МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Воронежский государственный аграрный университет имени императора Петра I»

Экономический факультет

Кафедра Информационного обеспечения и моделирования агроэкономических систем

Информационная безопасность

Методические указания для обучающихся по освоению дисциплины и самостоятельной работе

Специальность:
38.05.01 Экономическая безопасность

Специализация:
Экономико-правовое обеспечение экономической безопасности

Воронеж 2017

Горюхина Е.Ю. Информационная безопасность: Методические указания для обучающихся по освоению дисциплины и самостоятельной работе (специальность 38.05.01 Экономическая безопасность: специализация Экономико-правовое обеспечение экономической безопасности)/ Е.Ю. Горюхина. – Воронеж: ВГАУ, 2017 – 15 с.

Рецензент: к.э.н., доцент кафедры управления и маркетинга в АПК федерального государственного образовательного учреждения высшего образования «Воронежский государственный аграрный университет имени императора Петра I» Сабетова Т.В.

Методические указания рассмотрены и рекомендованы к изданию на заседании кафедры Информационного обеспечения и моделирования агроэкономических систем (протокол № 8 от 10 апреля 2017 г.).

Методические указания рассмотрены и рекомендованы к изданию на заседании методической комиссии экономического факультета (протокол № 3 от 16 мая 2017 г.).

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

1. Цель и задачи дисциплины. Формирование знаний и умений для проведения анализа информационных угроз для предприятий и организаций, обеспечения комплексной защиты информационных ресурсов и управления информационными рисками; ознакомление студентов с основами современных методов и средств защиты информации, обучение приемам практического использования программно-аппаратных средств защиты информации.

Основными задачами изучения дисциплины являются:

Изучение сущности и понятия информационной безопасности.

Изучение современной концепции информационной безопасности.

Изучение методов анализа и оценки состояния обеспечения информационной безопасности в организации.

Изучение методов и средств комплексной защиты информации в информационных системах коммерческих предприятий и государственных учреждений

Владение основами использования информационно-коммуникационных технологий с учетом основных требований информационной безопасности.

Владение навыками анализа защищенности информационных систем, использования возможностей технических и программных средств защиты и обеспечения безопасности информации.

Владение программно-техническими средствами обеспечения информационной безопасности.

Умение использовать в практической деятельности нормативно-правовые документы и стандарты в области информационной безопасности при эксплуатации информационных систем и технологий.

Умение использовать в практической деятельности существующие методы и средства контроля и защиты информации.

2. Требования к уровню освоения дисциплины.

Дисциплина нацелена на формирование компетенций:

Компетенция		Планируемые результаты обучения
Код	Название	
ОК-12	Способность работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации	**Знать**: - основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации с использованием правил информационной безопасности **Уметь:** - применять в профессиональной сфере деятельности основные методы, способы и средства получения, хранения, передачи и защиты информации с учетом правил информационной безопасности **Иметь навыки**: - работы с различными информационными ресурсами и технологиями с учетом правил информационной безопасности
ПК-48	Способность проводить специальные исследования в целях определения потенциальных и реальных угроз экономической безопасности организации	**Знать**: - основные виды угроз информационной и экономической безопасности организаций **Уметь**: - проводить специальные исследования в целях определения потенциальных и реальных угроз экономической безопасности организации **Иметь навыки**: - осуществления мероприятий, направленных на определение потенциальных и реальных угроз экономической безопасности организации

1. УКАЗАНИЯ ПО ИЗУЧЕНИЮ ТЕОРЕТИЧЕСКОЙ ЧАСТИ ДИСЦИПЛИНЫ

1.1. Общие сведения

Лекция является важнейшей формой усвоения теоретического материала, поскольку в режиме реального времени преподаватель может ответить на любой вопрос, возникающий у студента по ходу восприятия лекционного материала, очень важны и комментарии преподавателя по самым разным вопросам теории и практики изучаемой дисциплины. Часто преподаватель дает на лекции самую актуальную информацию, почерпнуть которую самостоятельно студенту не всегда удастся. Кроме указанных объективных причин, требующих от студента посещения лекций, можно отметить и субъективные причины. Посещение лекций является одним из важнейших факторов, характеризующих отношение студента к учебному процессу в целом, и к данной дисциплине в частности. А при текущем и итоговом контроле знаний удельный вес субъективных критериев у каждого преподавателя довольно высок. Следует помнить, что лекция – это не монолог преподавателя. Вопросы, заданные лектору по изучаемой теме, помогут лучше разобраться в ней не только Вам, но и всем остальным студентам, присутствующим на лекции. Несмотря на то, что каждому студенту предоставляется доступ к компьютерным презентациям всего лекционного материала, рекомендуется делать конспекты лекций, в которых необходимо фиксировать наиболее важные моменты, связанные с освоением того или иного теоретического вопроса. Чтение лекций осуществляется в соответствии с рабочей программой учебной дисциплины и календарным планом, разрабатываемым ведущим курса.

1.2. Особенности освоения отдельных тем

Раздел 1. Информационная безопасность

1.1. Основные понятия и термины в области информационной безопасности

При освоении материалов по данному вопросу следует использовать знания, полученные при изучении дисциплины «Экономическая информатика». Особое внимание следует уделить специфическим особенностям информационной безопасности, основным аспектам ее рассмотрения, а также важности обеспечения информационной безопасности в современном мире как на уровне государства, так и для каждого индивида.

1.2. Основные составляющие информационной безопасности

При освоении материалов по данному вопросу необходимо обратить внимание на выявление субъектов информационных отношений и их интересов; рассмотреть такие категории безопасности как обеспечение доступности, целостности и конфиденциальности ресурсов информационной среды и поддерживающей инфраструктуры.

1.3. Понятие и сущность защиты информации

При освоении материалов по данному вопросу необходимо обратить внимание на предупреждение угроз; выявление угроз; обнаружение угроз; пресечение и локализация угроз; ликвидацию угроз; ликвидацию последствий угроз, а также обратить внимание на общие признаки защиты информации

1.4. Предмет и объект защиты информации

При освоении материалов по данному вопросу необходимо обратить внимание на характеристики качества информации; подходы к градации ценности информации; подходы объективной оценки количества информации. Особое внимание следует обратить на совокупность носителей информации, которая представляет собой комплекс физических, аппаратных, программных и документальных средств.

Раздел 2. Угрозы информационной безопасности

2.1. Понятие и классификация угроз информационной безопасности.

При освоении материалов по данному вопросу необходимо обратить внимание на понятие и классификацию угроз информационной безопасности.

2.2. Случайные угрозы. Преднамеренные угрозы

При освоении материалов по данному вопросу необходимо обратить внимание на такие случайные виды угроз как стихийные бедствия и аварии; сбои и отказы; ошибки при разработке ИС. Особое внимание следует обратить на такие виды преднамеренных угроз как традиционный или универсальный шпионаж и диверсии; несанкционированный доступ к информации; электромагнитные излучения и наводки; модификация структур информационных систем; вредительские программы.

2.3. Модель гипотетического нарушителя информационной безопасности

При освоении материалов по данному вопросу необходимо обратить внимание на понятия злоумышленника и нарушителя. Особое внимание следует обратить внимание на понятия внутреннего и внешнего нарушителей. Рассмотреть группы нарушителей по уровню знаний, по уровню возможностей, по времени и месту действия. Следует уделить внимание неформальной модели нарушителя.

Раздел 3. Компьютерные преступления и их особенности

3.1. Понятие компьютерных преступлений и их виды

При освоении материалов по данному вопросу необходимо обратить внимание на понятие компьютерных преступлений, рассмотреть их особенности. Особое внимание следует обратить внимание на такие категории как преступления, связанные с вмешательством в работу компьютера, и преступления, использующие компьютер как необходимые технические средства.

3.2. Вредоносное программное обеспечение

При освоении материалов по данному вопросу необходимо обратить внимание на понятие вредоносного программного обеспечения. Особое внимание следует обратить на такие группы вредоносного программного обеспечения ка компьютерные вирусы, их жизненный цикл, места размещения, разновидности по среде обитания, по способу заражения, по деструктивным особенностям, по особенностям алгоритма функционирования, разрушительные функции; Шпионские программные закладки и их деструктивные действия, механизмы проникновения, их виды в соответствии с методами внедрения в ПК и размещения, модели воздействия программных закладок; Троянские программы и их особенности и отличия от др. вредоносных программ, наиболее распространенные разновидности.

3.3. Методы и технологии борьбы с вредоносными программами

При освоении материалов по данному вопросу необходимо обратить внимание на такие методы обнаружения вирусов как сканирование, обнаружение изменений, эвристический анализ, использование резидентных сторожей, вакцинация, аппаратно-программные антивирусные средства. Особое внимание следует обратить на современные антивирусные средства.

Раздел 4. Законодательные аспекты информационной безопасности в РФ

4.1. Законодательство РФ области информационной безопасности

При освоении материалов по данному вопросу необходимо обратить внимание на основополагающие документы по информационной безопасности в РФ, на общие основные законы, включающие нормы по вопросам информатизации, подзаконные нормативные акты в области информатизации, а также правоохранительное законодательство РФ, содержащее нормы ответственности за правонарушения в области информатизации.

4.2. Нормативно-правовые основы информационной безопасности в РФ

При освоении материалов по данному вопросу необходимо обратить внимание на такие общие основные законы, включающие нормы по вопросам информатизации , как Закон РФ «О государственной тайне», Закон РФ «Об информации, информационных технологиях и о защите информации» № 149-ФЗ от 27.08.2006 г. (новая редакция закона от 27.07.2010 № 227-ФЗ). Особое внимание следует обратить на 5 категорий государственных информационных ресурсов и их особенности.

4.3 Ответственность за нарушения в сфере информационной безопасности в РФ

При освоении материалов по данному вопросу необходимо обратить внимание на статьи 272, 273 и 274 УК РФ.

Раздел 5. Криптографические методы защиты информации

5.1 Основные понятия и определения криптографии. История развития криптографии

При освоении материалов по данному вопросу необходимо обратить внимание на понятия криптографии, криптология и криптоанализ, стеганография, шифрование и дешифрование, ключ, криптосистема. Следует рассмотреть историю развития криптографических методов закрытия информации и примеры их использования.

5.2 Классификация криптографических методов защиты информации

При освоении материалов по данному вопросу необходимо обратить внимание на особенности методов подстановки, перестановки, аддитивных методов, метод аналитических преобразований.

5.3 Электронная подпись

При освоении материалов по данному вопросу необходимо обратить внимание на назначение и особенности. Особое внимание следует обратить на законодательную базу ЭЦП и преимущества использования ЭП. Также следует рассмотреть 3 вида ЭП: простые ЭП, усиленную неквалифицированную ЭП, усиленную квалифицированную ЭП, их назначение и особенности применения. Необходимо рассмотреть криптографическую основу ЭП.

Раздел 6. Системное обеспечение защиты информации

6.1 Концептуальная модель информационной безопасности

При освоении материалов по данному вопросу необходимо обратить внимание на меры законодательного, административного, процедурного и программно-технического уровней обеспечения информационной безопасности. Особое внимание следует обратить на понятие и содержание политики безопасности предприятия, а также основные шаги и алгоритм ее разработки.

6.2 Основные принципы построения системы защиты информации

При освоении материалов по данному вопросу необходимо обратить внимание на такие основные принципы построения системы защиты информации как системность, комплексность, непрерывность, разумная достаточность, гибкость управления и применения, открытость алгоритмов и механизмов защиты информации, простота применения защитных мер и средств.

6.3 Методы защиты информации

При освоении материалов по данному вопросу необходимо обратить внимание на такие методы защиты как минимизация ущерба от аварий и стихийных бедствий, дублирование информации, повышение надежности информационной системы, создание отказоустойчивых информационных систем, оптимизация взаимодействия пользователей и обслуживающего персонала, криптографические методы.

2. УКАЗАНИЯ ПО ПОДГОТОВКЕ К ЛАБОРАТОРНЫМ ЗАНЯТИЯМ

2.1. Общие сведения

Лабораторные занятия – вид учебных занятий, ориентированный на практическое усвоение материала с помощью приборов, инструментов, технических средств обучения, компьютеров и другого специального оборудования.

Обучающая функция лабораторных занятий заключается в освоении студентом практических навыков разработки и реализации экономико-математических моделей, позволяющих решать прикладные задачи из будущей профессиональной деятельности студентов.

Развивающая функция лабораторных занятий реализуется через ориентацию студента на самостоятельное решение отдельных проблем из будущей профессиональной деятельности с помощью специальных методов и инструментов реализации экономических задач.

Воспитательная функция лабораторных занятий заключена в тесном контакте преподавателя с каждым студентом, позволяющем максимально эффективно воздействовать на мировоззрение студента, на формирование у студентов навыков культуры общения и чувства корпоративной этики.

Организующая функция лабораторных занятий предусматривает управление самостоятельной работой студентов как в процессе лабораторных занятий, так и после них. В ходе лабораторных занятий осваиваются методы и средства обработки информации, технологии разработки и реализации АИС, которые создают базис для дальнейшей самостоятельной работы студентов, для формирования навыков исследовательской работы, для генерации новых знаний через использование различного рода информационных ресурсов.

Лабораторные занятия по дисциплине проводятся по подгруппам в компьютерных классах.

Цель лабораторных занятий по дисциплине заключается в установлении связей теории с практикой в форме экспериментального подтверждения положений теории; обучении студентов умению анализировать информационные ресурсы предприятия, анализировать угрозы информационной безопасности предприятия; проведении контроля самостоятельной работы студентов по освоению курса; обучении навыкам профессиональной деятельности.

Основными структурными элементами лабораторных занятий являются:

- обсуждение преподавателем совместно со студентами темы занятий с пояснением ее взаимосвязи с будущей профессиональной деятельностью;
- определение целей защиты информации на предприятии регионального уровня, выявление особенностей объекта защиты информации, определение угроз информационной безопасности, проведение анализа рисков информационной безопасности на предприятии, построение концепции информационной безопасности предприятия;
- консультации преподавателя во время занятий;
- обсуждение и оценка полученных результатов;
- письменный или устный отчет студентов о выполнении заданий;
- текущий контроль знаний.

Проведение лабораторных занятий должно осуществляться в соответствии с рабочей программой учебной дисциплины и календарным планом, разрабатываемым ведущим курса.

Задания для лабораторных занятий берутся из Практикума по информационной безопасности.

2.2. Особенности освоения отдельных тем

Раздел 1. Информационная безопасность

Определение целей защиты информации на предприятии регионального уровня

Для выполнения задания по данной теме следует восстановить в памяти лекционный материал по данному вопросу. Необходимо самостоятельно изучить раздел 1 «Определение

целей защиты информации на предприятии регионального уровня. Рассмотрение особенностей объекта защиты информации» Практикума по информационной безопасности .

Необходимо выполнить задания 1-5 из раздела 1 Практикума по информационной безопасности.

Раздел 2. Угрозы информационной безопасности

Определение угроз информационной безопасности и анализ рисков на предприятии

Для выполнения задания по данной теме следует восстановить в памяти лекционный материал по данному вопросу. Необходимо самостоятельно изучить раздел 3 «Определение угроз информационной безопасности и Анализ рисков предприятия» Практикума по информационной безопасности .

Необходимо выполнить задание 7 из подраздела 3 Практикума по информационной безопасности.

Раздел 3. Компьютерные преступления и их особенности

Работа с антивирусными программами

Для выполнения задания по данной теме следует восстановить в памяти лекционный материал по данному вопросу. Необходимо самостоятельно изучить подраздел «Пакеты антивирусных программ» раздела 4 из Практикума по информационной безопасности .

Необходимо выполнить задание 16-18 из подраздела 4 Практикума по информационной безопасности.

Раздел 4. Законодательные аспекты информационной безопасности

Работа с поисково-справочной системой КонсультантПлюс и нормативно-правовой базой защиты информации

Для выполнения задания по данной теме следует восстановить в памяти лекционный материал по данному вопросу. Необходимо самостоятельно изучить раздел 5 «Законодательные основы защиты информации» Практикума по информационной безопасности .

Необходимо выполнить задание 19 из подраздела 5 Практикума по информационной безопасности.

Необходимо самостоятельно изучить раздел 2 «Определение сведений конфиденциального характера» Практикума по информационной безопасности .

Необходимо выполнить задание 6 из раздела 2 Практикума по информационной безопасности.

Раздел 5. Криптографические методы защиты информации

5.1 Простые шифры.

Для выполнения задания по данной теме следует восстановить в памяти лекционный материал по данному вопросу. Необходимо самостоятельно изучить раздел 7 «Реализация криптографических методов» Практикума по информационной безопасности . Необходимо выполнить задание 29 из подраздела 7 Практикума по информационной безопасности, используя алгоритмы простых шифров.

5.2 Криптографические алгоритмы на основе метода подстановок и метода перестановок

Для выполнения задания по данной теме следует восстановить в памяти лекционный материал по данному вопросу. Необходимо самостоятельно изучить раздел 7 «Реализация криптографических методов» Практикума по информационной безопасности . Необходимо выполнить задание 29 из подраздела 7 Практикума по информационной безопасности, используя алгоритмы метода подстановок и метода перестановок.

5.3 Ассиметричные криптографические системы

Для выполнения задания по данной теме следует восстановить в памяти лекционный материал по данному вопросу. Необходимо самостоятельно изучить раздел 7 «Реализация криптографических методов» Практикума по информационной безопасности и подраздел « Парольные системы» того же Практикума. Необходимо выполнить задание 8-12 из подраздела 4 Практикума по информационной безопасности.

Раздел 6. Системное обеспечение защиты информации

6.1 Построение концепции и политики безопасности предприятия

Для выполнения задания по данной теме следует восстановить в памяти лекционный материал по данному вопросу. Необходимо самостоятельно изучить подразделы «Основные концептуальные положения системы защиты информации», «Построение концепции информационной безопасности предприятия» раздела 6 из Практикума по информационной безопасности

Необходимо выполнить задание 20 из раздела 6 Практикума по информационной безопасности.

6.2 Защита средствами операционных систем

Для выполнения задания по данной теме следует восстановить в памяти лекционный материал по данному вопросу. Необходимо самостоятельно изучить подраздел «Защита информации средствами операционной системы» раздела 6 из Практикума по информационной безопасности

Необходимо выполнить задание 21-28 из раздела 6 Практикума по информационной безопасности.

6.3 Защита информации средствами файловых менеджеров

Для выполнения задания по данной теме следует использовать знания, полученные при изучении раздела «Сервисные программы» дисциплины «Информатика». Для выполнения задания по данной теме следует восстановить в памяти лекционный материал по данному вопросу.

6.4 Защита информации средствами программ-архиваторов

Для выполнения задания по данной теме следует использовать знания, полученные при изучении раздела «Сервисные программы» дисциплины «Информатика». Для выполнения задания по данной теме следует восстановить в памяти лекционный материал по данному вопросу. Необходимо самостоятельно изучить подраздел «Архивирование с паролем» раздела 4 Практикума по информационной безопасности

Необходимо выполнить задание 13-15 из подраздела 4 Практикума по информационной безопасности.

6.5 Защита информации в приложениях MS Office

Для выполнения задания по данной теме следует использовать знания, полученные при изучении раздела «Пакеты прикладных программ» дисциплины «Информатика». Для выполнения задания по данной теме следует восстановить в памяти лекционный материал по данному вопросу.

Необходимо выполнить защиту файла, содержащего отчет о выполнении лабораторных заданий по дисциплине, используя возможности MS Office

3. УКАЗАНИЯ ПО ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Самостоятельная работа при изучении дисциплины складывается из самостоятельной работы на аудиторных занятиях и внеаудиторной самостоятельной работы.

Самостоятельная работа предполагает широкое использование различных источников информации (учебников и учебных пособий, специальной научной и научно-популярной литературы, ресурсов глобальной сети Интернет, материалов личных наблюдений и умозаключений и т.д.).

Связь студента с преподавателем при необходимости и в ходе самостоятельной работы может осуществляться по электронной почте, адрес которой преподаватель должен дать студенту на первом же занятии.

Основными видами самостоятельной работы при изучении дисциплины являются:

- самостоятельная подготовка к лабораторным занятиям через проработку лекционного материала по соответствующей теме;
- самостоятельное изучение тем теоретического курса, не вошедших в лекционный материал;
- самостоятельное изучение тем лабораторных занятий;
- систематизация знаний путем проработки пройденных лекционных материалов по конспекту лекций, учебникам и пособиям на основании перечня экзаменационных вопросов, тестовых вопросов по материалам лекционного курса и базовых вопросов по результатам освоения тем, вынесенных на лабораторные занятия, приведенных в Практикуме по дисциплине;
- подготовка к текущему и итоговому контролю;
- самостоятельное выполнение лабораторных работ.

Студенты всех форм обучения самостоятельно изучают все темы дисциплины на основе собственных конспектов лекций, материалов компьютерных презентаций лекционного курса, основной и дополнительной литературы и других информационных ресурсов.

Все практические задания выполняются как на лабораторных занятиях (в то числе и самостоятельно), так и вне аудиторий.

Систематизацию знаний необходимо осуществлять самостоятельно как в ходе отдельных аудиторных занятий, так и во время внеаудиторной работы. Систематизация знаний проводится на основе проработки собственных конспектов лекций, материалов компьютерных презентаций лекционного курса, формирования отчета о выполняемых темах лабораторных занятий, изучения основной и дополнительной литературы и поиска необходимой информации в других информационных ресурсах.

В этой связи на каждом лабораторном занятии проводятся опросы студентов с целью как контроля самостоятельной работы, так и с целью побуждения к осознанной работе по целенаправленной систематизации знаний.

Важным аспектом при систематизации знаний являются консультации преподавателя, который на каждом занятии должен обращать внимание студентов на ключевые вопросы каждой темы и на взаимосвязь тем между собой.

4. ПОДГОТОВКА К ТЕКУЩЕМУ КОНТРОЛЮ ЗНАНИЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

4.1. Общие сведения

Целью текущего контроля знаний со стороны преподавателя является оценка качества освоения студентами данной дисциплины в течение всего периода ее изучения. К главной задаче текущего контроля относится повышение мотивации студентов к регулярной учебной работе, самостоятельной работе, углублению знаний, дифференциации итоговой оценки знаний.

Преподаватель, осуществляющий текущий контроль, на первом занятии доводит до сведения студентов требования и критерии оценки знаний по дисциплине. В целях предупреждения возникновения академической задолженности (либо своевременной ее ликвидации) преподаватель проводит регулярные консультации и иные необходимые мероприятия в пределах учебных часов, предусмотренных учебным планом.

При преподавании данной дисциплины предусматриваются следующие формы текущего контроля знаний: текущий контроль в форме индивидуальных опросов, текущий контроль в форме тестирования, текущий контроль в форме проверки контрольных работ и собеседования со студентом (для студентов заочной формы обучения).

Промежуточная аттестация проводится в форме сдачи экзамена.

Студент должен с первого занятия помнить, что по каждому разделу дисциплины будет проводиться тестирование по материалам теоретического курса, а по результатам выполненных тем лабораторных занятий будет производиться индивидуальный опрос.

Подготовка к текущему и итоговому контролю происходит как в ходе отдельных аудиторных занятий, так и во время внеаудиторной работы.

По итогам выполнения заданий по каждой теме лабораторных занятий необходимо сформировать письменный отчет с результатами каждого задания. При подготовке к защите отчета (сдаче работы) необходимо самостоятельно повторить лекционный материал по данной теме и провести самоконтроль знаний на основании перечня вопросов для самоконтроля по отдельным темам, приведенных в Практикуме по дисциплине.

После изучения каждого раздела учебной дисциплины подготовка к тестированию знаний проводится на основании тестовых вопросов, приведенных в Практикуме по дисциплине.

К итоговому контролю следует готовиться на основании вопросов, приведенных в рабочей программе учебной дисциплины.

4.2. Текущий контроль знаний в форме индивидуальных опросов

Постоянный текущий контроль знаний (после изучения каждой темы и раздела) позволяет студенту систематизировать знания, как в разрезе отдельных тем, так и отдельных разделов дисциплины. По итогам каждой темы лабораторных занятий должен быть сформировать отчет с результатами выполнения индивидуального задания. В ходе индивидуального опроса преподаватель должен проверить правильность выполнения задания и уровень освоения студентом данной темы. Вопросы для самоконтроля по отдельным темам лабораторных занятий приведены в Практикуме по информатике. При индивидуальном опросе преподаватель обращает особое внимание на знание студентами основных вопросов темы. По результатам опроса по каждой теме студенту выставляется оценка.

Критерии оценки знаний по отдельным темам:

- оценка «отлично» выставляется, если студент выполнил задание полностью и без ошибок, показал полные и глубокие знания по изученной теме, логично и аргументировано ответил на все вопросы по выполненному заданию;
- оценка «хорошо» выставляется, если студент выполнил задание полностью и без ошибок, твердо знает материал по данной теме, грамотно его излагает, не допускает существенных неточностей в ответе, достаточно полно отвечает на вопросы по выполненному заданию;
- оценка «удовлетворительно» выставляется, если студент выполнил задание полностью, но с незначительными ошибками, показал знание только основ материала по данной теме, усвоил его поверхностно, но не допускал при ответе на вопросы грубых ошибок или неточностей;

- оценка «неудовлетворительно» выставляется, если студент выполнил задание полностью, но с грубыми ошибками, не знает основ материала по данной теме, допускает при ответе на вопросы грубые ошибки или неточности.

Студент не аттестуется по данной теме, если задание по теме не выполнено или выполнено не полностью.

Если студент не аттестован хотя бы по одной из тем лабораторных занятий или имеет оценку «неудовлетворительно», то преподаватель, ведущий лабораторные занятия, имеет право не допустить студента до сдачи экзамена.

4.3. Текущий контроль знаний в форме тестирования

Тестирование - форма унифицированного контроля знаний, умений и навыков на основе тестов, стандартизированных процедур проведения тестового контроля, обработки, анализа и представления результатов. Тестирование как форма текущего контроля знаний используется по мере изучения отдельных разделов дисциплины. Также тестирование проводится и после изучения всего курса.

Вопросы тестов приведены в Учебном пособии по дисциплине. Тестирование по разделам дисциплины и в целом по дисциплине проходит в соответствии с графиком тестирования, составляемым на основе календарных планов проведения аудиторных занятий.

На основании аттестации по отдельным темам лабораторных занятий и результатов тестирования преподаватель, ведущий лабораторные занятия, выводит среднюю интегрированную оценку, которой он оценивает результаты освоения дисциплины каждым студентом.

4.4. Текущий контроль знаний в форме проверки контрольной работы и собеседования со студентом (для заочной формы обучения)

Контрольная работа (для заочной формы обучения) является одной из наиболее эффективных форм самостоятельной работы студента, позволяющей не только глубоко изучить теорию того или иного вопроса, связанного с профессиональной деятельностью специалиста, но и получить навыки практической работы.

Цель выполняемой контрольной работы заключается в изучении теоретических и методических основ информационной безопасности; в определении номенклатуры информационных активов предприятия; в определении перечня сведений, относящихся к конфиденциальным; в определении наиболее опасных каналов утечки информации, способов и средств противодействия утечке.

Данная цель может быть достигнута при успешном решении студентами следующих задач:

1. Изучение теоретических аспектов информационной безопасности;
2. Исследование конкретного хозяйствующего субъекта регионального уровня в качестве предметной области для анализа информационных ресурсов;
3. Приобретение навыков практического проведения анализа информационных ресурсов предприятия регионального уровня;
4. Закрепление навыков самостоятельного использования современных информационных технологий через:

– подбор и освоение информации по теме с помощью электронных каталогов, поисковых систем Интернета, электронных библиотек и других информационных ресурсов;

– оформление электронной версии контрольной работы в соответствии с предъявляемыми требованиями.

4.5. Промежуточная аттестация в форме зачета

Зачет учебным планом не предусмотрен

4.6. Промежуточная аттестация в форме дифференцированного зачета по результатам защиты курсового проекта

Курсовой проект учебным планом не предусмотрен

4.7. Промежуточная аттестация в форме экзамена

К экзамену допускаются студенты:

- аттестованные по всем темам лабораторных занятий;
- не имеющие по этим темам ни одной оценки «неудовлетворительно»;
- набравшие в ходе заключительного тестирования (по всем разделам дисциплины) не менее 30 баллов.

Студенты, имеющие по всем темам лабораторных занятий оценки «отлично» и набравшие в ходе заключительного тестирования не менее 90 баллов, могут быть рекомендованы к освобождению от экзамена с выставлением итоговой оценки «отлично».

Экзаменационный билет содержит два теоретических вопроса.

Вопросы, выносимые на экзамен, приведены в Фонде оценочных средств по дисциплине.

Экзамен проходит в устной форме, но с предоставлением экзаменатору тезисов ответов на вопросы экзаменационного билета. Тезисы ответов на вопросы экзаменационного билета хранятся у экзаменатора 30 дней со дня проведения экзамена.

Критерии оценки знаний, продемонстрированных при сдаче экзамена:

- оценка «отлично» выставляется, если студент показал полные и глубокие знания программного материала, логично и аргументировано ответил на все вопросы экзаменационного билета, а также на дополнительные вопросы;
- оценка «хорошо» выставляется, если студент твердо знает программный материал, грамотно его излагает, не допускает существенных неточностей в ответе, достаточно полно ответил на вопросы экзаменационного билета и дополнительные вопросы;
- оценка «удовлетворительно» выставляется, если студент показал знание только основ программного материала, усвоил его поверхностно, но не допускал грубых ошибок или неточностей, требует наводящих вопросов для правильного ответа, не ответил на дополнительные вопросы;
- оценка «неудовлетворительно» выставляется, если студент не знает основ программного материала, допускает грубые ошибки в ответе.