Министерство образования Азербайджанской Республики
Общество с ограниченной ответственностью
«Азербайджанский Государственный Экономический Университет»
Дербентский филиал Общества с ограниченной ответственностью
«Азербайджанский Государственный Экономический Университет»

«Утверждаю»
Ректор, профессор
_____ А.Д.Мурадов
«___» _____ 2015 г.

РАБОЧАЯ ПРОГРАММА
по дисциплине

Б2.В.ДВ.2.2 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки
38.03.01 «Экономика»

Профиль подготовки
Общий профиль

Квалификация (степень) выпускника
Бакалавр

Форма обучения
очная; заочная

Дербент – 2015

Содержание

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель учебной дисциплины: изучение основ информационной безопасности, применение в современных информационных технологиях методов и средств защиты информации, используемых для решения проблем компьютерной безопасности; приобретение навыков владения основным инструментарием и его применения для построения защищенных информационных систем. Достижение указанных целей позволит обучающемуся продолжить профессиональное образование в магистратуре и/или успешно начать профессиональную деятельность.

Задачи учебной дисциплины «Информационная безопасность»:

- познакомить студентов с определением, классификацией и характеристиками информационной безопасности;
- познакомить с организационными и экономическими аспектами работы с информационными ресурсами и методами оценки эффективности их безопасности;
- дать представление об особенностях информационной безопасности, сегментах и участниках информационного рынка, особенностях формирования безопасности информации;
- рассмотреть основные технологические принципы безопасности мировых информационных ресурсов на основе глобальной сети Интернет;
- рассмотреть возможности применения безопасности ресурсов Интернете.

2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- способен понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны (ОК-12);
- способен использовать для решения аналитических и исследовательских задач современные технические средства и информационные технологии (ПК-10).

Изучив курс, студент должен:

Знать:

- основные понятия информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации (ОК-12);
- принципы организации информационных систем в соответствии с требованиями по защите информации, методы и средства выявления угроз безопасности предприятия (ПК-10);

Уметь:

- определять наличие угроз и использовать методы и средства для обеспечения информационной безопасности (ОК-10); анализировать и оценивать угрозы информационной безопасности объекта (ПК-10);

Владеть:

- методами формирования требований по обеспечению информационной безопасности, навыками осуществления профессиональной деятельности в условиях информационного противоборства(ОК-10; навыками организации и обеспечения

режима секретности, методами организации и управления деятельностью служб защиты информации на предприятии (ПК-10).

3. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВПО

Дисциплина «Информационная безопасность» относится к вариативной части математического и естественнонаучного цикла.

Для изучения данной дисциплины необходимы знания, умения и навыки, формируемые предшествующими дисциплинами: Информационные технологии и коммуникации, Информационные системы в экономике, Информационные технологии в профессиональной деятельности.

Наименования последующих учебных дисциплин: Производственная практика и ИГА.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЗАЧЕТНЫХ ЕДИНИЦАХ И АКАДЕМИЧЕСКИХ ЧАСАХ

Общая трудоемкость дисциплины составляет 108 часов, 3 зачетных единиц.

Вид учебной работы		**Форма обучения**	
		очная	**заочная**
Семестр		**7**	**9**
Общая трудоемкость дисциплины	**час**	**108**	**108**
	ЗЕТ	**3**	**3**
1.Контактная работа обучающихся с преподавателем, всего		48	18
Аудиторная работа, всего		*44*	*14*
из них в интерактивной форме		*12*	*4*
Лекции		*16*	*6*
Практические занятия		*28*	*8*
Внеаудиторная работа, всего		*4*	*4*
в том числе			
- индивидуальная работа обучающихся с преподавателем;		*4*	-
- промежуточная аттестация – зачет		-	*4*
2. Самостоятельная работа обучающихся, всего		60	90

5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

5.1.Структура дисциплины

для очной формы обучения

Наименование разделов (модулей) и тем	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего контроля успеваемости. Форма промежуточной аттестации
	ЛК	ПР	СРС	КСР	

Тема 1. Понятие информационной безопасности и защищенной системы	4	4	15	2	Устный опрос, защита рефератов, контрольная работа
Тема 2. Основные положения теории информационной безопасности информационных систем	4	8	15		
Тема 3. Общее представление о структуре защищенной информационной системы	4	8	15	2	
Тема 4. Роль стандартов информационной безопасности	4	8	15		
Итоговый контроль					**зачет**
Итого	**16**	**28**	**60**	**4**	

для заочной формы обучения

Наименование разделов (модулей)	**Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)**				**Формы текущего контроля успеваемости Форма промежуточной аттестации**
	ЛК	**ПК**	**СРС**	**Конт роль**	
Тема 1. Понятие информационной безопасности и защищенной системы	1	1	15		Устный опрос, Защита рефератов, контрольная работа
Тема 2. Основные положения теории информационной безопасности информационных систем	1	1	25		Устный опрос, тестирование, защита рефератов, контрольная работа
Тема 3. Общее представление о структуре защищенной информационной системы	2	2	25		
Тема 4. Роль стандартов информационной безопасности	2	4	25		
Итоговый контроль				4	**зачет**
Итого	6	8	90	4	

5.2. Содержание тем лекционных занятий

Тема 1. Понятие информационной безопасности и защищенной системы.

1. Основные понятия информационной безопасности.
2. Классификация и характеристика случайных угроз.
3. Общая характеристика преднамеренных угроз.
4. Особенности несанкционированного доступа к информации.
5. Виды возможных нарушений информационной системы.
6. Оценка создания более безопасных продуктов ИТ по направлениям.

7. Особенности видов угроз как вредительских программ.
8. Особенности угроз безопасности информации, связанных с несанкционированной модификацией структур КС.

Тема 2. Основные положения теории информационной безопасности информационных систем.

1. Основные положения теории информационной безопасности информационных систем.
2. Классификацию видов и свойств вирусов.
3. Вредительские программы и их особенности.
4. Технические и программные способы защиты от вирусов.
5. Основные типы политики безопасности управления доступом к данным.
6. Виды нарушений информационной системы.
7. Особенности защиты информационных систем.
8. Нормативные руководящие документы, касающиеся государственной тайны и нормативно справочные документы.
9. Системы с закрытым и открытым ключом

Тема 3. Общее представление о структуре защищенной информационной системы.

1. Принципы построения комплексных систем защиты информации.
2. Концепции создания защищенных КС.
3. Виды и способы защиты от несанкционированного проникновения в систему.
4. Программное обеспечения защиты компьютерных систем.
5. Идентификации и аутентификации и различные виды схем аутентификации.
6. Механизмы доступа данных в операционных системах, системах управления базами данных.
7. Способы защиты данных и сервисов от воздействия вредоносных программ.
8. Методы и средства шифрования и дешифровки.
9. Кодирования и средства защиты при шифровании данных.
10. Использование защищенных компьютерных систем. Политика безопасности.
11. Основные этапы разработки защищенной системы.

Тема 4. Роль стандартов информационной безопасности.

1. Удаленный доступ к файлам, защищенным путем криптографии.
2. Методика защиты компьютерных систем.
3. Основные технологии построения защищенных ЭИС.
4. Базовые требования безопасности и их структуру, функциональные требования и требования доверия.
5. Международные стандарты информационной безопасности и руководящих документах Гостехкомиссии России.

6. Основные положения Единых критериев.

7. Концепция информационной безопасности.

8.Организация функционирования комплексных систем защиты информации.

9.Информационная безопасность экономических систем. Особенности сертификации и стандартизации криптографических услуг.

5.3. Содержание тем лабораторных (практических) занятий

Тема 1. Понятие информационной безопасности и защищенной системы.

1. Сформулировать основные понятия информационной безопасности.
2. Перечислить и охарактеризовать случайные угрозы.
3. Дать общую характеристику преднамеренных угроз.
4. Определить особенности несанкционированного доступа к информации.
5. Перечислить виды возможных нарушений информационной системы.
6. Составить перечень требований безопасности, отображенных в краткой спецификации в составе задания по безопасности.
7. Произвести оценку создания более безопасных продуктов ИТ по направлениям.
8. Назвать особенности такого вида угроз как вредительские программы.
9. Охарактеризовать особенности угроз безопасности информации, связанных с несанкционированной модификацией структур КС.

Тема 2. Основные положения теории информационной безопасности информационных систем.

1. Знать основные положения теории информационной безопасности информационных систем.
2. Дать классификацию видов и свойств вирусов.
3. Иметь представления о вредительских программах и их особенностях.
4. Знать технические и программные способы защиты от вирусов.
5. Перечислить основные типы политики безопасности управления доступом к данным.
6. Перечислить виды возможных нарушений информационной системы.
7. Иметь представление об особенностях защиты информационных систем.
8. Знать основные нормативные руководящие документы, касающиеся государственной тайны и нормативно справочные документы.
9. Системы с закрытым и открытым ключом

Тема 3. Общее представление о структуре защищенной информационной системы.

1. Сформулировать принципы построения комплексных систем защиты информации.
2. Провести анализ концепции создания защищенных КС.
3. Назвать виды и способы защиты от несанкционированного проникновения в систему.
4. Программное обеспечения защиты компьютерных систем.
5. Дать определения идентификации и аутентификации и различные виды

схем аутентификации.

6. Знать механизмы доступа данных в операционных системах, системах управления базами данных.

7. Способы защиты данных и сервисов от воздействия вредоносных программ.

8. Методы и средства шифрования и дешифровки.

9. Кодирования и средства защиты при шифровании данных.

10. Использование защищенных компьютерных систем.

11. Дать определение политики безопасности.

12. Знать основные этапы разработки защищенной системы.

Тема 4. Роль стандартов информационной безопасности.

1. Удаленный доступ к файлам, защищенным путем криптографии.
2. Методика защиты компьютерных систем.
3. Основные технологии построения защищенных ЭИС.

4. Сформулировать базовые требования безопасности и их структуру, функциональные требования и требования доверия.

5. Иметь представление о международных стандартах информационной безопасности и руководящих документах Гостехкомиссии России.

6.Создать классификацию показателей защищенности средств вычислительной техники от НСД.

7. Представить в виде таблицы классы защищенности автоматизированных систем.

8. Основные положения Единых критериев.

9. Концепция информационной безопасности.

10.Организация функционирования комплексных систем защиты информации.

11.Информационная безопасность экономических систем. Определить особенности сертификации и стандартизации криптографических услуг.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (ПО МОДУЛЮ)

Самостоятельная работа студентов по дисциплине «Информационная безопасность» подразумевает применение следующих форм:

- самостоятельная работа во время основных аудиторных занятий;
- самостоятельная работа во внеаудиторное время.

1. Самостоятельная работа во время основных аудиторных занятий:

- во время лекций предполагается предоставление студентам возможности формулировать и излагать вопросы преподавателю, а также комментировать и дополнять предлагаемый преподавателем материал;
- во время семинара студент может задавать направление обсуждаемым проблемам, предложить собственный вариант проведения семинара, активно участвовать в дискуссии, выступить с самостоятельно подготовленным материалом, подготовить реферат;

- на практическом занятии самостоятельная работа заключается в решении задач, предложенных в качестве дополнительного задания, выполнении тестовых заданий, упражнений, контрольных работ.

2. Самостоятельная работа во внеаудиторное время:

- написание рефератов, представляющих собой самостоятельное изучение и краткое изложение содержания учебной и дополнительной литературы по определенной преподавателем или выбранной студентом теме;
- подготовка дополнительных вопросов к семинару, не вошедших в лекционный материал;
- выполнение домашних контрольных работ, включающих тестовые задания, упражнения, задачи и пр.;
- выполнение заданий творческого характера (например, написание эссе по какой-либо проблеме, анализ практической ситуации, и пр.).

Самостоятельное изучение дисциплины

Раздел, тема учебной дисциплины, вопросы для самостоятельного изучения	**Форма контроля**
Тема 1. Понятие информационной безопасности и защищенной системы 1. Сформулировать основные понятия информационной безопасности. 2. Перечислить и охарактеризовать случайные угрозы. 3. Дать общую характеристику преднамеренных угроз. 4. Определить особенности несанкционированного доступа к информации. 5. Перечислить виды возможных нарушений информационной системы. 6. Составить перечень требований безопасности, отображенных в краткой спецификации в составе задания по безопасности. 7. Произвести оценку создания более безопасных продуктов ИТ по направлениям. 8. Назвать особенности такого вида угроз как вредительские программы. Охарактеризовать особенности угроз безопасности информации, связанных с несанкционированной модификацией структур КС. *Тема 2. Основные положения теории информационной безопасности информационных систем.* 1. Знать основные положения теории информационной безопасности информационных систем. 2. Дать классификацию видов и свойств вирусов. 3. Иметь представления о вредительских программах и их особенностях. 4. Знать технические и программные способы защиты от вирусов. 5. Перечислить основные типы политики безопасности управления доступом к данным.	Устный опрос, доклад, собеседование, контрольная работа

6. Перечислить виды возможных нарушений информационной системы. 7. Иметь представление об особенностях защиты информационных систем. 8. Знать основные нормативные руководящие документы, касающиеся государственной тайны и нормативно-справочные документы. Системы с закрытым и открытым ключом. *Тема 3. Общее представление о структуре защищенной информационной системы.* 1. Сформулировать принципы построения комплексных систем защиты информации. 2. Провести анализ концепции создания защищенных КС. 3. Назвать виды и способы защиты от несанкционированного проникновения в систему. 4. Программное обеспечения защиты компьютерных систем. 5. Дать определения идентификации и аутентификации и различные виды схем аутентификации. 6. Знать механизмы доступа данных в операционных системах, системах управления базами данных. 7. Способы защиты данных и сервисов от воздействия вредоносных программ. 8. Методы и средства шифрования и дешифровки. 9. Кодирования и средства защиты при шифровании данных. 10.Использование защищенных компьютерных систем. 11.Дать определение политики безопасности. 12.Знать основные этапы разработки защищенной системы. *Тема 4. Роль стандартов информационной безопасности.* 1. Удаленный доступ к файлам, защищенным путем криптографии. 2. Методика защиты компьютерных систем. 3. Основные технологии построения защищенных ЭИС. 4. Сформулировать базовые требования безопасности и их структуру, функциональные требования и требования доверия. 5. Иметь представление о международных стандартах информационной безопасности и руководящих документах Гостехкомиссии России. 6. Создать классификацию показателей защищенности средств 7. вычислительной техники от НСД. 8. Представить в виде таблицы классы защищенности автоматизированных систем. 9. Основные положения Единых критериев. 10.Концепция информационной безопасности. 11.Организация функционирования комплексных систем защиты информации.	

12.Информационная безопасность экономических систем. 13.Определить особенности сертификации и стандартизации криптографических услуг.	

Примерные темы рефератов

1. Подготовка концепции информационной безопасности фирмы.

2. Создание нормативно-правовых документов деятельности фирмы на базе российского законодательства в сфере информационного права.

3.Подготовка описания охраняемой информации, «портрета» нарушителя, модели угроз, дизайн модели информационной безопасности.

4.Гарантия разработки параметров защищенности программных и информационных ресурсов компании.

5. Разработка стратегической и тактических политик ИБ фирмы.

6. Гарантия подготовки нормативного документа (стандарта предприятия) для введения в действие политик ИБ.

7. Гарантия описания структуры информационных рисков, синтез модели оценки рисков.

8. Гарантия составления списка мероприятий для уменьшения информационных рисков.

9. Гарантия обзора программных продуктов для снижения информационных рисков.

10. Гарантия формирования опорной системы стандартов для реализации комплексной системы ИБ предприятия.

11. Гарантия выбора и внедрения средств криптографической защиты информации.

12. Гарантия формирования программно-аппаратных и технических средств защиты информационных ресурсов от внешних (внутренних) атак и вирусной опасности.

13. Построение комплексной системы информационной защиты.

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины

№ п/п	Темы дисциплины	Компетенции (код)	Оценочные средства
1	Тема 1. Понятие информационной безопасности и защищенной системы	ОК-12, ПК-10	Устный опрос, собеседования, контрольная работа
2	Тема 2. Основные положения теории информационной безопасности информационных систем	ОК-12, ПК-10	
3	Тема 3. Общее представление о структуре защищенной информационной системы	ОК-12, ПК-10	
4	Тема 4. Роль стандартов информационной безопасности	ОК-12, ПК-10	

Промежуточный контроль	Зачет

7.2. Показатели и критерии оценивания компетенций (знать, уметь, владеть; освоено, частично освоено, не освоено)

7.3. Примерные (типовые) контрольные задания или иные материалы для проведения промежуточной аттестации

Вопросы для текущего контроля успеваемости

1. Понятие угрозы?
2. Виды противников или «нарушителей»?
3. Виды возможных нарушений информационной системы?
4. Анализ угроз информационной безопасности?
5. Классификация видов угроз информационной безопасности по различным признакам.
6. Свойства информации: конфиденциальность, доступность, целостность?
7. Угроза раскрытия параметров системы, угроза нарушения конфиденциальности, угроза нарушения целостности, угроза отказа служб?
8. Понятие угрозы?
9. Виды противников или «нарушителей»?
10. Виды возможных нарушений информационной системы?
11. Анализ угроз информационной безопасности?
12. Классификация видов угроз информационной безопасности по различным признакам.
13. Свойства информации: конфиденциальность, доступность, целостность?
14. Угроза раскрытия параметров системы, угроза нарушения конфиденциальности, угроза нарушения целостности, угроза отказа служб**?**
15. Примеры реализации угроз информационной безопасности?
16. Защита информации?
17. Основные принципы обеспечения информационной безопасности в автоматизированных системах?
18. Причины, виды и каналы утечки информации?
19. Основные положения теории информационной безопасности информационных систем?
20. Формальные модели безопасности их значение для построения защищенных информационных систем?
21. Понятие доступа к данным и монитора безопасности?
22. Функции монитора безопасности?
23. Понятие политики безопасности информационных систем?
24. Разработка и реализация политики безопасности?
25. Управление доступом к данным?
26. Основные типы политики безопасности управления доступом к данным: дискреционная и мандатная политика безопасности?
27. Анализ способов нарушений безопасности?
28. Таксономия нарушений информационной безопасности вычислительной

системы и причины, обуславливающие их существование?

29. Методы криптографии?
30. Средства криптографической защиты информации (СКЗИ)?
31. Криптографические преобразования?
32. Шифрование и дешифрование информации?
33. Причины нарушения безопасности информации при ее обработке СКЗИ?
34. Использование криптографических средств для решения задач идентификация и аутентификация?
35. Электронная цифровая подпись (ЭЦП), принципы ее формирования и использования?
36. Подтверждение подлинности объектов и субъектов информационной системы?
37. Контроль за целостностью информации?
38. Хэш-функции, принципы использования хэш-функций для обеспечения целостности данных?
39. Общее представление о структуре защищенной информационной системы?
40. Особенности современных информационных систем, факторы, влияющие на безопасность информационной системы?
41. Понятие информационного сервиса безопасности?
42. Виды сервисов безопасности?
43. Идентификация и аутентификация?
44. Парольные схемы аутентификации?
45. Симметричные схемы аутентификации субъекта?
46. Несимметричные схемы аутентификации (с открытым ключом)?
47. Аутентификация с третьей доверенной стороной (схема Kerberos)?
48. Токены, смарт-карты, их применение?
49. Использование биометрических данных при аутентификации пользователей?
50. Сервисы управления доступом?
51. Механизмы доступа данных в операционных системах, системах управления базами данных?
52. Ролевая модель управления доступом?
53. Протоколирование и аудит?
54. Задачи и функции аудита?
55. Структура журналов аудита?
56. Активный аудит, методы активного аудита?
57. Обеспечение защиты корпоративной информационной среды от атак на информационные сервисы?
58. Защита Интернет-подключений, функции и назначение межсетевых экранов?
59. Понятие демилитаризованной зоны?
60. Виртуальные частные сети (VP№), их назначение и использование в корпоративных информационных системах?
61. Защита данных и сервисов от воздействия вредоносных программ?
62. Вирусы, троянские программы?

63. Антивирусное программное обеспечение?
64. Защита системы электронной почты?
65. Спам, борьба со спамом?
66. Использование защищенных компьютерных систем?
67. Общие принципы построения защищенных систем?
68. Иерархический метод разработки защищенных систем?
69. Структурный принцип?
70. Принцип модульного программирования?
71. Исследование корректности реализации и верификации автоматизированных систем?
72. Спецификация требований предъявляемых к системе?
73. Основные этапы разработки защищенной системы: проектирование модели ИС, разработка кода ИС.
74. Роль стандартов информационной безопасности?
75. Квалификационный анализ уровня безопасности?
76. Критерии безопасности компьютерных систем министерства обороны США (“Оранжевая книга”)?
77. Базовые требования безопасности: требования политики безопасности, требования подотчетности (аудита), требования корректности?
78. Классы защищенности компьютерных систем?
79. Интерпретация и развитие Критериев безопасности?
80. Структура требований безопасности?
81. Основные положения концепции защиты средств вычислительной техники от несанкционированного доступа (НСД) к информации?
82. Показатели защищенности средств вычислительной техники от НСД?
83. Классы защищенности автоматизированных систем?
84. Международные стандарты информационной безопасности?
85. Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий» («Единые критерии»)?
86. Основные положения Единых критериев?
87. Функциональные требования и требования доверия?
88. Понятие Профиля защиты и Проекта защиты?
89. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы?
90. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства?
91. Особенности сертификации и стандартизации криптографических услуг?
92. Законодательная база информационной безопасности?
93. Место информационной безопасности экономических систем в национальной безопасности страны?
94. Концепция информационной безопасности?

Вопросы для рубежного контроля успеваемости

1. Какие физические процессы лежат в основе появления побочных электромагнитных излучений и наводок?

2. Охарактеризуйте особенности угроз безопасности информации, связанных с несанкционированной модификацией структур КС.

3. Продемонстрируйте на примерах особенности такого вида угроз как вредительские программы.

4. Представьте классификацию видов возможных нарушений информационной системы.

5. Защита информационных систем.

6. Критерии оценки процессов проектирования и правовой базы.

7. Особенности требований безопасности, отображенных в краткой спецификации в составе задания по безопасности.

8. Модель разработки ОО.

9. Оценка создания более безопасных продуктов ИТ по направлениям.

10. Понятия о видах вирусов.

11. Свойство вирусов.

12. Вредительские программы.

13. Способы защита от вирусов технические.

14. Способы защита от вирусов программные.

15. Вида возможных нарушений информационной системы.

16. Защита информационных систем.

17. Основные нормативные руководящие документы, касающиеся государственной тайны.

18. Нормативно-справочные документы.

19. Системы с закрытым и открытым ключом.

20. Основные нормативные руководящие документы, касающиеся государственной тайны.

21. Нормативно-справочные документы.

22. Построение комплексных систем защиты информации.

23. Концепция создания защищенных КС.

24. Виды и способы защиты от проникновения в систему.

25. Программное обеспечение защиты компьютерных систем.

26. Модели безопасности и их применение.

27. Модели безопасности и их применение.

28. Методы защиты информации, с использованием голографии.

29. Методы и средства шифрования и дешифровки.

30. Кодирования и средства защиты при шифровании данных.

31. Использование защищенных компьютерных систем.

32. Удаленный доступ к криптографически защищенным файлам.

33. Методика защиты компьютерных систем.

34. Основные технологии построения защищенных ЭИС.

35. Концепция информационной безопасности.

36. Основные технологии построения защищенных ЭИС.

37. Концепция информационной безопасности.

38. Организация функционирования комплексных систем защиты информации.

39. Информационная безопасность экономических систем.

40. Основные положения национальной безопасности страны.

7.4. Перечень вопросов к зачету

1. Сервисы безопасности.
2. Информационная безопасность в Интернете.
3. Концепция информационной войны.
4. Подделка информации. Компьютерные преступления.
5. Угрозы компьютерной безопасности.
6. Политика информационной безопасности.
7. Сетевые аспекты информационной безопасности.
8. Клавиатурные шпионы.
9. Резервное копирование данных.
10. Виды информационных посягательств.
11. Устройства противодействия съему данных. Скремблеры.
12. Комплексная система информационной безопасности.
13. Работа с конфиденциальной информацией.
14. Методы обеспечения информационной безопасности.
15. Обеспечение защиты информационных систем.
16. Организационные меры защиты информации.
17. Аппаратные средства защиты информации.
18. Программные средства защиты информации.
19. Способы идентификации личности пользователей.
20. Повышение уровня контроля за посягательствами.
21. Аутентификация в информационных системах.
22. Безопасность информационных ресурсов.
23. Классификация нарушений ИБ информационных систем (ИС).
24. Анализ нарушений информационной безопасности.
25. Основные приемы построения защищенных ИС.
26. ИБ в условиях глобальных сетей.
27. Устройства защиты помещений от прослушивания.
28. Основные виды закладных устройств.
29. Телефонные и компьютерные закладки.
30. Проводные устройства противодействия.
31. Законодательные акты по защите информации.

7.5. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Знания, умения, навыки студента на зачете оцениваются оценками: «зачтено», «не зачтено».

Основой для определения оценки служит уровень усвоения студентами материала, предусмотренного данной рабочей программой

Оценивание студента на зачете по дисциплине (модулю)

Оценка зачета	Требования к знаниям

(стандартная)	
«зачтено» («компетенции освоены»)	Оценка «зачтено» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения.
«не зачтено» («компетенции не освоены»)	Оценка «не зачтено» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. Как правило, оценка «не зачтено» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

8. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ УЧЕБНАЯ ЛИТЕРАТУРА, НЕОБХОДИМАЯ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

а) нормативные правовые акты

Доктрина информационной безопасности Российской Федерации (утверждена 9 сентября 2000 года Президентом Российской Федерации)

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне»

Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»

ISO 27000 - Международные стандарты управления информационной безопасностью.

ГОСТ РФ - Национальные стандарты Российской Федерации в области защиты информации

а) основная литература

1. Барабанова М.И., Кияев В.И. Информационные технологии: открытые системы, сети, безопасность в системах и сетях. Учебное пособие.- СПб, изд-во СПбГУЭФ, 2010. - 270 с.

2. Партыка Т.П., Попов И.И. Информационная безопасность.- М.: ФОРУМ, 2010. - 432 с.

в) дополнительная литература

1. Галатенко В.А. Основы информационной безопасности.- М.: ИНТУИТ, 2006, 208 с.

2. Черкасов В.Н. Бизнес и безопасность. Комплексный подход. М.: Армада-пресс, 2007. - 382 с.

9. РЕСУРСЫ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

При изучении дисциплины «Информационная безопасность» студентам полезно пользоваться следующими Интернет – ресурсами:

- специальные программные средства по защите информации для работы на компьютере.
- средство анализа сетевых уязвимостей X-Spider (http://www.ptsecurity.ru)
- средство оценки безопасности Microsoft Security Assessment Tool (http://technet.microsoft.com)
- http://citforum.ru/security/
- http://dehack.ru/
- http://ispdn.ru/ www.itpc.ru
- http://itsecblog.ru/organizacionnaya-zashhita/
- http://nf-bez.ru www.zki.infosec.ru/
- http://www.academy.fsb.ru/
- http://www.bezopasnik.org/
- http://www.iso27000.ru

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Приступая к изучению дисциплины, студенту необходимо ознакомиться с тематическим планом занятий, списком рекомендованной учебной литературы. Следует уяснить последовательность выполнения индивидуальных учебных заданий, занести в свою рабочую тетрадь темы и сроки проведения семинаров, написания учебных и творческих работ.

При изучении дисциплины студенты выполняют следующие задания: изучают рекомендованную учебную и научную литературу; пишут контрольные работы, готовят доклады и сообщения к практическим занятиям; выполняют самостоятельные творческие работы, участвуют в выполнении практических заданий.

Уровень и глубина усвоения дисциплины зависят от активной и систематической работы на лекциях, изучения рекомендованной литературы, выполнения контрольных письменных заданий.

Лекции - форма учебного занятия, цель которого состоит в рассмотрении теоретических вопросов излагаемой дисциплины в логически выдержанной форме.

В состав учебно-методических материалов лекционного курса включаются:

- учебники и учебные пособия, в том числе разработанные преподавателями кафедры, конспекты (тексты, схемы) лекций в печатном виде и /или электронном представлении - электронный учебник, файл с содержанием материала, излагаемого на лекциях, файл с раздаточными материалами;
- тесты и задания по различным темам лекций (разделам учебной дисциплины) для самоконтроля студентов;
- списки учебной литературы, рекомендуемой студентам в качестве основной и дополнительной по темам лекций (по соответствующей дисциплине).

Практические занятия – одна из форм учебного занятия, направленная на развитие самостоятельности учащихся и приобретение умений и навыков практической деятельности.

Особая форма практических занятий – лабораторные занятия, направленные на экспериментальное подтверждение теоретических положений и формирование учебных и профессиональных практических умений. В процессе лабораторной работы студенты выполняют одно или несколько лабораторных заданий, под руководством преподавателя в соответствии с изучаемым содержанием учебного материала.

Семинары – составная часть учебного процесса, групповая форма занятий при активном участии студентов. Семинары способствуют углублённому изучению наиболее сложных проблем науки и служат основной формой подведения итогов самостоятельной работы студентов. На семинарах студенты учатся грамотно излагать проблемы, свободно высказывать свои мысли и суждения, рассматривают ситуации, способствующие развитию профессиональной компетентности. Следует иметь в виду, что подготовка к семинару зависит от формы, места проведения семинара, конкретных заданий и поручений. Это может быть написание доклада, эссе, реферата (с последующим их обсуждением), коллоквиум.

Учебно-методические материалы практических (семинарских) занятий включают:

А) Методические указания по подготовке практических/ семинарских занятий, содержащие:

- план проведения занятий с указанием последовательности рассматриваемых тем занятий, объема аудиторных часов, отводимых для освоения материалов по каждой теме;
- краткие теоретические и УММ по каждой теме, позволяющие студенту ознакомиться с сущностью вопросов, изучаемых на практических/лабораторных семинарских занятиях, со ссылками на дополнительные УММ, которые позволяют изучить более глубоко рассматриваемые вопросы;
- вопросы, выносимые на обсуждение и список литературы с указанием конкретных страниц, необходимый для целенаправленной работы студента в ходе подготовки к семинару (список литературы оформляется в соответствии с правилами библиографического описания);
- тексты ситуаций для анализа, заданий, задач и т.п., рассматриваемых на занятиях. Практические занятия рекомендуется проводить и с использованием деловых ситуаций для анализа (case-study method).

Б) Методические указания для преподавателей, ведущих практические/ семинарские занятия, определяющие методику проведения занятий, порядок решения задач, предлагаемых студентам, варианты тем рефератов и организацию их обсуждения, методику обсуждения деловых ситуаций для анализа.

Методические указания по организации самостоятельной работы

Самостоятельная работа студентов - способ активного, целенаправленного приобретения студентом новых для него знаний и умений без непосредственного участия в этом процессе преподавателей. Повышение роли самостоятельной работы студентов при проведении различных видов учебных занятий предполагает:

- оптимизацию методов обучения, внедрение в учебный процесс новых технологий обучения, повышающих производительность труда преподавателя, активное использование информационных технологий, позволяющих студенту в удобное для него время осваивать учебный материал;
- широкое внедрение компьютеризированного тестирования;
- совершенствование методики проведения практик и научно-исследовательской работы студентов, поскольку именно эти виды учебной работы студентов в первую очередь готовят их к самостоятельному выполнению профессиональных задач;
- модернизацию системы курсового и дипломного проектирования, которая должна повышать роль студента в подборе материала, поиске путей решения задач.

Предметно и содержательно самостоятельная работа студентов определяется образовательным стандартом, рабочими программами учебных дисциплин, содержанием учебников, учебных пособий и методических руководств.

Для успешного самостоятельного изучения материала сегодня используются различные средства обучения, среди которых особое место занимают информационные технологии разного уровня и направленности: электронные учебники и курсы лекций, базы тестовых заданий и задач.

Электронный учебник представляет собой программное средство, позволяющее представить для изучения теоретический материал, организовать апробирование, тренаж и самостоятельную творческую работу, помогающее студентам и преподавателю оценить уровень знаний в определенной тематике, а также содержащее необходимую справочную информацию. Электронный учебник может интегрировать в себе возможности различных педагогических программных средств: обучающих программ, справочников, учебных баз данных, тренажеров, контролирующих программ.

Для успешной организации самостоятельной работы все активнее применяются разнообразные образовательные ресурсы в сети Интернет: системы тестирования по различным областям, виртуальные лекции, лаборатории, при этом пользователю достаточно иметь компьютер и подключение к Интернету для того, чтобы связаться с преподавателем, решать вычислительные задачи и получать знания. Использование сетей усиливает роль самостоятельной работы студента и позволяет кардинальным образом изменить методику преподавания. Студент может получать все задания и методические указания через сервер, что дает ему возможность привести в соответствие личные возможности с необходимыми для выполнения работ трудозатратами. Студент имеет возможность выполнять работу дома или в аудитории.

Большое воспитательное и образовательное значение в самостоятельном учебном труде студента имеет самоконтроль. Самоконтроль возбуждает и поддерживает внимание и интерес, повышает активность памяти и мышления, позволяет студенту своевременно обнаружить и устранить допущенные ошибки и недостатки, объективно определить уровень своих знаний, практических умений.

Самое доступное и простое средство самоконтроля с применением информационно-коммуникационных технологий - это ряд тестов «on-line», которые позволяют в режиме реального времени определить свой уровень владения

предметным материалом, выявить свои ошибки и получить рекомендации по самосовершенствованию.

Методические указания по выполнению рефератов

Реферат представляет собой сокращенный пересказ содержания первичного документа (или его части) с основными фактическими сведениями и выводами.

Написание реферата используется в учебном процессе вуза в целях приобретения студентом необходимой профессиональной подготовки, развития умения и навыков самостоятельного научного поиска: изучения литературы по выбранной теме, анализа различных источников и точек зрения, обобщения материала, выделения главного, формулирования выводов и т. п. С помощью рефератов студент глубже постигает наиболее сложные проблемы курса, учится лаконично излагать свои мысли, правильно оформлять работу, докладывать результаты своего труда.

Процесс написания реферата включает:

- выбор темы;
- подбор нормативных актов, специальной литературы и иных источников, их изучение;
- составление плана;
- написание текста работы и ее оформление;
- устное изложение реферата.

Рефераты пишутся по наиболее актуальным темам. В них на основе тщательного анализа и обобщения научного материала сопоставляются различные взгляды авторов и определяется собственная позиция студента с изложением соответствующих аргументов.

Темы рефератов должны охватывать и дискуссионные вопросы курса. Они призваны отражать передовые научные идеи, обобщать тенденции практической деятельности, учитывая при этом изменения в текущем законодательстве. Рекомендованная ниже тематика рефератов примерная. Студент при желании может сам предложить ту или иную тему, предварительно согласовав ее с научным руководителем.

Реферат, как правило, состоит из введения, в котором кратко обосновывается актуальность, научная и практическая значимость избранной темы, основного материала, содержащего суть проблемы и пути ее решения, и заключения, где формируются выводы, оценки, предложения.

Объем реферата - от 5 до 15 машинописных страниц.

Содержание реферата студент докладывает на семинаре, кружке, научной конференции. Предварительно подготовив тезисы доклада, студент в течение 7-10 минут должен кратко изложить основные положения своей работы. После доклада автор отвечает на вопросы, затем выступают оппоненты, которые заранее познакомились с текстом реферата, и отмечают его сильные и слабые стороны. На основе обсуждения студенту выставляется соответствующая оценка.

11. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ИСПОЛЬЗУЕМЫЕ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине (модулю) включают;

- проверка заданий и консультирование посредством электронный почты;
- использование слайд-презентаций при проведении семинарских (практических) занятий.

12.МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для материально-технического обеспечения дисциплины «Информационная безопасность» необходимы следующие средства:

- компьютерные классы для работы с рабочими программами с доступом в Интернет;
- проектор, совмещенный с ноутбуком.

Отдельные лекции и лабораторные занятия проводятся с использованием вспомогательных средств: раздаточных материалов, слайдов, мультимедийных презентаций.

13. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В соответствии с требованиями ФГОС ВПО реализация компетентностного подхода предусматривает использование в учебном процессе традиционных, активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой студентов.

По учебной дисциплине «Информационная безопасность» предусмотрены следующие образовательные технологии. Причем проведение занятий в рамках этих технологий может осуществляться как в традиционной, так и в активной и интерактивной формах:

- лекции (эвристического характера, проблемная, с элементами дискуссии);
- активные / интерактивные формы (на всех практических и семинарских занятиях);
- практические занятия;
- семинарские занятия;
- обсуждение вариантов решений проблемных задач и конкретных жизненных и профессиональных ситуаций в ходе семинаров и практических занятий (на всех занятиях);
- выполнение тестовых заданий;
- самостоятельная работа;
- подготовка и сдача зачета;
- написание рефератов и письменных работ.

Важной формой углубленного изучения конкретных проблем учебной дисциплины «Электронная торговля» для студентов при самостоятельном изучении тем и разделов курса, является выполнение письменной работы. Эта работа предполагает систематизацию и анализ различных источников и литературы по

этике по выбранной из перечня проблеме. Письменная работа предусматривает собственное осмысление студентами избранной проблемы и изложение своих мыслей в письменной форме. Она выполняется учащимся самостоятельно, оформляется должным образом и считается одним из элементов учебной работы по самостоятельному освоению курса «Электронная торговля».

Важной составляющей профессионально - этического образования является овладение категориальным аппаратом. Незнание категорий препятствует усвоению знаний по морально – этическим проблемам. При изучении профессиональной этики обучаемым оказывается помощь в виде разнообразных форм учебной работы. Таковыми являются консультации, лекции, семинары, практические занятия, индивидуальные контрольные собеседования и др.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью программы, особенность контингента обучающегося и содержанием конкретных дисциплин, и в целом в учебном процессе они должны составлять не менее 20 % аудиторных занятий.

Программа составлена в соответствии с требованиями ФГОС ВПО с учетом рекомендаций и ООП ВО по направлению подготовки 38.03.01. – «Экономика».

Составитель: к. техн. н., доцент Мехтиев М.А.
Рецензент: к. пед. н., доцент Гюльмагомедов Т.Х.

Программа рассмотрена и одобрена на заседании Ученого совета филиала от 27.02.2015 г., протокол № 05.