используются следующие технологии:

- методы проблемного и проектного обучения,

- компьютерные симуляции,

- деловые и ролевые игры,

- тренинги,

- исследовательские и кейс-методы и т.д.

Привлекаются для проведения открытых занятий ведущие специалисты по профилю ООП. Организуются выходы студентов на территорию предприятий-партнеров для ознакомления с практическими аспектами рассматриваемых в рамках изучаемого курса проблем.

**Методы проблемного и проектного обучения**

Технология проблемного обучения основывается на теоретических положениях американского философа, психолога и педагога Д. Дьюи. Сегодня под проблемным обучением понимается такая организация учебных занятий, которая предполагает создание под руководством педагога проблемных ситуаций и активную самостоятельную деятельность студентов по их разрешению, в результате чего и происходит творческое овладение профессиональными знаниями, навыками, умениями и развитие мыслительных способностей.

Целью проблемной технологии выступает приобретение ЗУН, усвоение способов самостоятельной деятельности, развитие познавательных и творческих способностей.

Проблемное обучение основано на создании особого вида мотивации – проблемной, поэтому требует адекватного конструирования дидактического содержания материала, который должен быть представлен как цепь проблемных ситуаций.

Проблемные методы – это методы, основанные на создании проблемных ситуаций, активной познавательной деятельности студентов, состоящей в поиске и решении сложных вопросов, требующих актуализации знаний, анализа, умения видеть за отдельными фактами явление, закон.

В современной теории проблемного обучения различают два вида проблемных ситуаций: психологическую и педагогическую. Первая касается деятельности учеников, вторая представляет организацию учебного процесса. Педагогическая проблемная ситуация создается с помощью активизирующих действий, вопросов педагога, подчеркивающих новизну, важность, красоту и другие отличительные качества объекта познания. Создание психологической проблемной ситуации сугубо индивидуально. Не слишком трудная, ни слишком легкая познавательная задача не создают проблемной ситуации для детей. Проблемные ситуации могут создаваться на всех этапах процесса обучения: при объяснении, закреплении, контроле.

Метод проектного обучения получил широкое распространение в России в 20-е и начале 30-х годов. Выделяют следующие отличительные черты проектного метода:

− участники проекта подхватывают проектную инициативу от кого-либо из жизни;

− участники проекта договариваются друг с другом о форме обучения;

− участники проекта развивают проектную инициативу и доводят ее до сведения всех;

− участники проекта организуют себя на дело;

− участники проекта информируют друг друга о ходе работы;

− участники проекта вступают в дискуссии и т.д.

Таким образом под проектным методом понимается система действий педагога и обучающихся по разработке проекта.

Цель проектного обучения состоит в том, чтобы создать условия, при которых студенты:

- самостоятельно и охотно приобретают недостающие знания из разных источников;

- учатся пользоваться приобретенными знаниями для решения познавательных и практических задач;

- приобретают коммуникативные умения, работая в различных группах;

- развивают у себя исследовательские умения (умения выявления проблем, сбора информации, наблюдения, проведения эксперимента, анализа, построения гипотез, обобщения);

- развивают системное мышление.

**Деловые, ролевые игры, тренинги**

Деловая игра - это метод группового обучения совместной деятельности в процессе решения общих задач в условиях максимально возможного приближения к реальным проблемным ситуациям. Деловые игры в профессиональном обучении воспроизводят действия участников, стремящихся найти оптимальные пути решения производственных, социально-экономических педагогических, управленческих и других проблем.

Специфика обучающих возможностей деловой игры как метода активного обучения состоит в следующем:

· процесс обучения максимально приближен к реальной практической деятельности руководителей и специалистов. Это достигается путем использования в деловых играх моделей реальных социально-экономических отношений.

· метод деловых игр представляет собой не что иное, как специально организованную деятельность по активизации полученных теоретических знаний, переводу их в деятельностный контекст. То, что в традиционных методах обучения «отдается на откуп» каждому учащемуся без учета его готовности и способности осуществить требуемое преобразование, в деловой игре приобретает статус метода. Происходит не механическое накопление информации, а деятельностное распредмечивание какой-то сферы человеческой реальности.

Виды деловых игр

На сегодняшний день существует большое разнообразие типологий и классификаций деловых игр. Можно выделить следующую классификацию:

1. По типу человеческой практики, воссоздаваемой в игре и каковы целям:

- учебная,

- исследовательская,

- управленческая,

- аттестационная;

2. По времени проведения:

- без ограничения времени;

- с ограничением времени;

- игры, проходящие в реальное время;

- игры, где время сжато;

3. По оценке деятельности:

- балльная или иная оценка деятельности игрока или команды;

- оценка того, кто как работал, отсутствует;

4. По конечному результату:

- жесткие игры – заранее известен ответ (например, сетевой график), существуют жесткие правила;

- свободные, открытые игры – заранее известного ответа нет, правила изобретаются для каждой игры свои, участники работают над решением неструктурированной задачи;

5. По конечной цели:

- обучающие – направлены на появление новых знаний и закрепление навыков участников;

- констатирующие - конкурсы профессионального мастерства;

- поисковые – направлены на выявление проблем и поиск путей их решения;

6. По методологии проведения:

- луночные игры – игра проходит на специально организованном поле, с жесткими правилами, результаты заносятся на бланки;

- ролевые игры – каждый участник имеет или определенное задание, или определенную роль, которую он должен исполнить в соответствии с заданием;

- групповые дискуссии – связаны с отработкой проведения совещаний или приобретением навыков групповой работы. Участники имеют индивидуальные задания, существуют правила ведения дискуссии;

- имитационные – имеют цель создать у участников представление, как следовало бы действовать в определенных условиях;

- организационно-деятельностные игры – не имеют жестких правил, у участников нет ролей, игры направлены на решение междисциплинарных проблем. Активизация работы участников происходит за счет жесткого давления на личность;

- инновационные игры – формируют инновационное мышление участников, выдвигают инновационные идеи в традиционной системе действий, отрабатывают модели реальной, желаемой, идеальной ситуаций, включают тренинги по самоорганизации;

- ансамблевые игры – формируют управленческое мышление у участников, направлены на решение конкретных проблем предприятия методом организации делового партнерского сотрудничества команд, состоящих из руководителей служб.

Началу деловой игры предшествует изложение проблемной ситуации педагогом, формирование цели и задач игры, организация команд и определение их заданий, уточнение роли каждого из участников. Взаимодействие участников игры определяется правилами, отражающими фактическое положение дел в соответствующей области деятельности. Подведение итогов и анализ оптимальных решений завершают деловую игру.

С помощью деловой игры можно определить: наличие тактического и стратегического мышления; способность анализировать собственные возможности и выстаивать соответствующую линию поведения; способность анализировать возможности и мотивы других людей и влиять на их поведение.

Проведение деловой игры состоит из следующих частей:

- инструктаж преподавателя о проведении игры (цель, содержание, конечный результат, формирование игровых коллективов и распределение ролей);

- изучение студентами документации (сценарий, правила, поэтапные задания), распределение ролей внутри подгруппы;

- собственно игра (изучение ситуации, обсуждение, принятие решения, оформление);

- публичная защита предлагаемых решений;

- определение победителей игры;

- подведение итогов и анализ игры преподавателем.

Использование деловых игр способствует развитию навыков критического мышления, коммуникативных навыков, навыков решения проблем, обработке различных вариантов поведения в проблемных ситуациях.

В учебном процессе применяют различные модификации деловых игр.

Имитационные игры. На занятиях имитируется деятельность какой-либо организации, предприятия или его подразделения. Имитироваться могут события, конкретная деятельность люден (деловое совещание, обсуждение плана) и обстановка, условия, в которых происходит событие или осуществляется деятельность (кабинет начальника цеха, зал заседаний). Сценарий имитационной игры, кроме сюжета события, содержит описание структуры и назначения имитируемых процессов и объектов.

Исполнение ролей (ролевые игры). В этих играх отрабатывается тактика поведения, действий, выполнение функций и обязанностей конкретного лица. Для проведения игр с исполнением роли разрабатывается модель-пьеса ситуации, между студентами распределяются роли с «обязательным содержанием», характеризующиеся различными интересами; в процессе их взаимодействия должно быть найдено компромиссное решение. В основе разыгрывания ролей всегда лежит конфликтная ситуация. Студенты, не получившие роли, наблюдают за ходом игры и участвуют в ее заключительном анализе.

«Деловой театр» (метод инсценировки). В нем разыгрывается какая-либо ситуация, поведение человека в этой обстановке, Студент должен вжиться в образ определенного лица, понять его действия, оценить обстановку и найти правильную линию поведения. Основная задача метода инсценировки - научить ориентироваться в различных обстоятельствах, давать объективную оценку своему поведению, учитывать возможности других людей, влиять на их интересы, потребности и деятельность, не прибегая к формальным атрибутам власти, к приказу. Для метода инсценировки составляется сценарий, где описывается конкретная ситуация, функции и обязанности конкретных лиц, их задачи.

Игровое проектирование является практическим занятием или циклом занятий, суть которых состоит в разработке инженерного, конструкторского, технологического и других видов проектов в игровых условиях, максимально воссоздающих реальность. Этот метод отличается высокой степень сочетания индивидуальной и совместной работы студентов. Создание общего для группы проекта требует, с одной стороны, знание каждым технологии процесса проектирования, а с другой - умений вступать в общение и поддерживать межличностные отношения с целью решения профессиональных вопросов. Игровое проектирование может перейти в реальное проектирование, если его результатом будет решение конкретной практической проблемы, а сам процесс будет перенесен в условия действующего предприятия.

Познавательно-дидактические игры не относятся к деловым играм. Они предполагают лишь включение изучаемого материала в необычный игровой контекст и иногда содержат лишь элементы ролевых игр. Такие игры могут проводиться в виде копирования научных, культурных, социальных явлений (конкурс знатоков, «Поле чудес», КВН и т.д.) и в виде предметно-содержательных моделей, (например, игры-путешествия, когда надо разработать рациональный маршрут, пользуясь различными картами).

Тренинг (англ.training от train— обучать, воспитывать)— метод активного обучения, направленный на развитие знаний, умений и навыков и социальных установок.

Тренинг – форма интерактивного обучения, целью которого является развитие компетентности межличностного и профессионального поведения в общении.

Достоинство тренинга заключается в том, что он обеспечивает активное вовлечение всех участников в процесс обучения.

**Кейс-метод**

Кейс-метод или метод конкретных ситуаций следует отнести к методам активного проблемного, эвристического обучения. Название метода происходит от английского case– случай, ситуация и от понятия «кейс»- чемоданчик для хранения различных бумаг, журналов, документов и пр.

Суть его в том, что учащимся предлагают осмыслить и найти решение для ситуации, имеющей отношения к реальным жизненным проблемам и описание которой отражает какую-либо практическую задачу. Отличительной особенностью данного метода является создание проблемной ситуации на основе фактов из реальной жизни. При этом сама проблема не имеет однозначных решений. Для работы с такой ситуацией необходимо правильно поставить учебную задачу, и для ее решения подготовить «кейс» с различными информационными материалами (статьи, литературные рассказы, сайты в сети Интернет, статистические отчеты и пр.)

Поставив правильно задачу и подготовив «кейс», необходимо организовать деятельность обучающихся по разрешению поставленной проблемы. Работа в режиме кейс-метода предполагает групповую деятельность. Непосредственная цель метода - совместными усилиями каждая из подгрупп, обучающихся анализирует ситуацию - case, и вырабатывает практическое решение. В результате организуется деятельность по оценке предложенных алгоритмов и выбору лучшего в контексте поставленной проблемы решения.

Основой изучения дисциплины является самостоятельная работа студента над рекомендуемым учебным материалом по темам, приведенным в УМК.

## Тема 1. Понятие "информационная безопасность", составляющие информационной безопасности

## Тема 2 Система формирования режима информационной безопасности.Нормативно-правовые основы информационной безопасности в РФ

## Тема 3. Стандарты информационной безопасности: "Общие критерии". Стандарты информационной безопасности распределенных систем.Стандарты информационной безопасности в РФ.

## Тема 4. Административный уровень обеспечения информационной безопасности. Классификация угроз "информационной безопасности"

## Тема 5. Вирусы как угроза информационной безопасности. Классификация компьютерных вирусов

## Тема 6. Характеристика "вирусоподобных" программ. Антивирусные программы

**Тема 7. Профилактика компьютерных вирусов. Обнаружение неизвестного вируса**

**Тема 8. Особенности обеспечения информационной безопасности в компьютерных сетях. Сетевые модели передачи данных**

**Тема 9. Модель взаимодействия открытых систем OSI/ISO. Адресация в глобальных сетях**

**Тема 10. Классификация удаленных угроз в вычислительных сетях. Типовые удаленные атаки и их характеристика**

**Тема 11. Причины успешной реализации удаленных угроз в вычислительных сетях. Принципы защиты распределенных вычислительных сетей**

**Тема 12. Идентификация и аутентификация. Криптография и шифрование**

**Тема 13. Методы разграничения, доступ**

**Тема 14. Регистрация и аудит**

**Тема 15. Межсетевое экранирование. Технология виртуальных частных сетей**

**Задание для домашней контрольной работы**

Тест:

1) К правовым методам, обеспечивающим информационную безопасность, относятся:

- Разработка аппаратных средств обеспечения правовых данных

- Разработка и установка во всех компьютерных правовых сетях журналов учета действий

- Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:

- Хищение жестких дисков, подключение к сети, инсайдерство

- Перехват данных, хищение данных, изменение архитектуры системы

- Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:

- Персональная, корпоративная, государственная

- Клиентская, серверная, сетевая

- Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:

- несанкционированного доступа, воздействия в сети

- инсайдерства в организации

- чрезвычайных ситуаций

5) Основные объекты информационной безопасности:

- Компьютерные сети, базы данных

- Информационные системы, психологическое состояние пользователей

- Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:

- Искажение, уменьшение объема, перекодировка информации

- Техническое вмешательство, выведение из строя оборудования сети

- Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:

- Экономической эффективности системы безопасности

- Многоплатформенной реализации системы

- Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:

- руководители, менеджеры, администраторы компаний

- органы права, государства, бизнеса

- сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное:

- Установление регламента, аудит системы, выявление рисков

- Установка новых офисных приложений, смена хостинг-компании

- Внедрение аутентификации, проверки контактных данных пользователей

тест 10) Принципом информационной безопасности является принцип недопущения:

- Неоправданных ограничений при работе в сети (системе)

- Рисков безопасности сети, системы

- Презумпции секретности

11) Принципом политики информационной безопасности является принцип:

- Невозможности миновать защитные средства сети (системы)

- Усиления основного звена сети, системы

- Полного блокирования доступа при риск-ситуациях

12) Принципом политики информационной безопасности является принцип:

- Усиления защищенности самого незащищенного звена сети (системы)

- Перехода в безопасное состояние работы сети, системы

- Полного доступа пользователей ко всем ресурсам сети, системы

13) Принципом политики информационной безопасности является принцип:

- Разделения доступа (обязанностей, привилегий) клиентам сети (системы)

- Одноуровневой защиты сети, системы

- Совместимых, однотипных программно-технических средств сети, системы

14) К основным типам средств воздействия на компьютерную сеть относится:

- Компьютерный сбой

- Логические закладки («мины»)

- Аварийное отключение питания

15) Когда получен спам по e-mail с приложенным файлом, следует:

- Прочитать приложение, если оно не содержит ничего ценного – удалить

- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама

- Удалить письмо с приложением, не раскрывая (не читая) его

16) Принцип Кирхгофа:

- Секретность ключа определена секретностью открытого сообщения

- Секретность информации определена скоростью передачи данных

- Секретность закрытого сообщения определяется секретностью ключа

17) ЭЦП – это:

- Электронно-цифровой преобразователь

- Электронно-цифровая подпись

- Электронно-цифровой процессор

18) Наиболее распространены угрозы информационной безопасности корпоративной системы:

- Покупка нелицензионного ПО

- Ошибки эксплуатации и неумышленного изменения режима работы системы

- Сознательного внедрения сетевых вирусов

19) Наиболее распространены угрозы информационной безопасности сети:

- Распределенный доступ клиент, отказ оборудования

- Моральный износ сети, инсайдерство

- Сбой (отказ) оборудования, нелегальное копирование данных

тест\_20) Наиболее распространены средства воздействия на сеть офиса:

- Слабый трафик, информационный обман, вирусы в интернет

- Вирусы в сети, логические мины (закладки), информационный перехват

- Компьютерные сбои, изменение админстрирования, топологии

21) Утечкой информации в системе называется ситуация, характеризуемая:

- Потерей данных в системе

- Изменением формы информации

- Изменением содержания информации

22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

- Целостность

- Доступность

- Актуальность

23) Угроза информационной системе (компьютерной сети) – это:

- Вероятное событие

- Детерминированное (всегда определенное) событие

- Событие, происходящее периодически

24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:

- Регламентированной

- Правовой

- Защищаемой

25) Разновидностями угроз безопасности (сети, системы) является все перечисленное в списке:

- Программные, технические, организационные, технологические

- Серверные, клиентские, спутниковые, наземные

- Личные, корпоративные, социальные, национальные

26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:

- Владелец сети

- Администратор сети

- Пользователь сети

27) Политика безопасности в системе (сети) – это комплекс:

- Руководств, требований обеспечения необходимого уровня безопасности

- Инструкций, алгоритмов поведения пользователя в сети

- Нормы информационного права, соблюдаемые в сети

28) Наиболее важным при реализации защитных мер политики безопасности является:

- Аудит, анализ затрат на проведение защитных мер

- Аудит, анализ безопасности

- Аудит, анализ уязвимостей, риск-ситуаций

Критерий оценки:

Полнота ответа на поставленный вопрос, понимание сущности излагаемой точки зрения, умение использовать методы анализа и оценки экономики для ответов на вопросы, умение читать и анализировать экономическую литературу.

Вопросы для обсуждения на практических занятиях:

1. Основы создания информационных систем в управлении предприятием.

2. Интегрированные информационные системы.

3. Информационные базы интегрированных информационных систем.

4. Информация как основа функционирования предприятия.

5. Основы управления информационными ресурсами.

6. Информационные системы управления документационным обеспечением предприятия.

7. Основы безопасности информационных систем.

8. Основы информационной безопасности.

9. Экономическая безопасность предприятия.

10. Анализ защищенности корпоративных систем.

11. Методологические основы открытых систем.

12. Программно-технологическая безопасность информационных систем.

13. Современные информационные технологии.

14. Информационные технологии управления в корпоративных системах.

15. Средства информационных технологий обеспечения управленческой деятельности.

16. Компьютерные технологии обработки экономической информации на основе табличных процессоров.

17. Компьютерные технологии использования систем управления базами данных (СУБД).

18. Компьютерные технологии интегрированных программных пакетов.

19. Интегрированные информационные технологии в управленческой деятельности.

20. Организация компьютерных информационных систем.

21. Компьютерные технологии интеллектуальной поддержки управленческих решений.