Автономная некоммерческая организация
высшего образования
«Институт непрерывного образования»

Рассмотрено
на заседании кафедры экономики и управления
(протокол от 28.08.2017 г. № 1)
Зав. кафедрой
_____ Коробко В.И.
28 августа 2017 г.

УТВЕРЖДАЮ:

Ректор АНО ВО «ИНО»
_____ Цветлюк Л.С.
29 августа 2017 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Информационная безопасность
для направления подготовки
38.03.01 «Экономика»,
профиль (направленность) «Бухгалтерский учет, анализ и аудит»

Уровень бакалавриата

Квалификация выпускника
Бакалавр

Очная, очно-заочная, заочная формы обучения

Рабочая программа учебной дисциплины «Информационная безопасность» разработана доц. к.т.н. Трубицыным А.С.

Руководитель основной
профессиональной
образовательной программы
_____ к.э.н., доц. Бодрова Е.Е
(подпись)

Москва, 2017 г

Рабочая программа учебной дисциплины «**Информационная безопасность**» разработана на основании федерального государственного образовательного стандарта высшего образования по направлению подготовки **38.03.01 Экономика (уровень бакалавриата)**, утвержденного приказом Министерства образования и науки Российской Федерации от 12 ноября 2015 г. №1327, учебного плана по основной профессиональной образовательной программе высшего образования «**Экономика**».

Рабочая программа учебной дисциплины рекомендована к утверждению представителями организаций-работодателей

Управление финансов и государственных закупок аппарата Московской областной Думы	Руководитель Мун Е.А.
_____ (подпись)	

СОДЕРЖАНИЕ

1. Общие положения 5
1.1 Цель и задачи дисциплины 5
1.2 Место учебной дисциплины в структуре основной профессиональной образовательной программы. 6
1.3. Планируемые результаты обучения по учебной дисциплине в рамках планируемых результатов освоения основной профессиональной образовательной программы. 6
2. Объем учебной дисциплины, включая контактную работы обучающегося с преподавателем и самостоятельную работу обучающегося 7
Очная форма обучения 7
Очно-заочная форма обучения 7
Заочная форма обучения 7
3. Содержание учебной дисциплины 8
3.1. Учебно-тематический план по очной форме обучения 8
3.2. Учебно-тематический план по очно-заочной форме обучения 10
3.3. Учебно-тематический план по заочной форме обучения 12
4. Учебно-методическое обеспечение самостоятельной работы обучающихся по учебной дисциплине 13
Тема 1. Международные стандарты информационного обмена. Понятие угрозы. 13
Тема 2 Информационная безопасность в условиях функционирования в России глобальных сетей. Виды противников или «нарушителей». 14
Тема 3. Три вида возможных нарушений информационной системы. Защита. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. 15
Тема 4. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. 15
Тема 5. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. 16
Тема 6. Концепция информационной безопасности. 17
Тема 7. Основные технологии построения защищенных ЭИС. Место информационной безопасности экономических систем в национальной безопасности страны. 18
Тема 8 Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем. Методы криптографии. 19
5. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по учебной дисциплине 19
5.1. Форма промежуточной аттестации обучающегося по учебной дисциплине. 19
5.2. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы. 19
5.3. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания 20
5.4. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы 24

5.5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций....34
6. Перечень основной и дополнительной учебной литературы для освоения учебной дисциплины....35
6.1. Основная литература....35
6.1 Дополнительная литература по дисциплине: 35
7. Перечень ресурсов информационно-коммуникационной сети «Интернет», необходимых для освоения учебной дисциплины 35
8. Методические указания для обучающихся по освоению учебной дисциплины 35
9. Информационно-технологическое обеспечение образовательного процесса по учебной дисциплине....37
9.1. Информационные технологии....37
9.2. Программное обеспечение....37
9.3. Информационные справочные системы....37
10. Материально-техническое обеспечение образовательного процесса по учебной дисциплине....37
11. Образовательные технологии....37

1. Общие положения

1.1 Цель и задачи дисциплины

Цель учебной дисциплины заключается ознакомлении студентов с современными системами информационной безопасности, технологическими способами защиты информации, организационными мерами по информационной защите, экономическими и правовыми принципами их функционирования, а также возможностями использования защиты в работе с информационными ресурсами в различных областях экономики и бизнеса.

Задачи учебной дисциплины:

В результате изучения дисциплины обучающийся должен:

знать:

- современную научную парадигму информационной безопасности;
- организационно-правовые основы защиты информационных ресурсов предприятия;
- теоретические и практические знания по правовым основам защиты информации при работе на вычислительной технике и в каналах связи;
- модели, стратегии, систем и технологических основ комплексного обеспечения информационной безопасности;
- вопросы правового и организационного обеспечения информационной безопасности;
- о концепции информационной безопасности;
- содержание основных понятий обеспечения информационной безопасности;
- источники угроз безопасности информации;
- методы оценки уязвимости информации;
- методы создания, организации и обеспечения функционирования систем комплексной защиты информации;
- методы пресечения разглашения конфиденциальной информации;
- виды и признаки компьютерных преступлений, особенности основных следственных действий при расследовании указанных преступлений.

уметь:

- решать вопросы в сфере обеспечения информационной безопасности;
- применить практические навыки и способности по осуществлению мероприятий по обеспечению информационной безопасности компьютерных сетей;
- использовать методы и средства защиты данных;
- выполнять анализ способов нарушений информационной безопасности;
- отыскивать необходимые нормативные правовые акты и информационные правовые нормы в системе действующего законодательства, в том числе с помощью систем правовой информации;
- применять действующую законодательную базу в области информационной безопасности;
- разрабатывать проекты положений, инструкций и других организационно-распорядительных документов, регламентирующих работу по защите информации

владеть:

- криптографическими, программно-аппаратными и техническими методами и средствами защиты информации;
- методами криптографической защиты;
- основными технологиями построения защищенных ЭИС;

- основными понятиями безопасности информации;
- средствами обеспечения информационной безопасностью

1.2 Место учебной дисциплины в структуре основной профессиональной образовательной программы.

Учебная дисциплина **«Информационная безопасность»** реализуется в **вариативной части** профессионального модуля и относится к дисциплинам по выбору профессиональной образовательной программы «**Экономика**» по направлению подготовки 38.03.01 Экономика (уровень бакалавриата), очной, очно-заочной, заочной форм обучения.

Изучение учебной дисциплины **«Информационная безопасность»** является заключительным модулем логически завершающим освоение современных информационных технологий рассмотренных в рамках учебной дисциплины «Информатика и информационные технологии в экономике».

1.3. Планируемые результаты обучения по учебной дисциплине в рамках планируемых результатов освоения основной профессиональной образовательной программы.

Процесс освоения учебной дисциплины направлен на формирование у обучающихся следующих компетенций: ОПК-1; ПК-10.

В результате освоения дисциплины студент должен демонстрировать следующие результаты образования:

Код компетенции	Содержание компетенции	Результаты обучения
ОПК-1	способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**знать:** способы защиты информации по средствам технических средств и информационных технологий;
		уметь: творчески применять знание современных методов защиты информации, используя отечественные и зарубежные программные и аппаратные средства;
		владеть: навыками защиты информации и противодействия хищению информации представляющей частную и корпоративную ценность
ПК-10	способность использовать для решения коммуникативных задач современные технические средства и информационные технологии	**знать:** способы защиты информации по средствам технических средств и информационных технологий
		уметь: использовать для решения коммуникативных задач современные технические средства и информационные технологии
		владеть: современными техническими средствами и информационными технологиями

2. Объем учебной дисциплины, включая контактную работы обучающегося с преподавателем и самостоятельную работу обучающегося

Общая трудоемкость учебной дисциплины составляет **3** зачетных единиц.

Очная форма обучения

Вид учебной работы	Всего зачетных единиц	Семестры
		6
Аудиторные учебные занятия, всего	**1,5**	
В том числе:		
Учебные занятия лекционного типа	0,5	
Учебные занятия семинарского типа	1	
Лабораторные занятия		
Самостоятельная работа обучающихся, всего	**1,5**	
В том числе:		
Индивидуальные и групповые проекты, в том числе курсовые		
Контрольная работа, РГР, РПР, др. письменные работы	0,5	
Рефераты, эссе, др. творческие работы		
Другие виды самостоятельной работы:		
Практические задания	1	
Вид промежуточной аттестации (зачет, экзамен)		**Зачет**
Общая трудоемкость учебной дисциплины	3	

Очно-заочная форма обучения

Вид учебной работы	Всего зачетных единиц	Семестры
		6
Аудиторные учебные занятия, всего	**0,72**	
В том числе:		
Учебные занятия лекционного типа	0,22	
Учебные занятия семинарского типа	0,5	
Лабораторные занятия		
Самостоятельная работа обучающихся, всего	**2,28**	
В том числе:		
Индивидуальные и групповые проекты, в том числе курсовые		
Контрольная работа, РГР, РПР, др. письменные работы	0,78	
Рефераты, эссе, др. творческие работы		
Другие виды самостоятельной работы:		
Практические задания	1,5	
Вид промежуточной аттестации (зачет, экзамен)		**Зачет**
Общая трудоемкость учебной дисциплины	3	

Заочная форма обучения

Вид учебной работы	Всего зачетных	Курс
		3

	единиц	
Аудиторные учебные занятия, всего	**0,28**	
В том числе:		
Учебные занятия лекционного типа	0,06	
Учебные занятия семинарского типа	0,22	
Лабораторные занятия		
Самостоятельная работа обучающихся, всего	**2,61**	
В том числе:		
Индивидуальные и групповые проекты, в том числе курсовые		
Контрольная работа, РГР, РПР, др. письменные работы	0,61	
Рефераты, эссе, др. творческие работы		
Другие виды самостоятельной работы:		
Практические задания	2	
Вид промежуточной аттестации (зачет, экзамен)	**0,11**	**Зачет**
Общая трудоемкость учебной дисциплины	3	

3. Содержание учебной дисциплины

3.1. Учебно-тематический план по очной форме обучения

Объем аудиторных занятий составляет 54ч.
Объем самостоятельной работы – 54 ч.

№ п/п	Модуль, раздел (тема)	Виды учебной работы, академических часов						Формы контроля освоения обучающимися учебной дисциплины, рейтинговых баллов						
		Всего	Самостоятельная работа обучающегося	Контактная работа преподавателя с обучающимися				Текущий контроль освоения обучающимися учебной дисциплины					Промежуточная аттестация обучающихся	
				Всего	Лекционного типа	Семинарского типа	Лабораторные занятия	Работа на учебных занятиях семинарского типа	Индивидуальные и групповые проекты, в том числе курсовые	Контрольная работа, РГР, РПР, др. письменные работы	Рефераты, эссе, др. творческие работы	Другие виды	Зачет	Экзамен
1	Тема 1. Международные стандарты информационного обмена. Понятие угрозы.	13	5	8	4	4		+		+		+		
2	Тема 2 Информационная безопасность в	13	7	6	2	4		+		+		+		

	условиях функционирования в России глобальных сетей. Виды противников или «нарушителей».													
3	Тема 3. Три вида возможных нарушений информационной системы. Защита. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.	13	7	6	2	4		+		+		+		
4	Тема 4. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.	13	7	6	2	4		+		+		+		
5	Тема 5. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.	14	8	6	2	4		+		+		+		
6	Тема 6. Концепция информационной безопасности.	14	8	6	2	4		+		+		+		
7	Тема 7. Основные технологии построения защищенных ЭИС. Место информационной безопасности экономических систем в национальной безопасности страны.	14	6	8	2	6		+		+		+		
8	Тема 8 Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем. Методы криптографии.	14	6	8	2	6		+		+		+		
Всего часов		**108**	**54**	**54**	**18**	**36**								

3.2. Учебно-тематический план по очно-заочной форме обучения

Объем аудиторных занятий составляет 26 ч.

Объем самостоятельной работы – 82 ч.

№ п/п	Модуль, раздел (тема)	Виды учебной работы, академических часов						Формы контроля освоения обучающимися учебной дисциплины, рейтинговых баллов						
		Всего	Самостоятельная работа обучающегося	Контактная работа преподавателя с обучающимися				Текущий контроль освоения обучающимися учебной дисциплины					Промежуточная аттестация обучающихся	
				Всего	Лекционного типа	Семинарского типа	Лабораторные занятия	Работа на учебных занятиях семинарского типа	Индивидуальные и групповые проекты, в том числе курсовые	Контрольная работа, РГР, РПР, др. письменные работы	Рефераты, эссе, др. творческие работы	Другие виды	Зачет	Экзамен
1	Тема 1. Международные стандарты информационного обмена. Понятие угрозы.	13	10	3	1	2		+		+		+		
2	Тема 2 Информационная безопасность в условиях функционирования в России глобальных сетей. Виды противников или «нарушителей».	13	10	3	1	2		+		+		+		
3	Тема 3. Три вида возможных нарушений информационной системы. Защита. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.	13	10	3	1	2		+		+		+		
4	Тема 4. Таксономия нарушений информационной безопасности	13	10	3	1	2		+		+		+		

	вычислительной системы и причины, обуславливающие их существование.													
5	Тема 5. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.	14	11	3	1	2		+		+		+		
6	Тема 6. Концепция информационной безопасности.	14	11	3	1	2		+		+		+		
7	Тема 7. Основные технологии построения защищенных ЭИС. Место информационной безопасности экономических систем в национальной безопасности страны.	14	11	3	1	2		+		+		+		
8	Тема 8 Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем. Методы криптографии.	14	9	5	1	4		+		+		+		
Всего часов		108	**82**	**26**	**8**	**18**								

3.3. Учебно-тематический план по заочной форме обучения

Объем аудиторных занятий составляет 10 ч.
Объем самостоятельной работы – 96 ч.
Контроль знаний – 4 ч.

№ п/п	Модуль, раздел (тема)	Виды учебной работы, академических часов						Формы контроля освоения обучающимися учебной дисциплины, рейтинговых баллов						
		Всего	Самостоятельная работа обучающегося	Контактная работа преподавателя с обучающимися				Текущий контроль освоения обучающимися учебной дисциплины					Промежуточная аттестация обучающихся	
				Всего	Лекционного типа	Семинарского типа	Лабораторные занятия	Работа на учебных занятиях семинарского типа	Индивидуальные и групповые проекты, в том числе курсовые	Контрольная работа, РГР, РПР, др. письменные работы	Рефераты, эссе, др. творческие работы	Другие виды	Зачет	Экзамен
1	Тема 1. Международные стандарты информационного обмена. Понятие угрозы.	13	12	1	1			+		+		+		
2	Тема 2 Информационная безопасность в условиях функционирования в России глобальных сетей. Виды противников или «нарушителей».	13	12	1	1			+		+		+		
3	Тема 3. Три вида возможных нарушений информационной системы. Защита. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.	13	12	1		1		+		+		+		
4	Тема 4. Таксономия нарушений информационной	13	12	1		1		+		+		+		

	безопасности вычислительной системы и причины, обуславливающие их существование.													
5	Тема 5. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.	13	12	1		1		+		+		+		
6	Тема 6. Концепция информационной безопасности.	13	12	1		1		+		+		+		
7	Тема 7. Основные технологии построения защищенных ЭИС. Место информационной безопасности экономических систем в национальной безопасности страны.	13	11	2		2		+		+		+		
8	Тема 8 Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем. Методы криптографии.	13	11	2		2		+		+		+		
Всего часов		**108**	**96**	**10**	**2**	**8**								**4**

4. Учебно-методическое обеспечение самостоятельной работы обучающихся по учебной дисциплине

Тема 1. Международные стандарты информационного обмена. Понятие угрозы.

Цель: сформировать компетенции: ОПК-1 - способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; ПК-10 способность использовать для решения коммуникативных задач современные технические средства и информационные технологии.

Перечень изучаемых элементов содержания учебной дисциплины:

Понятие информационной безопасности и защищенной системы. Необходимость защиты информационных систем и телекоммуникаций. Технические предпосылки кризиса информационной безопасности. Информационная безопасность в условиях функционирования в России глобальных сетей. Основные задачи обеспечения защиты информации. Основные методы и средства защиты информационных систем.

Вопросы для самоподготовки

1. В чем заключается информационная безопасность и защищенность системы.
2. Почему следует защищать информационные системы телекоммуникаций.
3. Перечислите технические предпосылки кризиса информационной безопасности.
4. Из каких элементов складывается информационная безопасность.
5. Перечислите основные задачи обеспечения защиты информации.
6. Назовите и охарактеризуйте основные методы и средства защиты информационных систем.

Формы контроля самостоятельной работы обучающихся:

проверка ответов на вопросы самоподготовки, анализ докладов, оценивание рефератов, эссе, проверка и оценивание выполнения практических заданий.

Тема 2 Информационная безопасность в условиях функционирования в России глобальных сетей. Виды противников или «нарушителей».

Цель: сформировать компетенции: ОПК-1 - способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; ПК-10 способность использовать для решения коммуникативных задач современные технические средства и информационные технологии

Перечень изучаемых элементов содержания учебной дисциплины:

Понятие угрозы. Виды противников или «нарушителей». Виды возможных нарушений информационной системы. Анализ угроз информационной безопасности. Классификация видов угроз информационной безопасности по различным признакам (по природе возникновения, степени преднамеренности и т.п.).

Свойства информации: конфиденциальность, доступность, целостность. Угроза раскрытия параметров системы, угроза нарушения конфиденциальности, угроза нарушения целостности, угроза отказа служб. Примеры реализации угроз информационной безопасности.

Защита информации. Основные принципы обеспечения информационной безопасности в автоматизированных системах. Причины, виды и каналы утечки информации.

Вопросы для самоподготовки

1. Перечислите виды противников или «нарушителей».
2. Основные виды возможных нарушений информационной системы.
3. Классификация видов угроз информационной безопасности по различным признакам (по природе возникновения, степени преднамеренности и т.п.).
4. Свойства информации: конфиденциальность, доступность, целостность.
5. Угроза раскрытия параметров системы, угроза нарушения конфиденциальности, угроза нарушения целостности, угроза отказа служб.
6. Примеры реализации угроз информационной безопасности.
7. Способы защиты информации.
8. Основные принципы обеспечения информационной безопасности в автоматизированных системах.
9. Причины, виды и каналы утечки информации.

Формы контроля самостоятельной работы обучающихся:

проверка ответов на вопросы самоподготовки, анализ докладов, оценивание рефератов, эссе, проверка и оценивание выполнения практических заданий.

Тема 3. Три вида возможных нарушений информационной системы. Защита. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.

Цель: сформировать компетенции: ОПК-1 - способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; ПК-10 способность использовать для решения коммуникативных задач современные технические средства и информационные технологии

Перечень изучаемых элементов содержания учебной дисциплины:

Основные положения теории информационной безопасности информационных систем. Формальные модели безопасности их значение для построения защищенных информационных систем. Понятие доступа к данным и монитора безопасности. Функции монитора безопасности. Понятие политики безопасности информационных систем. Разработка и реализация политики безопасности. Управление доступом к данным. Основные типы политики безопасности управления доступом к данным: дискреционная и мандатная политика безопасности. Анализ способов нарушений безопасности. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.

Вопросы для самоподготовки

1. Основные положения теории информационной безопасности информационных систем.
2. Формальные модели безопасности их значение для построения защищенных информационных систем.
3. Понятие доступа к данным и монитора безопасности.
4. Функции монитора безопасности.
5. Понятие политики безопасности информационных систем.
6. Разработка и реализация политики безопасности.
7. Управление доступом к данным.
8. Перечислите основные типы политики безопасности управления доступом к данным: дискреционная и мандатная политика безопасности.
9. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.

Формы контроля самостоятельной работы обучающихся:

проверка ответов на вопросы самоподготовки, анализ докладов, оценивание рефератов, эссе, проверка и оценивание выполнения практических заданий.

Тема 4. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.

Цель: сформировать компетенции: ОПК-1 - способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; ПК-10 способность использовать для решения коммуникативных задач современные технические средства и информационные технологии

Перечень изучаемых элементов содержания учебной дисциплины:

Методы криптографии. Средства криптографической защиты информации (СКЗИ). Криптографические преобразования. Шифрование и дешифрование информации.

Причины нарушения безопасности информации при ее обработке СКЗИ (утечки информации по техническому каналу, неисправности в элементах СКЗИ, работа

совместно с другими программами).Использование криптографических средств для решения задач идентификация и аутентификация.

Электронная цифровая подпись (ЭЦП), принципы ее формирования и использования. Подтверждение подлинности объектов и субъектов информационной системы. Контроль за целостностью информации. Хэш-функции, принципы использования хэш-функций для обеспечения целостности данных.

Вопросы для самоподготовки

1. Какие методы криптографии существую, перечислите и охарактеризуйте.
2. Основные средства криптографической защиты информации (СКЗИ).
3. Методы шифрование и дешифрование информации.
4. Основные причины нарушения безопасности информации при ее обработке
5. Электронная цифровая подпись (ЭЦП), принципы ее формирования и использования.
6. Способы подтверждения подлинности объектов и субъектов информационной системы.
7. Хэш-функции, принципы использования хэш-функций для обеспечения целостности данных.

Формы контроля самостоятельной работы обучающихся:

проверка ответов на вопросы самоподготовки, анализ докладов, оценивание рефератов, эссе, проверка и оценивание выполнения практических заданий.

Тема 5. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.

Цель: сформировать компетенции: ОПК-1 - способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; ПК-10 способность использовать для решения коммуникативных задач современные технические средства и информационные технологии

Перечень изучаемых элементов содержания учебной дисциплины:

Общее представление о структуре защищенной информационной системы. Особенности современных информационных систем, факторы влияющие на безопасность информационной системы. Понятие информационного сервиса безопасности. Виды сервисов безопасности.

Идентификация и аутентификация. Парольные схемы аутентификации. Симметричные схемы аутентификации субъекта. Несимметричные схемы аутентификации (с открытым ключом). Аутентификация с третьей доверенной стороной (схема Kerberos). Токены, смарт-карты, их применение. Использование биометрических данных при аутентификации пользователей.

Сервисы управления доступом. Механизмы доступа данных в операционных системах, системах управления базами данных. Ролевая модель управления доступом.

Протоколирование и аудит. Задачи и функции аудита. Структура журналов аудита. Активный аудит, методы активного аудита.

Обеспечение защиты корпоративной информационной среды от атак на информационные сервисы. Защита Интернет-подключений, функции и назначение межсетевых экранов. Понятие демилитаризованной зоны. Виртуальные частные сети (VPN), их назначение и использование в корпоративных информационных системах.

Защита данных и сервисов от воздействия вредоносных программ. Вирусы, троянские программы. Антивирусное программное обеспечение. Защита системы электронной почты. Спам, борьба со спамом.

Вопросы для самоподготовки

1. Особенности современных информационных систем, факторы влияющие на безопасность информационной системы.
2. Понятие информационного сервиса безопасности.
3. Виды сервисов безопасности.
4. Парольные схемы аутентификации.
5. Симметричные схемы аутентификации субъекта.
6. Несимметричные схемы аутентификации (с открытым ключом).
7. Аутентификация с третьей доверенной стороной (схема Kerberos).
8. Токены, смарт-карты, их применение.
9. Использование биометрических данных при аутентификации пользователей.
10. Механизмы доступа данных в операционных системах, системах управления базами данных.
11. Ролевая модель управления доступом.
12. Протоколирование и аудит.
13. Задачи и функции аудита.
14. Структура журналов аудита.
15. Активный аудит, методы активного аудита.
16. Обеспечение защиты корпоративной информационной среды от атак на информационные сервисы.
17. Защита Интернет-подключений, функции и назначение межсетевых экранов.
18. Понятие демилитаризованной зоны.
19. Виртуальные частные сети (VPN), их назначение и использование в корпоративных информационных системах.
20. Защита данных и сервисов от воздействия вредоносных программ.
21. Вирусы, троянские программы.
22. Антивирусное программное обеспечение.
23. Защита системы электронной почты.
24. Спам, борьба со спамом.

Формы контроля самостоятельной работы обучающихся:

проверка ответов на вопросы самоподготовки, анализ докладов, оценивание рефератов, эссе, проверка и оценивание выполнения практических заданий.

Тема 6. Концепция информационной безопасности.

Цель: сформировать компетенции: ОПК-1 - способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; ПК-10 способность использовать для решения коммуникативных задач современные технические средства и информационные технологии

Перечень изучаемых элементов содержания учебной дисциплины:

Использование защищенных компьютерных систем. Общие принципы построения защищенных систем. Иерархический метод разработки защищенных систем. Структурный принцип. Принцип модульного программирования. Исследование корректности реализации и верификации автоматизированных систем. Спецификация требований предъявляемых к системе. Основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политике безопасности.

Вопросы для самоподготовки

1. Способы использования защищенных компьютерных систем.

2. Общие принципы построения защищенных систем.
3. Иерархический метод разработки защищенных систем.
4. Спецификация требований предъявляемых к системе.
5. Основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политике безопасности.

Формы контроля самостоятельной работы обучающихся:

проверка ответов на вопросы самоподготовки, анализ докладов, оценивание рефератов, эссе, проверка и оценивание выполнения практических заданий.

Тема 7. Основные технологии построения защищенных ЭИС. Место информационной безопасности экономических систем в национальной безопасности страны.

Цель: сформировать компетенции: ОПК-1 - способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; ПК-10 способность использовать для решения коммуникативных задач современные технические средства и информационные технологии

Перечень изучаемых элементов содержания учебной дисциплины:

Роль стандартов информационной безопасности. Квалификационный анализ уровня безопасности. Критерии безопасности компьютерных систем министерства обороны США (“Оранжевая книга”). Базовые требования безопасности: требования политики безопасности, требования подотчетности (аудита), требования корректности. Классы защищенности компьютерных систем. Интерпретация и развитие Критериев безопасности.

Руководящие документы Гостехкомиссии России. Структура требований безопасности. Основные положения концепции защиты средств вычислительной техники от несанкционированного доступа (НСД) к информации. Показатели защищенности средств вычислительной техники от НСД. Классы защищенности автоматизированных систем.

Международные стандарты информационной безоапсности. Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий» («Единые критерии»). Основные положения Единых критериев. Функциональные требования и требования доверия. Понятие Профиля защиты и Проекта защиты.

Вопросы для самоподготовки

1. Критерии безопасности компьютерных систем министерства обороны США (“Оранжевая книга”).
2. Базовые требования безопасности: требования политики безопасности, требования подотчетности (аудита), требования корректности.
3. Классы защищенности компьютерных систем.
4. Интерпретация и развитие Критериев безопасности.
5. Основные положения концепции защиты средств вычислительной техники от несанкционированного доступа (НСД) к информации.
6. Показатели защищенности средств вычислительной техники от НСД.
7. Классы защищенности автоматизированных систем.
8. Международные стандарты информационной безоапсности.
9. Основные положения Единых критериев.

Формы контроля самостоятельной работы обучающихся:

проверка ответов на вопросы самоподготовки, анализ докладов, оценивание рефератов, эссе, проверка и оценивание выполнения практических заданий.

Тема 8 Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем. Методы криптографии.

Цель: сформировать компетенции: ОПК-1 - способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; ПК-10 способность использовать для решения коммуникативных задач современные технические средства и информационные технологии

Перечень изучаемых элементов содержания учебной дисциплины:

Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Особенности сертификации и стандартизации криптографических услуг. Законодательная база информационной безопасности. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.

Вопросы для самоподготовки

1. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
2. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.
3. Особенности сертификации и стандартизации криптографических услуг.
4. Законодательная база информационной безопасности.
5. Место информационной безопасности экономических систем в национальной безопасности страны.
6. Концепция информационной безопасности.

Формы контроля самостоятельной работы обучающихся:

проверка ответов на вопросы самоподготовки, анализ докладов, оценивание рефератов, эссе, проверка и оценивание выполнения практических заданий.

5. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по учебной дисциплине

5.1. Форма промежуточной аттестации обучающегося по учебной дисциплине.

Контрольными мероприятиями промежуточной аттестации обучающихся по учебной дисциплине являются зачет (6 семестр), который проводятся в устной форме.

5.2. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.

Код компетенции	Содержание компетенции	Результаты обучения	Результаты обучения
ОПК-1	способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической	Компоненты компетенции соотносятся с содержанием дисциплины, компетенция реализуется	знать: способы защиты информации по средствам технических средств и информационных технологий;
			уметь: творчески применять знание современных методов защиты информации, используя отечественные и зарубежные программные и аппаратные средства;

	культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	частично	владеть: навыками защиты информации и противодействия хищению информации представляющей частную и корпоративную ценность
ПК-10	способность использовать для решения коммуникативных задач современные технические средства и информационные технологии	Компоненты компетенции соотносятся с содержанием дисциплины, компетенция реализуется частично	знать: способы защиты информации по средствам технических средств и информационных технологий;
			уметь: творчески применять знание современных методов защиты информации, используя отечественные и зарубежные программные и аппаратные средства;
			владеть: навыками защиты информации и противодействия хищению информации представляющей частную и корпоративную ценность

5.3. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции	Этапы формирования компетенции	Инструмент, оценивающий сформированность компетенции*	Показатель оценивания компетенции	Критерии оценки
ОПК-1	Этап формирования знаниевой основы компетенций (этап формирования содержательно-теоретического базиса компетенции) Лекционные и лабораторные занятия по темам: *Тема 1. Международные стандарты информационного обмена. Понятие угрозы.* *Тема 2 Информационная безопасность в условиях функционирования в России глобальных сетей. Виды противников или «нарушителей».* *Тема 3. Три вида возможных нарушений информационной системы. Защита.* *Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные*	Реферат* Доклад* Эссе*	А) полностью сформирована - 5 баллов Б) частично сформирована - 3-4 балла С) не сформирована- 2 и менее баллов	Сумма баллов (max=5) по следующим критериям оценки: 1. Соответствие содержания реферата, доклада заявленной тематике (1 балл). 2. Владение информацией и способность отвечать на вопросы аудитории (1 балл). 3. Качество источников и их количество при подготовке работы (I балл). 4. Качество самой представленной работы, ее научная обоснованность и практическая (профессионально-

	документы. *Тема 4. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.* *Тема 5. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.* *Тема 6. Концепция информационной безопасности.* *Тема 7. Основные технологии построения защищенных ЭИС. Место информационной безопасности экономических систем в национальной безопасности страны.* *Тема 8 Анализ способов нарушений информационной безопасности.* *Использование защищенных компьютерных систем.* *Методы криптографии.*			ориентированная направленность) (1 балл). 5. Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл).
ПК-10	Этап формирования знаниевой основы компетенций (этап формирования содержательно-теоретического базиса компетенции) Лекционные и лабораторные занятия по темам: *Тема 1. Международные стандарты информационного обмена. Понятие угрозы.* *Тема 2 Информационная безопасность в условиях функционирования в России глобальных сетей. Виды противников или «нарушителей».* *Тема 3. Три вида возможных нарушений информационной системы. Защита.* *Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.*	Реферат* Доклад* Эссе*	А) полностью сформирована - 5 баллов Б) частично сформирована - 3-4 балла С) не сформирована- 2 и менее баллов	Сумма баллов (max=5) по следующим критериям оценки: 1. Соответствие содержания реферата, доклада заявленной тематике (1 балл). 2. Владение информацией и способность отвечать на вопросы аудитории (1 балл). 3. Качество источников и их количество при подготовке работы (I балл). 4. Качество самой представленной работы, ее научная обоснованность и практическая (профессионально-ориентированная

	Тема 4. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование. *Тема 5. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.* *Тема 6. Концепция информационной безопасности.* *Тема 7. Основные технологии построения защищенных ЭИС. Место информационной безопасности экономических систем в национальной безопасности страны.* *Тема 8 Анализ способов нарушений информационной безопасности. Использование защищенных компьютерных систем. Методы криптографии.*			направленность) (1 балл). 5. Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл).

*Характеристики инструментов (средств), оценивающих сформированность компетенций:

Реферат – продукт самостоятельной работы студента, представляющий собой краткое изложение в письменном виде полученных результатов теоретического анализа определенной научной (учебно-исследовательской) темы, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее. В реферате должна быть раскрыта тема, структура должна соответствовать теме и быть отражена в оглавлении, размер работы – 10-15 стр. печатного текста (список литературы и приложения в объем не входят), снабженного сносками и списком использованной литературы. Текстовая часть работы состоит из введения, основной части и заключения. Во введении обучающийся кратко обосновывает актуальность избранной темы реферата, раскрывает цель и задачи, которые он собирается решить в ходе своего небольшого исследования. В основной части (может состоять из 2-3 параграфов) подробно раскрывается содержание вопросов темы. В заключении должны быть кратко сформулированы полученные результаты исследования, приведены обобщающие выводы. Заключение может включать предложения автора, в том числе и по дальнейшему изучению заинтересовавшей его проблемы. В список литературы обучающийся включает только те издания, которые он использовал при написании реферата (не менее 5-7). В тексте обязательны ссылки на использованную литературу, оформленные в соответствии с ГОСТом. В приложении к реферату могут выноситься таблицы, графики, схемы и другие вспомогательные материалы, на которые имеются ссылки в тексте реферата. Критерии оценки реферата: 1) Степень раскрытия сущности вопроса: а) соответствие плана теме реферата; б) соответствие содержания теме и плану реферата; в) полнота проанализированного материала по теме; умение работать с отечественными и зарубежными научными исследованиями, критической литературой, периодикой, систематизировать и структурировать материал; г) обоснованность способов и методов

работы с материалом, адекватное и правомерное использование методов классификации, сравнения и др.; е) умение обобщать, делать выводы, сопоставлять различные точки зрения по одному вопросу (проблеме). 2) Оригинальность текста: а) самостоятельность в постановке проблемы, формулирование нового аспекта известной проблемы в установлении новых связей (межпредметных, внутрипредметных, интеграционных); б) явленность авторской позиции, самостоятельность оценок и суждений; д) стилевое единство текста, единство жанровых черт. 3) Обоснованность выбора источников: а) оценка использованной литературы: привлечены ли наиболее известные работы по теме исследования (в т.ч. журнальные публикации последних лет, последние статистические данные, сводки, справки и т.д.). 4) Соблюдение требований к оформлению: а) насколько верно оформлены ссылки на используемую литературу, список литературы. б) оценка грамотности и культуры изложения (в т.ч. орфографической, пунктуационной, стилистической культуры), владение терминологией; в) соблюдение требований к объёму реферата.

Доклад – продукт самостоятельной работы обучающегося, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы. Доклад – это научное сообщение на семинарском занятии, заседании научного кружка или учебно-теоретической конференции. Критерии оценки доклада: соответствие содержания заявленной теме; актуальность, новизна и значимость темы; аргументированность, полнота, структурированность и логичность изложения; свободное владение материалом: последовательность, умение вести дискуссию, правильно отвечать на вопросы; самостоятельность, степень оригинальности предложенных решений, иллюстративности, обобщений и выводов; наличие собственного отношения автора к рассматриваемой проблеме/теме (насколько точно и аргументировано выражено отношение автора к теме доклада); представление материала: качество презентации, оформления; культура речи, ораторское мастерство (соблюдение норм литературного языка, правильное произношения слов и фраз, оптимальный темп речи; умение правильно расставлять акценты; умение говорить достаточно громко, четко и убедительно); использование профессиональной терминологии (оценка того, насколько полно отражены в выступлении обучающегося профессиональные термины и общекультурные понятия по теме, а также насколько уверенно выступающий ими владеет); выдержанность регламента.

Практическое задание – это частично регламентированное задание, имеющее алгоритмическое или нестандартное решение, позволяющее диагностировать умения интегрировать знания различных научных областей, аргументировать собственную точку зрения, доказывать правильность своей позиции. Может выполняться в индивидуальном порядке или группой обучающихся.

Деловая и/или ролевая игра – совместная деятельность группы обучающихся и преподавателя под управлением преподавателя с целью решения учебных и профессионально-ориентированных задач путем игрового моделирования реальной проблемной ситуации. Позволяет оценивать умение анализировать и решать типичные профессиональные задачи. Критерии оценки: 2 балла – репродуктивный уровень участия в деловой игре (участвующий воспроизводит предлагаемые задания); 3 балла – продуктивный уровень (участвующий предлагает свои варианты действия); 4 балла – поисково-исследовательский уровень (участвующий применяет полученную информацию в нестандартных ситуациях); 5 баллов – креативный уровень (участвующий моделирует новое видение заданной проблемы).

Контрольная работа – средство проверки умений обучающихся применять полученные знания для решения задач определенного типа по теме или разделу; состоит из теоретической части (ответа на поставленные вопросы) и решения психолого-педагогической задачи. Контрольная работа обучающимися очной формы обучения выполняется на семинарском занятии, обучающимися заочной формы обучения

выполняется вне аудиторной работы. Обучающийся должен предварительно изучить и осмыслить материал, относящийся к объявленной теме контрольной работы. Критерии оценки контрольной работы: от 90% до 100% правильно выполненных заданий – отлично; от 70% до 89% правильно выполненных заданий - хорошо; от 50% до 69% правильно выполненных заданий - удовлетворительно; от 0 до 49 % правильно выполненных заданий – не удовлетворительно.

Тестирование – это контрольное мероприятие по учебному материалу, состоящее в выполнении обучающимся системы стандартизированных заданий, которая позволяет автоматизировать процедуру измерения уровня знаний и умений обучающегося. Тестирование включает в себя следующие типы заданий: задание с единственным выбором ответа из предложенных вариантов, задание на определение верных и неверных суждений; задание с множественным выбором ответов. Критерии оценки: от 90% до 100% правильно выполненных заданий – отлично; от 70% до 89% правильно выполненных заданий - хорошо; от 50% до 69% правильно выполненных заданий – удовлетворительно; от 0 до 49 % правильно выполненных заданий – не удовлетворительно.

Зачет, экзамен – контрольные мероприятия, которые проводятся по учебной дисциплине в виде, предусмотренном учебным планом, по окончании изучения курса. Занятие аудиторное, проводится в устной или письменной форме с использованием фондов оценочных средств по учебной дисциплине.

5.4. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Темы докладов (рефератов):

1. Административные и организационно-правовые методы защиты информации.
2. Программно-аппаратные методы защиты информации.
3. Криптографические методы защиты информации.
4. Государственное регулирование в сфере информационных технологий и информационной безопасности.
5. Международные и национальные (российские) стандарты управления информационной безопасностью и защиты информации.
6. Развитие информационного права в Российской Федерации.
7. Правовые основы электронного документооборота, использо¬ва¬ния электронно-цифровой подписи.
8. Правонарушения в информационной сфере.
9. Требования к обеспечению безопасности государственных информационных систем.
10. Категории, права и ограничение прав доступа к информации (общедоступная информация и информация с ограниченным доступом) в российском законодательстве.
11. Угрозы информационной безопасности компьютерных систем.
12. Основные принципы и направления обеспечения информационной безопасности компьютерных систем.
13. Анализ информационных рисков и политика безопасности предприятия.
14. Методы обеспечения конфиденциальности информации.
15. Методы обеспечения целостности данных.
16. Защита от разрушающих воздействий компьютерных вирусов.
17. Защита информации в компьютерных сетях.
18. Системы анализа защищенности (сканеры безопасности).
19. Межсетевые экраны (брандмауэры).

20. Системы и методы идентификации и аутентификации.
21. Защищенные операционные системы.
22. Обеспечение безопасности при работе с электронной почтой и другими сервисами Интернет.
23. Современные алгоритмы симметричного шифрования.
24. Применение алгоритмов шифрования с открытым ключом.
25. Технология электронных цифровых подписей.

Тестирование по учебной дисциплине «Информационная безопасность»

Примерные задания

Инструкция: внимательно прочитайте задания, выберите один или несколько вариантов, отметьте в бланке ответов.

Типовые тестовые задания

Вопрос 1

Какие законы существуют в России в области компьютерного права?

Выберите несколько из 6 вариантов ответа:

1) О государственной тайне
2) об авторском праве и смежных правах
3) о гражданском долге
4) о правовой охране программ для ЭВМ и БД
5) о правовой ответственности
6) об информации, информатизации, защищенности информации

Вопрос 2

Какие существуют основные уровни обеспечения защиты информации?

Выберите несколько из 7 вариантов ответа:

1) законодательный
2) административный
3) программно-технический
4) физический
5) вероятностный
6) процедурный
7) распределительный

Вопрос 3

Физические средства защиты информации

Выберите один из 4 вариантов ответа:

1) средства, которые реализуются в виде автономных устройств и систем
2) устройства, встраиваемые непосредственно в аппаратуру АС или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу
3) это программы, предназначенные для выполнения функций, связанных с защитой информации
4) средства, которые реализуются в виде электрических, электромеханических и электронных устройств

Вопрос 4

В чем заключается основная причина потерь информации, связанной с ПК?

Выберите один из 3 вариантов ответа:

1) с глобальным хищением информации
2) с появлением интернета
3) с недостаточной образованностью в области безопасности

Вопрос 5

Технические средства защиты информации

Выберите один из 4 вариантов ответа:

1) средства, которые реализуются в виде автономных устройств и систем

2) устройства, встраиваемые непосредственно в аппаратуру АС или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу

3) это программы, предназначенные для выполнения функций, связанных с защитой информации

4) средства, которые реализуются в виде электрических, электромеханических и электронных устройств

Вопрос 6

К аспектам ИБ относятся

Выберите несколько из 5 вариантов ответа:

1) дискретность

2) целостность

3) конфиденциальность

4) актуальность

5) доступность

Вопрос 7

Что такое криптология?

Выберите один из 3 вариантов ответа:

1) защищенная информация

2) область доступной информации

3) тайная область связи

Вопрос 8

Что такое несанкционированный доступ (нсд)?

Выберите один из 5 вариантов ответа:

1) Доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа

2) Создание резервных копий в организации

3) Правила и положения, выработанные в организации для обхода парольной защиты

4) Вход в систему без согласования с руководителем организации

5) Удаление не нужной информации

Вопрос 9

Что является основой для формирования государственной политики в сфере информации? (Ответьте 1 словом)

Запишите ответ:

Вопрос 10

Что такое целостность информации?

Выберите один из 4 вариантов ответа:

1) Свойство информации, заключающееся в возможности ее изменения любым субъектом

2) Свойство информации, заключающееся в возможности изменения только единственным пользователем

3) Свойство информации, заключающееся в ее существовании в виде единого набора файлов

4) Свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию)

Вопрос 11

Кто является знаковой фигурой в сфере информационной безопасности

Выберите один из 4 вариантов ответа:

1) Митник

2) Шеннон

3) Паскаль

4) Беббидж

Вопрос 12

В чем состоит задача криптографа?

Выберите один из 2 вариантов ответа:

1) взломать систему защиты

2) обеспечить конфиденциальность и аутентификацию передаваемых сообщений

Вопрос 13

Под ИБ понимают

Выберите один из 3 вариантов ответа:

1) защиту от несанкционированного доступа

2) защиту информации от случайных и преднамеренных воздействий естественного и искуственного характера

3) защиту информации от компьютерных вирусов

Вопрос 14

Что такое аутентификация?

Выберите один из 5 вариантов ответа:

1) Проверка количества переданной и принятой информации

2) Нахождение файлов, которые изменены в информационной системе несанкционированно

3) Проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы (обычно осуществляется перед разрешением доступа).

4) Определение файлов, из которых удалена служебная информация

5) Определение файлов, из которых удалена служебная информация

Вопрос 15

"Маскарад"- это

Выберите один из 2 вариантов ответа:

1) осуществление специально разработанными программами перехвата имени и пароля

2) выполнение каких-либо действий одним пользователем от имени другого пользователя, обладающего соответствующими полномочиями

Вопрос 16

Верификация -

Выберите один из 3 вариантов ответа:

1) это проверка принадлежности субъекту доступа предъявленного им идентификатора.

2) проверка целостности и подлинности инф, программы, документа

3) это присвоение имени субъекту или объекту

Вопрос 17

Кодирование информации -

Выберите один из 2 вариантов ответа:

1) представление информации в виде условных сигналов с целью автоматизации ее хранения, обработки, передачи и т.д.

2) метод специального преобразования информации, с целью защиты от ознакомления и модификации посторонним лицом

Вопрос 18

Утечка информации

Выберите один из 3 вариантов ответа:

1) несанкционированное изменение информации, корректное по форме, содержанию, но отличное по смыслу

2) ознакомление постороннего лица с содержанием секретной информации

3) потеря, хищение, разрушение или неполучение переданных данных

Вопрос 19

Под изоляцией и разделением (требование к обеспечению ИБ) понимают

Выберите один из 2 вариантов ответа:

1) разделение информации на группы так, чтобы нарушение одной группы информации не влияло на безопасность других групп информации (документов)

2) разделение объектов защиты на группы так, чтобы нарушение защиты одной группы не влияло на безопасность других групп

Вопрос 20

К аспектам ИБ относятся

Выберите несколько из 5 вариантов ответа:

1) дискретность

2) целостность

3) конфиденциальность

4) актуальность

5) доступность

Вопрос 21

Линейное шифрование -

Выберите один из 3 вариантов ответа:

1) несанкционированное изменение информации, корректное по форме и содержанию, но отличное по смыслу

2) криптографическое преобразование информации при ее передаче по прямым каналам связи от одного элемента ВС к другому

3) криптографическое преобразование информации в целях ее защиты от ознакомления и модификации посторонними лицами

Вопрос 22

Прочность защиты в АС

Выберите один из 3 вариантов ответа:

1) вероятность не преодоления защиты нарушителем за установленный промежуток времени

2) способность системы защиты информации обеспечить достаточный уровень своей безопасности

3) группа показателей защиты, соответствующая определенному классу защиты

Вопрос 23

Уровень секретности - это

Выберите один из 2 вариантов ответа:

1) ответственность за модификацию и НСД информации

2) административная или законодательная мера, соответствующая мере ответственности лица за утечку или потерю конкретной секретной информации, регламентируемой специальным документом, с учетом государственных, военно-стратегических, коммерческих, служебных или частных интересов

Вопрос 24

Угроза - это

Выберите один из 2 вариантов ответа:

1) возможное событие, действие, процесс или явление, которое может привести к ущербу чьих-либо интересов

2) событие, действие, процесс или явление, которое приводит к ущербу чьих-либо интересов

Вопрос 25

Под ИБ понимают

Выберите один из 3 вариантов ответа:

1) защиту от несанкционированного доступа

2) защиту информации от случайных и преднамеренных воздействий естественного и искуственного характера

3) защиту информации от компьютерных вирусов

Вопрос 26

Что такое криптография?

Выберите один из 3 вариантов ответа:

1) метод специального преобразования информации, с целью защиты от ознакомления и модификации посторонним лицом

2) область доступной информации

3) область тайной связи, с целью защиты от ознакомления и модификации посторонним лицом

Вопрос 27

Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, установленными собственником информации называется

Выберите один из 4 вариантов ответа:

1) кодируемой

2) шифруемой

3) недостоверной

4) защищаемой

Вопрос 28

Продолжите фразу: "Административная и законодательная мера, соответствующая мере ответственности лица за потерю конкретной секретной информации, регламентирующаяся специальным документом с учетом государственных и военно-стратегических, коммерческих или частных интересов - это..."

Запишите ответ:

_____

Вопрос 29

Продолжите фразу: " Последовательность символов, недоступная для посторонних, предназначенная для идентификации и аутентификации субъектов и объектов между собой - это..."

Запишите ответ:

_____

Вопрос 30

Способ представления информации в вычислительных системах

Запишите ответ:

_____

Вопрос 31

Вставьте пропущенное слово:

Информация может быть защищена без аппаратных и программных средств защиты с помощью _____ преобразований.

Запишите ответ:

_____

Вопрос 32

Абстрактное содержание какого-либо высказывания, описание, указание, сообщение либо известие - это

Выберите один из 4 вариантов ответа:

1) текст

2) данные

3) информация

4) пароль

Вопрос 33

Какие атаки предпринимают хакеры на программном уровне?

Выберите несколько из 4 вариантов ответа:

1) атаки на уровне ОС
2) атаки на уровне сетевого ПО
3) атаки на уровне пакетов прикладных программ
4) атаки на уровне СУБД

Вопрос 34

Организационные угрозы подразделяются на

Выберите несколько из 4 вариантов ответа:

1) угрозы воздействия на персонал
2) физические угрозы
3) действия персонала
4) несанкционированный доступ

Вопрос 35

Виды технической разведки (по месту размещения аппаратуры)

Выберите несколько из 7 вариантов ответа:

1) космическая
2) оптическая
3) наземная
4) фотографическая
5) морская
6) воздушная
7) магнитометрическая

Вопрос 36

Основные группы технических средств ведения разведки

Выберите несколько из 5 вариантов ответа:

1) радиомикрофоны
2) фотоаппараты
3) электронные "уши"
4) дистанционное прослушивание разговоров
5) системы определения местоположения контролируемого объекта

Вопрос 37

Разновидности угроз безопасности

Выберите несколько из 6 вариантов ответа:

1) техническая разведка
2) программные
3) программно-математичекие
4) организационные
5) технические
6) физические

Вопрос 38

Потенциально возможное событие, действие, процесс или явление, которое может причинить ущерб чьих-нибудь данных, называется

Выберите один из 4 вариантов ответа:

1) угрозой;
2) опасностью;
3) намерением;
4) предостережением.

Вопрос 39

Какая угроза возникает в результате технологической неисправности за пределами информационной системы?

Запишите ответ:

_____

Вопрос 40

Из каких компонентов состоит программное обеспечение любой универсальной компьютерной системы?

Выберите один из 4 вариантов ответа:

1) операционной системы, сетевого программного обеспечения

2) операционной системы, сетевого программного обеспечения и системы управления базами данных;

3) операционной системы, системы управления базами данных;

4) сетевого программного обеспечения и системы управления базами данных.

Вопрос 41

Комплекс мер и средств, а также деятельность на их основе, направленная на выявление, отражение и ликвидацию различных видов угроз безопасности объектам защиты называется

Выберите один из 4 вариантов ответа:

1) системой угроз;

2) системой защиты;

3) системой безопасности;

4) системой уничтожения.

Вопрос 42

К угрозам какого характера относятся действия, направленные на сотрудников компании или осуществляемые сотрудниками компании с целью получения конфиденциальной информации или нарушения функции бизнес-процессов?

Запишите ответ:

_____

Вопрос 43

К видам защиты информации относятся:

Выберите несколько из 4 вариантов ответа:

1) правовые и законодательные:

2) морально-этические;

3) юридические;

4) административно-организационные;

Вопрос 44

Доступ к информации в нарушение должностных полномочий сотрудника, доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации называется

Запишите ответ:

_____

Вопрос 45

К методам защиты от НСД относятся

Выберите несколько из 5 вариантов ответа:

1) разделение доступа;

2) разграничение доступа;

3) увеличение доступа;

4) ограничение доступа.

5) аутентификация и идентификация

Вопрос 46

Метод пароля и его модификация, метод вопрос-ответ, метод секретного алгоритма - это методы

Запишите ответ:

_____

Вопрос 47

Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности называется

Выберите один из 4 вариантов ответа:

1) политикой информации

2) защитой информации

3) политикой безопасности

4) организацией безопасности

Вопрос 48

Выделите группы, на которые делятся средства защиты информации:

Выберите один из 3 вариантов ответа:

1) физические, аппаратные, программные, криптографические, комбинированные;

2) химические, аппаратные, программные, криптографические, комбинированные;

3) физические, аппаратные, программные, этнографические, комбинированные;

Вопрос 49

Техническое, криптографическое, программное и иное средство, предназначенное для защиты информации, средство, в котором оно реализовано, а также средство контроля эффективности защиты информации- все это есть

Запишите ответ:

_____

Вопрос 50

Что такое компьютерный вирус?

Выберите один из 4 вариантов ответа:

1) Разновидность программ, которые способны к размножению

2) Разновидность программ, которые самоуничтожаются

3) Разновидность программ, которые не работают

4) Разновидность программ, которые плохо работают

Вопрос 51

Как подразделяются вирусы в зависимости от деструктивных возможностей?

Выберите один из 4 вариантов ответа:

1) Сетевые, файловые, загрузочные, комбинированные

2) Безвредные, неопасные, опасные, очень опасные

3) Резидентные, нерезидентные

4) Полиморфные, макровирусы, вирусы-невидимки, "паразитические", "студенческие", "черви", компаньон-вирусы

Вопрос 52

Нежелательная цепочка носителей информации, один или несколько из которых являются правонарушителем или его специальной аппаратурой называется

Запишите ответ:

_____

Вопрос 53

Установите соответствие

Укажите соответствие для всех 4 вариантов ответа:

1) это комплекс мероприятий, исключающих или ослабляющих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны за счет электромагнитных полей побочного характера и наводок

2) это комплекс мероприятий, исключающих или уменьшающих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны в виде производственных или промышленных отходов

3) это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет акустических полей

4) это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет распространения световой энергии

__ защита информации от утечки по акустическому каналу

__ Защита информации от утечки по визуально-оптическому каналу

__ Защита информации от утечки по электромагнитным каналам

__ Защита информации от утечки по материально-вещественному каналу

Вопрос 54

Надежным средством отвода наведенных сигналов на землю служит

Запишите ответ:

_____

Вопрос 55

Установите соответствие

Укажите соответствие для всех 2 вариантов ответа:

1) наука о скрытой передаче информации путем сохранения в тайне самого факта передачи

2) наука скрывающая содержимое секретного сообщения

__ стеганография

__ криптография

Примерный перечень вопросов для итогового контроля знаний на зачете (6 семестр):

1. Понятие информационной безопасности.
2. Важность и сложность проблемы информационной безопасности
3. Сервисные службы защиты
4. Нарушения
5. Механизмы защиты
6. Абстрактные модели защиты информации
7. Модели защиты сети
8. Модели защиты доступа к сети
9. Основные определения и критерии классификации угроз
10. Действия, приводящие к неправомерному овладении конфиденциальной информацией: разглашение
11. Действия, приводящие к неправомерному овладении конфиденциальной информацией: утечка
12. Действия, приводящие к неправомерному овладении конфиденциальной информацией: несанкционированный доступ
13. Наиболее распространенные угрозы доступности
14. Некоторые примеры угроз доступности
15. Вредоносное программное обеспечение
16. Основные угрозы целостности
17. Основные угрозы конфиденциальности
18. Основные принципы информационной безопасности
19. Основные задачи в сфере обеспечения информационной безопасности.
20. Функции государственной системы по обеспечению информационной безопасности
21. Направления обеспечения информационной безопасности
22. Законодательный уровень информационной безопасности

23. Правовые акты общего назначения, затрагивающие вопросы информационной безопасности

24. Закон "Об информации, информатизации и защите информации"

25. Другие законы и нормативные акты

26. Административный уровень информационной безопасности

27. Политика безопасности

28. Программа безопасности

29. Процедурный уровень информационной безопасности

30. Основные классы мер процедурного уровня

31. Управление персоналом

32. Физическая защита

33. Поддержание работоспособности

34. Реагирование на нарушения режима безопасности

35. Планирование восстановительных работ

36. Основные понятия программно-технического уровня информационной безопасности

37. Особенности современных информационных систем, существенные с точки зрения безопасности

38. Архитектурная безопасность

39. Оценочные стандарты и технические спецификации. "Оранжевая книга" как оценочный стандарт

40. Информационная безопасность распределенных систем. Рекомендации X.800

41. Стандарт ISO/IEC 15 408 "Критерии оценки безопасности информационных технологий"

42. Гармонизированные критерии Европейских стран

43. Интерпретация "Оранжевой книги" для сетевых конфигураций

44. Руководящие документы Гостехкомиссии России

45. Основные аспекты криптографии

46. Основные аспекты криптоанализа

47. Модели криптографии К. Шеннона

48. Теоретико-информационные оценки стойкости симметричных криптосистем

49. Потоковые шифры

50. Блочные шифры

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

Ответы обучающегося на зачете оцениваются каждым педагогическим работником по варианту зачтено/незачтено.

Критерии оценки ответа на вопросы теоретического блока:

«Зачтено» – обучающийся глубоко и прочно освоил программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагает, тесно увязывает с задачами и будущей деятельностью, не затрудняется с ответом при видоизменении задания, свободно справляется с задачами и практическими заданиями, правильно обосновывает принятые решения, умеет самостоятельно обобщать и излагать материал, не допуская ошибок;

«Незачтено» - обучающийся не знает значительной части программного материала, допускает существенные ошибки, с большими затруднениями выполняет практические задания, задачи.

Критерии оценки практического задания:

«зачтено» – задание выполнено верно;

«не зачтено» – задание не выполнено, либо выполнено с существенными ошибками, сделаны неверные выводы.

6. Перечень основной и дополнительной учебной литературы для освоения учебной дисциплины

6.1. Основная литература.

1. Теория информационной безопасности и методология защиты информации: учебное пособие\\Загинайлов Ю. Н. Издательство:Директ-Медиа 2015 г., 253 стр. (URL: http://www.knigafund.ru/books/181420)

6.1 Дополнительная литература по дисциплине:

1. Основы информационной безопасности : курс визуальных лекций: учебное пособие\\Загинайлов Ю. Н. Издательство:Директ-Медиа 2015 г., 105 стр. (URL: http://www.knigafund.ru/books/183103).

7. Перечень ресурсов информационно-коммуникационной сети «Интернет», необходимых для освоения учебной дисциплины

http://mon.gov.ru – сайт Минобрнауки РФ

http://www.edu.ru/ – библиотека федерального портала «Российское образование» (содержит каталог ссылок на интернет-ресурсы, электронные библиотеки по различным вопросам образования)

http://www.prlib.ru – Президентская библиотека

http://www.rusneb.ru – Национальная электронная библиотека

http://elibrary.rsl.ru/ – сайт Российской государственной библиотеки (раздел «Электронная библиотека»)

http://elibrary.ru – научная электронная библиотека «Elibrary»

www.knigafund.ru - Электронно-библиотечная система «КнигаФонд

8. Методические указания для обучающихся по освоению учебной дисциплины

Освоение обучающимся учебной дисциплины **«Информационная безопасность»** предполагает изучение материалов дисциплины на аудиторных занятиях и в ходе самостоятельной работы. Аудиторные занятия проходят в форме лекций, семинаров, практических занятий. Самостоятельная работа включает разнообразный комплекс видов и форм работы обучающихся.

Для успешного освоения учебной дисциплины и достижения поставленных целей необходимо внимательно ознакомиться настоящей рабочей программы учебной дисциплины. Ее может представить преподаватель на вводной лекции или самостоятельно обучающийся использует информацию на официальном Интернет-сайте Института.

Следует обратить внимание на список основной и дополнительной литературы, на предлагаемые преподавателем ресурсы информационно-телекоммуникационной сети Интернет. Эта информация необходима для самостоятельной работы обучающегося.

При подготовке к аудиторным занятиям необходимо помнить особенности каждой формы его проведения.

Подготовка к учебному занятию лекционного типа заключается в следующем.

С целью обеспечения успешного обучения обучающийся должен готовиться к лекции, поскольку она является важнейшей формой организации учебного процесса, поскольку:

– знакомит с новым учебным материалом;

– разъясняет учебные элементы, трудные для понимания;

– систематизирует учебный материал;

– ориентирует в учебном процессе.

С этой целью:

– внимательно прочитайте материал предыдущей лекции;

– ознакомьтесь с учебным материалом по учебнику и учебным пособиям с темой прочитанной лекции;

– внесите дополнения к полученным ранее знаниям по теме лекции на полях лекционной тетради;

– запишите возможные вопросы, которые вы зададите лектору на лекции по материалу изученной лекции;

– постарайтесь уяснить место изучаемой темы в своей подготовке;

– узнайте тему предстоящей лекции (по тематическому плану, по информации лектора) и запишите информацию, которой вы владеете по данному вопросу

Подготовка к занятию семинарского типа

При подготовке к занятию семинарского типа следует обратить внимание на следующие моменты: на процесс предварительной подготовки, на работу во время занятия, обработку полученных результатов, исправление полученных замечаний.

Предварительная подготовка к учебному занятию семинарского типа заключается в изучении теоретического материала в отведенное для самостоятельной работы время, ознакомление с инструктивными материалами с целью осознания задач практического занятия.

Работа во время проведения учебного занятия семинарского типа включает несколько моментов:

– консультирование студентов преподавателями с целью предоставления исчерпывающей информации, необходимой для самостоятельного выполнения предложенных преподавателем задач, ознакомление с правилами техники безопасности при работе в аудитории;

– самостоятельное выполнение заданий согласно обозначенной учебной программой тематики.

Главным результатом практического занятия является получение положительной оценки за доклад, реферат, эссе по тематике занятия. Это является необходимым условием при проведении рубежного контроля и допуска к зачету. При получении неудовлетворительных результатов обучающийся имеет право в дополнительное время пересдать преподавателю работу до проведения промежуточной аттестации.

Самостоятельная работа.

Для более углубленного изучения темы задания для самостоятельной работы рекомендуется выполнять параллельно с изучением данной темы. При выполнении заданий по возможности используйте наглядное представление материала. Более подробная информация о самостоятельной работе представлена в разделах «Учебно-методическое обеспечение самостоятельной работы по дисциплине (модулю)», «Методические указания к самостоятельной работе по дисциплине (модулю»).

Подготовка к зачету, экзамену. К зачету и экзамену необходимо готовится целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине. Попытки освоить учебную дисциплину в период зачетно-экзаменационной сессии, как правило, приносят не слишком удовлетворительные результаты.

При подготовке к зачету и экзамену обратите внимание на практические задания на основе теоретического материала.

При подготовке к ответу на вопросы зачета и экзамена по теоретической части учебной дисциплины выделите в вопросе главное, существенное (понятия, признаки, классификации и пр.), приведите примеры, иллюстрирующие теоретические положения.

После предложенных указаний у обучающихся должно сформироваться четкое представление об объеме и характере знаний и умений, которыми надо будет овладеть по дисциплине.

9. Информационно-технологическое обеспечение образовательного процесса по учебной дисциплине

9.1. Информационные технологии

1. Персональные компьютеры;
2. Доступ к интернет
3. Проектор.

9.2. Программное обеспечение

1. Microsoft Office (Word, Excel)

9.3. Информационные справочные системы

1. Университетская информационная система РОССИЯ - http://www.cir.ru/
2. Гарант

10. Материально-техническое обеспечение образовательного процесса по учебной дисциплине

Для изучения учебной дисциплины **«Информационная безопасность»** в рамках реализации основной профессиональной образовательной программы по направлению подготовки 38.03.01 Экономика (уровень бакалавриата), используются:

Учебная аудитория для занятий лекционного типа оснащена специализированной мебелью (стол для преподавателя, парты, стулья, доска для написания мелом); техническими средствами обучения (видеопроекционное оборудование, средства звуковоспроизведения, экран и имеющие выход в сеть Интернет),

Учебная аудитория для занятий семинарского типа: оснащена специализированной мебелью (стол для преподавателя, персональные компьютеры с доступом в сеть интернет, парты, стулья, доска для написания мелом); техническими средствами обучения (видеопроекционное оборудование, средства звуковоспроизведения, экран и имеющие выход в сеть Интернет).

Учебная аудитория для занятий лабораторного типа: оснащена специализированной мебелью (стол для преподавателя, персональные компьютеры с доступом в сеть интернет и специализированным программным обеспечением, стулья); техническими средствами обучения (видеопроекционное оборудование, средства звуковоспроизведения, экран и имеющие выход в сеть Интернет).

Помещения для самостоятельной работы обучающихся: оснащены специализированной мебелью (парты, стулья) техническими средствами обучения (персональные компьютеры с доступом в сеть интернет и обеспечением доступа в электронно-информационную среду института, программным обеспечением).

11. Образовательные технологии

При реализации учебной дисциплины **«Информационная безопасность»** применяются различные образовательные технологии.

Освоение учебной дисциплины **«Информационная безопасность»** предусматривает использование в учебном процессе активных форм проведения учебных занятий в форме, разбор конкретных ситуаций и практических задач в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.