Приложение Л.РПД Б1.Б.19

Филиал федерального государственного бюджетного образовательного учреждения высшего образования
«Национальный исследовательский университет «МЭИ»
в г. Смоленске

УТВЕРЖДАЮ
Зам. директора
филиала ФГБОУ ВО «НИУ «МЭИ»
в г. Смоленске
по учебно-методической работе
_____ В.В. Рожков
«_31_» _08_ 20_15_ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

(НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ)

Направление подготовки: 09.03.03 Прикладная информатика

Профиль подготовки: Прикладная информатика в управлении производством

Уровень высшего образования: бакалавриат

Нормативный срок обучения: 4 года

Смоленск – 2015 г.

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Целью освоения дисциплины является подготовка обучающихся к производственно-технологическому и организационно-управленческому видам деятельности по направлению подготовки 09.03.03 Прикладная информатика (профиль подготовки: Прикладная информатика в управлении производством) посредством обеспечения этапов формирования компетенций, предусмотренных ФГОС ВО, в части представленных ниже знаний, умений и навыков.

Задачами дисциплины является получение обучающимися:

- знаний о современных автоматизированных системах, об угрозах информационной безопасности, о нормативных правовых документов по информационной безопасности и о методах и средствах обеспечения информационной безопасности;
- умений выявлять угрозы информационной безопасности, использовать нормативные правовые документы по информационной безопасности, использовать методы и средства обеспечения информационной безопасности и проводить обследование организаций;
- навыков определения угроз информационной безопасности, приемами разработки политики безопасности предприятия и навыками использования методов и средств обеспечения информационной безопасности.

То есть, задачами дисциплины является изучение понятийного аппарата дисциплины, основных теоретических положений и методов, формирование умений и привитие навыков применения теоретических знаний для решения практических и прикладных задач.

Дисциплина «Информационная безопасность» направлена на формирование следующих общепрофессиональных и профессиональных компетенций:

ОПК-1 способностью использовать нормативно-правовые документы, международные и отечественные стандарты в области информационных систем и технологий

В результате изучения дисциплины студент должен:

Знать:

- основные нормативные правовые документы, международные и отечественные стандарты в области информационных систем (ИС) и технологий (в том числе регламентирующие сферу информационной безопасности);

Уметь:

-ориентироваться в системе законодательства и нормативных правовых актов, регламентирующих область ИС (в том числе сферу защиты информации в ИС);

- использовать правовые нормы в сфере информационной безопасности;

Владеть:

- навыками поиска необходимых нормативных и законодательных документов и навыками работы с ними в области ИС (в том числе сфере информационной безопасности ИС).

ОПК-3 способностью использовать основные законы естественнонаучных дисциплин и современные информационно-коммуникационные технологии в профессиональной деятельности

В результате изучения дисциплины студент должен:

Знать:

- методы, способы и средства получения, хранения и переработки информации;
- принципы построения современных информационно-коммуникационных технологий;

Уметь:

- использовать источники экономической, социальной, управленческой информации;

Владеть:

- навыками применения современных методов сбора, обработки и анализа данных.

ОПК-4 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

В результате изучения дисциплины студент должен:

Знать:

- виды и источники угроз безопасности информации для различных профессиональных областей;
- законодательную базу в сфере информационной безопасности;
- основные требования информационной безопасности.

Уметь:

- определять актуальные источники угроз безопасности для различных профессиональных областей.

Владеть:

- навыками владения современных средств информационной безопасности.

ПК-14 способностью осуществлять ведение базы данных и поддержку информационного обеспечения решения прикладных задач

В результате изучения дисциплины студент должен:

Знать:

- основные методы администрирования базы данных (БД);
- основные элементы информационной поддержки решения задачи защиты информации.

Уметь:

- проводить анализ методы администрирования БД, для обеспечения информационной безопасности;

Владеть:

- навыками ведения БД, которые обеспечивают приемлемый уровень информационной безопасности.

ПК-18 способностью принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью

В результате изучения дисциплины студент должен:

Знать:

- основные методы и средства управления информационной безопасностью;

Уметь:

- выбирать методы и разрабатывать средства защиты информации;

Владеть:

- навыками работы с инструментальными средствами обеспечения информационной безопасности.

2. Место дисциплины в структуре образовательной программы

Дисциплина относится к базовой части блока 1 «Дисциплина (модули)» образовательной программы подготовки бакалавров по профилю Прикладная информатика в управлении производством направления 09.03.03 Прикладная информатика (индекс дисциплины в соответствии с учебным планом: Б1.Б.19).

В соответствии с учебным планом по направлению 09.03.03 Прикладная информатика дисциплина «Информационная безопасность» (Б1.Б.19) базируется на следующих дисциплинах:

«Вычислительные системы, сети и телекоммуникации»

«Операционные системы»

«Информационные системы и технологии»
«Проектирование информационных систем»
«Проектный практикум»
«Метрология, стандартизация и сертификация программных продуктов»
«Правовые вопросы информатики»
«Предметно-ориентированные экономические информационные системы»
«Мультимедийные технологии»
«Корпоративные информационные системы»
« Разработка и стандартизация программных средств и информационных технологий»
«Информатика и программирование»
«Базы данных»
«Информационный менеджмент»
«Информационная логистика»

Дисциплина базируется на знаниях, умениях и навыках, полученных в ходе прохождения учебной и производственной практик, выполнения научно-исследовательской работы.

Знания, умения и навыки, полученные студентами в процессе изучения дисциплины, являются базой для изучения следующих дисциплин:

«Маркетинговые коммуникации»
«Интеллектуальные информационные системы»
«Мировые информационные ресурсы»

Знания, умения и навыки, полученные студентами в процессе изучения дисциплины, являются базой для прохождения преддипломной практики и государственной итоговой аттестации (выпускная квалификационная работа).

3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Аудиторная работа

Цикл:	Блок 1	Семестр
Часть цикла:	Базовая часть	
Индекс дисциплины по учебному плану:	Б1.Б.19	
Часов (всего) по учебному плану:	**180**	8 семестр
Трудоемкость в зачетных единицах (ЗЕТ)	5	8 семестр
Лекции (ЗЕТ, часов)	0,56 ЗЕТ, 20 час.	8 семестр
Практические занятия (ЗЕТ, часов)	-	-
Лабораторные работы (ЗЕТ, часов)	0,83 ЗЕТ, 30 час	8 семестр
Курсовая работа (ЗЕТ, часов)	-	-
Объем самостоятельной работы по учебному плану (ЗЕТ, часов всего)	2,61 ЗЕТ, 94 час.	8 семестр
Зачет с оценкой (в объеме самостоятельной работы)	-	-
Экзамен	1 ЗЕТ, 36 час	8 семестр

Самостоятельная работа студентов

Вид работ	Трудоёмкость, ЗЕТ, час
Изучение материалов лекций (лк)	0,56 ЗЕТ, 20 час
Подготовка к практическим занятиям (пз)	-
Подготовка к защите лабораторной работы (лаб)	0,83 ЗЕТ, 30 час
Выполнение расчетно-графической работы	0,5 ЗЕТ, 18 час
Выполнение реферата	-
Выполнение курсовой работы	-
Самостоятельное изучение дополнительных материалов дисциплины (СРС)	0,72 ЗЕТ, 26 час
Подготовка к тестированию	-
Подготовка к зачету	-
Всего (в соответствии с УП)	2,61 ЗЕТ, 94 час
Подготовка к экзамену	1 ЗЕТ, 36 час

4. Содержание дисциплины, структурированное по темам с указанием отведенного на них количества академических часов и видов учебных занятий

№ п/п	Темы дисциплины	Всего часов на тему	Виды учебных занятий, включая самостоятельную работу студентов и трудоемкость (в часах) (*в соответствии с УП*)					
			лк	пр	лаб	СРС	экз	в т.ч. интеракт.
1	2	3	4	5	6	7	8	9
1	Международные стандарты информационного обмена. Понятие угрозы. Концепция информационной безопасности. Виды противников (или «нарушителей»).	13	2			8 (РГР 2)	3	1
2	Основные нормативные руководящие документы, законы РФ и т.п. касающиеся государственной тайны и защиты информации.	14	2			8 (РГР 2)	4	1
3	Виды возможных нарушений информационных систем. Особенности нарушений информационных систем в конкретных предметных областях	16	2			10 (РГР 6)	4	1
4	Основные положения теории информационной безопасности информационных систем.	13	2			8	3	1
5	Защита программного обеспечения, основанная на идентификации пользователя. Защита программного обеспечения, основанная на идентификации ПЭВМ. Защита программного обеспечения, основанная на идентификации исполняемого модуля.	23	2		8	10	3	1

6	Методы криптографии. Защита данных. Шифрование данных и программ. Понятие идеального шифра.	28	2		12	10 (РГР 2)	4	1
7	Понятие о вредоносных программах. Виды компьютерных вирусов.	24	2		4	14	4	1
8	Методы защиты информации в вычислительных сетях. Обеспечение информационной безопасности в глобальной сети Интернет.	15	2			10 (РГР 4)	3	1
9	Использование защищенных компьютерных систем.	22	2		6	10 (РГР 2)	4	1
10	Таксономия нарушений информационной безопасности вычислительной системы и причины, обусловливающие их существование. Оценка надежности защитных механизмов.	12	2			6	4	1
всего по видам учебных занятий		**180**	**20**		**30**	**94**	**36**	**10**

Содержание по видам учебных занятий

Тема 1. Международные стандарты информационного обмена. Понятие угрозы. Концепция информационной безопасности. Виды противников (или «нарушителей»).

Лекция 1. Международные стандарты информационного обмена. Понятие угрозы. Концепция информационной безопасности. Виды противников (или «нарушителей») (2 час).

Самостоятельная работа студента (СРС, 8 час)

Подготовка к лекции (2 час).

Выполнение расчетно-графической работы (2 час).

Изучение дополнительного теоретического материала (4 час).

Подготовка к экзамену (3 час)

Текущий контроль:

- устный опрос: собеседование;

- письменный опрос: проверка конспектов лекций.

Тема 2. Основные нормативные руководящие документы, законы РФ и т.п. касающиеся государственной тайны и защиты информации.

Лекция 2. Основные нормативные руководящие документы, законы РФ и т.п. касающиеся государственной тайны и защиты информации (2 час).

Самостоятельная работа студента (СРС, 8 час)

Подготовка к лекции (2 час).

Выполнение расчетно-графической работы (2 час).

Изучение дополнительного теоретического материала (4 час).

Подготовка к экзамену (4 час).

Текущий контроль:

- устный опрос: собеседование;

- письменный опрос: проверка конспектов лекций; проверка выполнения расчетно-графической работы;

Тема 3. Виды возможных нарушений информационных систем. Особенности нарушений информационных систем в конкретных предметных областях.

Лекция 3. Виды возможных нарушений информационных систем. Особенности нарушений информационных систем в конкретных предметных областях.

Самостоятельная работа студента (СРС, 10 час)

Подготовка к лекции (2 час).

Выполнение расчетно-графической работы (6 час).

Изучение дополнительного теоретического материала (2 час).

Подготовка к экзамену (4 час)

Текущий контроль:

- устный опрос: собеседование;

- письменный опрос: проверка конспектов лекций; проверка выполнения расчетно-графической работы;

Тема 4. Основные положения теории информационной безопасности информационных систем.

Лекция 4. Основные положения теории информационной безопасности информационных систем (2 час).

Самостоятельная работа студента (СРС, 8 час)

Подготовка к лекции (2 час).

Изучение дополнительного теоретического материала (6 час).

Подготовка к экзамену (3 час)

Текущий контроль:

- устный опрос: собеседование;

- письменный опрос: проверка конспектов лекций.

Тема 5. Защита программного обеспечения, основанная на идентификации пользователя. Защита программного обеспечения, основанная на идентификации ПЭВМ. Защита программного обеспечения, основанная на идентификации исполняемого модуля.

Лекция 5. Защита программного обеспечения, основанная на идентификации пользователя. Защита программного обеспечения, основанная на идентификации ПЭВМ. Защита программного обеспечения, основанная на идентификации исполняемого модуля.

Лабораторная работа 1-4. Защита от несанкционированного использования программ, основанная на привязке программного обеспечения к аппаратным средствам конкретного компьютера и использовании электронного ключа (8 час).

Самостоятельная работа студента (СРС, 10 час)

Подготовка к лекции (2 час).

Подготовка к защите лабораторной работы (8 час).

Подготовка к экзамену (3 час)

Текущий контроль:

- устный опрос: собеседование; защита лабораторной работы;

- письменный опрос: проверка конспектов лекций; проверка отчета по лабораторной работе.

Тема 6. Методы криптографии. Защита данных. Шифрование данных и программ. Понятие идеального шифра.

Лекция 6. Методы криптографии. Защита данных. Шифрование данных и программ. Понятие идеального шифра.

Лабораторная работа 5-10. Изучение и использование различных методов криптографии для защиты данных. (12 час).

Самостоятельная работа студента (СРС, 10 час)
Подготовка к лекции (2 час).
Подготовка к защите лабораторной работы (6 час).
Выполнение расчетно-графической работы (2 час).
Подготовка к экзамену (4 час)
Текущий контроль:
- устный опрос: собеседование; защита лабораторной работы;
- письменный опрос: проверка конспектов лекций; проверка выполнения расчетно-графической работы; проверка отчета по лабораторной работе.
- контроль с помощью технических средств и информационных технологий: электронное тестирование знаний, умений и навыков.

Тема 7. Понятие о вредоносных программах. Виды компьютерных вирусов.
Лекция 7. Понятие о вредоносных программах. Виды компьютерных вирусов (2 час).
Лабораторная работа 11-12. Изучение программных средств, обеспечивающих защиту от вредоносных программ (4 час).
Самостоятельная работа студента (СРС, 14 час)
Подготовка к лекции (2 час).
Подготовка к защите лабораторной работы (10 час).
Изучение дополнительного теоретического материала (2 час).
Подготовка к экзамену (4 час)
Текущий контроль:
- устный опрос: собеседование; защита лабораторной работы;
- письменный опрос: проверка конспектов лекций; проверка отчета по лабораторной работе.
- контроль с помощью технических средств и информационных технологий: электронное тестирование знаний, умений и навыков.

Тема 8. Методы защиты информации в вычислительных сетях. Обеспечение информационной безопасности в глобальной сети Интернет.
Лекция 8. Методы защиты информации в вычислительных сетях. Обеспечение информационной безопасности в глобальной сети Интернет (2 час).
Самостоятельная работа студента (СРС, 10 час)
Подготовка к лекции (2 час).
Выполнение расчетно-графической работы (4 час).
Изучение дополнительного теоретического материала (4 час).
Подготовка к экзамену (3 час)
Текущий контроль:
- устный опрос: собеседование;
- письменный опрос: проверка конспектов лекций; проверка выполнения расчетно-графической работы.
Тема 9. Использование защищенных компьютерных систем.
Лекция 9. Использование защищенных компьютерных систем (2 час).
Лабораторная работа 13-15. Организация комплексной защиты информационных систем (6 час).
Самостоятельная работа студента (СРС, 10 час)
Подготовка к лекции (2 час).
Подготовка к защите лабораторной работы (6 час).
Выполнение расчетно-графической работы (2 час).
Подготовка к экзамену (4 час)
Текущий контроль:

- устный опрос: собеседование; защита лабораторной работы;
- письменный опрос: проверка конспектов лекций; проверка выполнения расчетно-графической работы; проверка отчета по лабораторной работе.

Тема 10. Таксономия нарушений информационной безопасности вычислительной системы и причины, обусловливающие их существование. Оценка надежности защитных механизмов.

Лекция 10. Таксономия нарушений информационной безопасности вычислительной системы и причины, обусловливающие их существование. Оценка надежности защитных механизмов (2 час).

Самостоятельная работа студента (СРС, 6 час)

Подготовка к лекции (2 час).

Изучение дополнительного теоретического материала (4 час).

Подготовка к экзамену (4 час)

Текущий контроль:

- устный опрос: собеседование;
- письменный опрос: проверка конспектов лекций.

Промежуточная аттестация по дисциплине:

Изучение дисциплины заканчивается экзаменом. Экзамен проводится в соответствии с Положением о зачетной и экзаменационной сессиях в ФГБОУ ВО «НИУ «МЭИ» и инструктивным письмом от 14.05.2012 г. № И-23.

Экзамен по дисциплине проводится в устной форме.

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Для обеспечения самостоятельной работы разработаны:
- учебно-методическое обеспечение лекционных занятий;
- методические рекомендации по выполнению лабораторных работ;
- методические рекомендации по выполнению расчетно-графической работы;
- методические рекомендации к самостоятельной работе студентов.

Учебно-методическое обеспечение аудиторной и внеаудиторной самостоятельной работы студентов, обучающихся по дисциплине «Информационная безопасность» представлены в методических указаниях для обучающихся по освоению дисциплины.

6 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

6.1 Перечень компетенций с указанием этапов их формирования

При освоении дисциплины формируются следующие компетенции: ОПК-1, ОПК-3, ОПК-4, ПК-14, ПК-18.

Указанные компетенции формируются в соответствии со следующими этапами:

1. Формирование и развитие теоретических знаний, предусмотренных указанными компетенциями (лекционные занятия, самостоятельная работа студентов).

2. Приобретение и развитие практических умений, предусмотренных компетенциями (лабораторные работы, самостоятельная работа студентов, РГР).

3. Закрепление теоретических знаний, умений и практических навыков, предусмотренных компетенциями, в ходе защит лабораторных работ, а также решения конкретных задач на лабораторных занятиях, успешной сдачи экзамена.

Матрица соотнесения тем/разделов дисциплины и формируемых в них компетенций

Темы, разделы дисциплины	Колич. часов	Код компетенции					Σ общее количество компетенций
		ОПК-1	ОПК-3	ОПК-4	ПК-14	ПК-18	
Тема 1. Международные стандарты информационного обмена. Понятие угрозы. Концепция информационной безопасности. Виды противников (или «нарушителей»).	13	+					1
Тема 2. Основные нормативные руководящие документы, законы РФ и т.п. касающиеся государственной тайны и защиты информации.	14	+					1
Тема 3. Виды возможных нарушений информационных систем. Особенности нарушений информационных систем в конкретных предметных областях.	16			+			1
Тема 4. Основные положения теории информационной безопасности информационных систем.	13		+				1
Тема 5. Защита программного обеспечения, основанная на идентификации пользователя. Защита программного обеспечения, основанная на идентификации ПЭВМ. Защита программного обеспечения, основанная на идентификации исполняемого модуля.	23				+		1
Тема 6. Методы криптографии. Защита данных. Шифрование данных и программ. Понятие идеального шифра.	28				+	+	2
Тема 7. Понятие о вредоносных программах. Виды компьютерных вирусов.	24		+				1
Тема 8. Методы защиты информации в вычислительных сетях. Обеспечение информационной безопасности в глобальной сети Интернет.	15					+	1
Тема 9. Использование защищенных компьютерных систем.	22	+		+		+	3
Тема 10. Таксономия нарушений информационной безопасности вычислительной системы и причины, обусловливающие их существование. Оценка надежности защитных механизмов.	12			+			1
Итого	**180**	3	2	3	2	3	

6.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описания шкал оценивания

Сформированность каждой компетенции в рамках освоения данной дисциплины оценивается по трехуровневой шкале:

- пороговый уровень является обязательным для всех обучающихся по завершении освоения дисциплины;
- продвинутый уровень характеризуется превышением минимальных характеристик сформированности компетенции по завершении освоения дисциплины;
- эталонный уровень характеризуется максимально возможной выраженностью компетенции и является важным качественным ориентиром для самосовершенствования.

Уровень сформированности каждой компетенции на различных этапах ее формирования в процессе освоения данной дисциплины оценивается в ходе текущего контроля успеваемости и представлен различными видами оценочных средств.

Для оценки уровня сформированности компетенции ОПК-1 «способностью использовать нормативно-правовые документы, международные и отечественные стандарты в области информационных систем и технологий» в рамках данной дисциплины оценивается

содержательная сторона и качество материалов, представленных в конспектах лекций, отчетах студента по лабораторным работам, отчете студента по расчетно-графической работе. Учитываются также ответы студента на вопросы по соответствующим видам занятий при текущем контроле – собеседование, защита лабораторных работ.

Принимается во внимание наличие:

знаний:

- основных нормативных правовых документов, международных и отечественных стандартов в области информационных систем (ИС) и технологий (в том числе регламентирующие сферу информационной безопасности);

умений:

-ориентироваться в системе законодательства и нормативных правовых актов, регламентирующих область ИС (в том числе сферу защиты информации в ИС);

- использовать правовые нормы в сфере информационной безопасности;

навыков:

- поиска необходимых нормативных и законодательных документов и навыками работы с ними в области ИС (в том числе сфере информационной безопасности ИС).

Таблица - Показатели и критерии оценивания уровня сформированности компетенции ОПК-1 «способностью использовать нормативно-правовые документы, международные и отечественные стандарты в области информационных систем и технологий»

Результаты освоения (Показатели)	Уровни сформированности	Критерии оценивания	Оценка (шкала оценивания)	Оцениваемая форма контроля
Знать: - основные нормативные правовые документы, международные и отечественные стандарты в области информационных систем (ИС) и технологий (в том числе регламентирующие сферу информационной безопасности); **Уметь:** -ориентироваться в системе законодательства и нормативных правовых актов, регламентирующих область ИС (в том числе сферу защиты информации в ИС); - использовать правовые нормы в сфере информационной безопасности; **Владеть:** - навыками поиска необходимых нормативных и законодательных документов и навыками работы с ними в области ИС (в том числе сфере информационной безопасности ИС).	Эталонный.	1. Перечислить и дать общую характеристику основных нормативно правовых документов в области информационной безопасности. 2. Дать оценку возможностей использования правовых методов защиты в сфере информационной безопасности. 3. Эффективно использовать правовые методы защиты информации (законодательные акты, законы РФ и т.д.).	5	Конспект лекций студента, Отчёт по лабораторным работам, Защита лабораторных работ, Собеседование, РГР, Экзамен
	Продвинутый	1. Перечислить и дать общую характеристику основных нормативно правовых документов в области информационной безопасности. 2. Дать оценку возможностей использования правовых методов защиты в сфере информационной безопасности.	4	
	Пороговый	1. Перечислить и дать общую характеристику основных нормативно правовых документов в области информационной безопасности.	3	
	Ниже порогового	Исключительно плохо ориентируется в основных нормативных документах в области информационной безопасности.	2	

Для оценки сформированности в рамках данной дисциплины компетенции ОПК-3 «способностью использовать основные законы естественнонаучных дисциплин и современные информационно-коммуникационные технологии в профессиональной деятельности» преподавателем оценивается содержательная сторона и качество материалов, представленных в конспектах лекций, отчетах студента по лабораторным работам, отчете студента по расчетно-графической работе. Учитываются также ответы студента на вопросы по соответствующим видам занятий при текущем контроле – собеседование, защита лабораторных работ.

Принимается во внимание наличие:

знаний:

- методов, способов и средств получения, хранения и переработки информации;
- принципов построения современных информационно-коммуникационных технологий;

умений:

- использовать источники экономической, социальной, управленческой информации;

навыков:

- применения современных методов сбора, обработки и анализа данных.

Таблица - Показатели и критерии оценивания уровня сформированности компетенции ОПК-3 «способностью использовать основные законы естественнонаучных дисциплин и современные информационно-коммуникационные технологии в профессиональной деятельности»

Результаты освоения (Показатели)	Уровни сформирован-ности	Критерии оценивания	Оценка (шкала оценивания)	Оцениваемая форма контроля
Знать: - методы, способы и средства получения, хранения и переработки информации; - принципы построения современных информационно-коммуникационных технологий; Уметь: - использовать источники экономической, социальной, управленческой информации; Владеть: - навыками применения современных методов сбора, обработки и анализа данных.	Эталонный.	1. Перечислить и дать общую характеристику методов и средств получения, хранения и переработки информации. 2. Перечислить основные принципы построения современных информационно-коммуникационных технологий. 3. Дать оценку возможностей использования различных источников экономической, социальной, управленческой информации для решения задач информационной безопасности. 4. Рационально применять современные методы сбора и обработки информации.	5	Конспект лекций студента, Отчёт по лабораторным работам, Защита лабораторных работ, Собеседование, РГР, Экзамен
	Продвинутый	1. Перечислить и дать общую характеристику методов и средств получения, хранения и переработки информации. 2. Перечислить основные принципы построения современных информационно-коммуникационных технологий. 3. Дать оценку возможностей использования различных источников экономической, социальной, управленческой информации для решения задач информационной безопасности.	4	

	Пороговый	1. Перечислить и дать общую характеристику методов и средств получения, хранения и переработки информации. 2. Перечислить основные принципы построения современных информационно-коммуникационных технологий.	3	
	Ниже порогового	Исключительно плохо ориентируется в основных принципах построения ИКТ	2	

Для оценки уровня сформированности компетенции ОПК-4 «способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности» в рамках данной дисциплины оценивается содержательная сторона и качество материалов, представленных в конспектах лекций, отчетах студента по лабораторным работам, отчете студента по расчетно-графической работе. Учитываются также ответы студента на вопросы по соответствующим видам занятий при текущем контроле – собеседование, защита лабораторных работ.

Принимается во внимание наличие:

знаний:

- видов и источников угроз безопасности информации для различных профессиональных областей;
- законодательной базы в сфере информационной безопасности;
- основных требований информационной безопасности.

умений:

- определять актуальные источники угроз безопасности для различных профессиональных областей.

навыков:

- владения современных средств информационной безопасности.

Таблица - Показатели и критерии оценивания уровня сформированности компетенции ОПК-4 «способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности»

Результаты освоения (Показатели)	Уровни сформирован-ности	Критерии оценивания	Оценка (шкала оценивания)	Оцениваемая форма контроля
Знать: - виды и источники угроз безопасности информации для различных профессиональных областей; - законодательную базу в сфере информационной безопасности; - основные требования информационной безопасности.	Эталонный.	1. Перечислить и дать общую характеристику видов и источников угроз безопасности. Основные требования по организации защиты информации. 2. Оценивать источники угроз информационной безопасности для различных профессиональных областей. 3. Использовать современные средства защиты информации.	5	Конспект лекций студента; Отчёт по лабораторным работам; Защита лабораторных работ; Собеседование, РГР; Экзамен.

Уметь: - определять актуальные источники угроз безопасности для различных профессиональных областей. **Владеть:** - навыками владения современных средств информационной безопасности.	Продвинутый	1. Перечислить и дать общую характеристику видов и источников угроз безопасности. Основные требования по организации защиты информации. 2. Оценивать источники угроз информационной безопасности для различных профессиональных областей.	4	
	Пороговый	1. Перечислить и дать общую характеристику видов и источников угроз безопасности. Основные требования по организации защиты информации.	3	
	Ниже порогового	Исключительно плохо ориентируется в основных требованиях к организации защиты информации	2	

Для оценки сформированности в рамках данной дисциплины компетенции ПК-14 «способностью осуществлять ведение базы данных и поддержку информационного обеспечения решения прикладных задач» преподавателем оценивается содержательная сторона и качество материалов, представленных в конспектах лекций, отчетах студента по лабораторным работам, отчете студента по расчетно-графической работе. Учитываются также ответы студента на вопросы по соответствующим видам занятий при текущем контроле – собеседование, защита лабораторных работ.

Принимается во внимание наличие:

знаний:

- основных методов администрирования базы данных (БД);
- основных элементов информационной поддержки решения задачи защиты информации.

умений:

- проводить анализ методы администрирования БД, для обеспечения информационной безопасности;

навыков:

- ведения БД, которые обеспечивают приемлемый уровень информационной безопасности.

Таблица - Показатели и критерии оценивания уровня сформированности компетенции ПК-14 «способностью осуществлять ведение базы данных и поддержку информационного обеспечения решения прикладных задач»

Результаты освоения (Показатели)	Уровни сформированности	Критерии оценивания	Оценка (шкала оценивания)	Оцениваемая форма контроля
Знать: - основные методы администрирования базы данных (БД); - основные элементы информационной поддержки решения задачи защиты информации. **Уметь:** - проводить анализ методы	Эталонный.	1. Перечислить и дать общую характеристику методов администрирования БД, а также основных элементов информационной поддержки решения задачи защиты информации. 2. Проводить сравнительную характеристику различных методов администрирования	5	Конспект лекций студента; Отчёт по лабораторным работам; Защита лабораторных работ; Собеседование,

администрирования БД, для обеспечения информационной безопасности; **Владеть:** - навыками ведения БД, которые обеспечивают приемлемый уровень информационной безопасности.		БД, позволяющих обеспечить защиту данных. 3. Использовать методы администрирования БД, обеспечивающие приемлемый уровень информационной безопасности.		РГР; Экзамен.
	Продвинутый	1. Перечислить и дать общую характеристику методов администрирования БД, а также основных элементов информационной поддержки решения задачи защиты информации. 2. Проводить сравнительную характеристику различных методов администрирования БД, позволяющих обеспечить защиту данных.	4	
	Пороговый	1. Перечислить и дать общую характеристику методов администрирования БД, а также основных элементов информационной поддержки решения задачи защиты информации.	3	
	Ниже порогового	Исключительно плохо ориентируется в назначении и применении методов защиты БД	2	

Для оценки сформированности в рамках данной дисциплины компетенции ПК-18 «способностью принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью» преподавателем оценивается содержательная сторона и качество материалов, представленных в конспектах лекций, отчетах студента по лабораторным работам, отчете студента по расчетно-графической работе. Учитываются также ответы студента на вопросы по соответствующим видам занятий при текущем контроле – собеседование, защита лабораторных работ.

Принимается во внимание наличие:

знаний:

- основных методов и средств управления информационной безопасностью;

умений:

- выбирать методы и разрабатывать средства защиты информации;

навыков:

- работы с инструментальными средствами обеспечения информационной безопасности.

Таблица - Показатели и критерии оценивания уровня сформированности компетенции ПК-18 «способностью принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью»

Результаты освоения (Показатели)	Уровни сформированности	Критерии оценивания	Оценка (шкала оценивания)	Оцениваемая форма контроля
Знать: - основные методы и средства управления информационной безопасностью;	Эталонный.	1. Перечислить и дать общую характеристику основных методов и средств управления информационной безопасностью.	5	Конспект лекций студента; Отчёт по лабораторным

Уметь: - выбирать методы и разрабатывать средства защиты информации; **Владеть:** - навыками работы с инструментальными средствами обеспечения информационной безопасности.		2. Проводить сравнительную характеристику различных методов и средств защиты информации. 3. Использовать методы и инструментальные средства обеспечения информационной безопасности.		работам; Защита лабораторных работ; Собеседование, РГР; Экзамен.
	Продвинутый	1. Перечислить и дать общую характеристику основных методов и средств управления информационной безопасностью. 2. Проводить сравнительную характеристику различных методов и средств защиты информации.	4	
	Пороговый	1. Перечислить и дать общую характеристику основных методов и средств управления информационной безопасностью.	3	
	Ниже порогового	Исключительно плохо ориентируется в назначении и применении методов и средств управления информационной безопасностью	2	

Критерии оценки результатов сформированности компетенций при использовании различных форм контроля.

Критерии оценивания конспекта лекций:

- оценки «отлично» заслуживает студент, который привел развёрнутые ответы на все вопросы конспектирования с приведением фактов и примеров;
- оценки «хорошо» заслуживает студент, который привел развёрнутые ответы на все вопросы конспектирования с незначительным числом фактов и примеров;
- оценки «удовлетворительно» заслуживает студент, который привел ответы на все вопросы конспектирования;
- оценки «неудовлетворительно» заслуживает студент, который не предоставил конспект.

Критерии оценивания собеседования (устного опроса):

- оценки «отлично» заслуживает студент, который полно и развернуто ответил на вопрос;
- оценки «хорошо» заслуживает студент, который полно ответил на вопрос;
- оценки «удовлетворительно» заслуживает студент, который не полно ответил на вопрос;
- оценки «неудовлетворительно» заслуживает студент, который не ответил на вопрос.

Критерии оценивания результатов уровня сформированности компетенций по выполнению лабораторных работ:

- оценки «отлично» заслуживает студент, который выполнил все задания, обосновал выполнение элементов заданий (привел цифровые данные, правильно провел расчеты, привел факты и пр.), оформил работу с учетом ГОСТ и требований кафедры, убедительно, полно и развернуто отвечает на вопросы при защите;
- оценки «хорошо» заслуживает студент, который выполнил все задания, обосновал выполнение элементов заданий (привел цифровые данные, правильно провел расчеты, привел факты и пр.), оформил работу с учетом ГОСТ и требований кафедры, практически отвечает на вопросы во время защиты;

- оценки «удовлетворительно» заслуживает студент, который выполнил все задания, обосновал выполнение элементов заданий (привел цифровые данные, правильно провел расчеты, привел факты и пр.), оформил работу с незначительными отклонениями в требованиях ГОСТ и кафедры, ошибается в ответах на вопросы во время защиты, но исправляет ошибки при ответе на наводящие вопросы;

- оценки «неудовлетворительно» заслуживает студент, который выполнил не все задания, не обосновал выполнение элементов заданий (не привел цифровые данные, неправильно провел расчеты, не привел факты и пр.), оформил работу с грубыми нарушениями ГОСТ и требований кафедры, практически не отвечает на вопросы во время защиты.

Критерии оценивания расчетно-графической работы:

- оценки «отлично» заслуживает студент, который привел полные, точные и развёрнутые материалы по работам/заданиям, оформил отчет по РГР с учетом ГОСТ и требований кафедры;

- оценки «хорошо» заслуживает студент, который привел полные, не совсем точные и развёрнутые материалы по работам/заданиям, оформил отчет по РГР с учетом ГОСТ и требований кафедры, однако не выдержал объем отчета по РГР;

- оценки «удовлетворительно» заслуживает студент, который привел не полные, не совсем точные материалы по работам/заданиям, оформил работу с незначительными отклонениями в требованиях ГОСТ и кафедры;

- оценки «неудовлетворительно» заслуживает студент, который привел не полные, не совсем точные материалы по работам/заданиям, сделал существенные ошибки в расчетах и выводах, оформил работу с грубыми нарушениями ГОСТ и требований кафедры.

Формой промежуточной аттестации по данной дисциплине является экзамен.

Экзамен проводится в устной форме. Критерии оценивания (в соответствии с инструктивным письмом ФГБОУ ВО «НИУ «МЭИ» от 14 мая 2012 года № И-23):

Оценки «отлично» заслуживает студент, обнаруживший всестороннее, систематическое и глубокое знание материалов изученной дисциплины, умение свободно выполнять задания, предусмотренные программой, усвоивший основную и знакомый с дополнительной литературой, рекомендованной рабочей программой дисциплины; проявивший творческие способности в понимании, изложении и использовании материалов изученной дисциплины, безупречно ответившему не только на вопросы билета, но и на дополнительные вопросы в рамках рабочей программы дисциплины, правильно выполнившему практическое задание.

Оценки «хорошо» заслуживает студент, обнаруживший полное знание материала изученной дисциплины, успешно выполняющий предусмотренные задания, усвоивший основную литературу, рекомендованную рабочей программой дисциплины; показавшему систематический характер знаний по дисциплине, ответившему на все вопросы билета, правильно выполнившему практические задание, но допустившему при этом непринципиальные ошибки.

Оценки «удовлетворительно» заслуживает студент, обнаруживший знание материала изученной дисциплины в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, справляющийся с выполнением заданий, знакомы с основной литературой, рекомендованной рабочей программой дисциплины; допустившим погрешность в ответе на теоретические вопросы и/или при выполнении практических заданий, но обладающий необходимыми знаниями для их устранения под руководством преподавателя, либо неправильно выполнившему практическое задание, но по указанию преподавателя выполнившим другие практические задания из того же раздела дисциплины.

Оценка «неудовлетворительно» выставляется студенту, обнаружившему серьезные пробелы в знаниях основного материала изученной дисциплины, допустившему принципиальные ошибки в выполнении заданий, не ответившему на все вопросы билета и дополнительные вопросы и неправильно выполнившему практическое задание (неправильное выполнение только практического задания не является однозначной причиной для выставления оценки «неудовлетворительно»). Как правило, оценка «неудовлетворительно ставится

студентам, которые не могут продолжить обучение по образовательной программе без дополнительных занятий по соответствующей дисциплины (формирования и развития компетенций, закреплённых за данной дисциплиной). Оценка «неудовлетворительно» выставляется также, если студент: после начала экзамена отказался его сдавать или нарушил правила сдачи экзамена (списывал, подсказывал, обманом пытался получить более высокую оценку и т.д.

В зачетную книжку студента и выписку к диплому выносится оценка экзамена по дисциплине за 8 семестр.

6.3 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

Оценка знаний, умений и навыков в процессе изучения дисциплины производится с использованием фонда оценочных средств.

Примерный перечень вопросов по закреплению теоретических знаний, умений и практических навыков, предусмотренных компетенциями (вопросы к экзамену)

1. Основные понятия и определения информационной безопасности.
2. Виды и источники угроз безопасности информации.
3. Классификация угроз информационной безопасности.
4. Методы и средства защиты информации.
5. Правовые меры обеспечения информационной безопасности.
6. Законодательные и нормативные акты Российской Федерации в области защиты информации.
7. Классификация систем защиты АС согласно документам Федеральной службы по техническому и экспортному контролю России (ранее Гостехкомиссии России).
8. Критерии оценки безопасности компьютерных систем. «Оранжевая книга».
9. Защита программного обеспечения, основанная на идентификации аппаратного и программного обеспечения.
10. Электронные ключи.
11. Организационно-административные методы защиты информационных систем.
12. Формирование политики безопасности организации.
13. Основные принципы формирования пользовательских паролей.
14. Идентификация пользователей (назначение и способы реализации).
15. Аутентификация пользователей (назначение и способы реализации).
16. Авторизации пользователей (назначение и способы реализации).
17. Криптографические методы защиты информации.
18. Симметричные криптосистемы.
19. Поточные шифры.
20. Свойства синхронных и асинхронных поточных шифров.
21. Шифры подстановки и перестановки.
22. Блочные шифры.
23. Шифр Файстеля.
24. Основные особенности стандарта шифрования DES.
25. Стандарт шифрования ГОСТ 28147-89.
26. Асимметричные криптосистемы.
27. Алгоритм шифрования RSA.
28. Сравнительная характеристика симметричных и асимметричных алгоритмов шифрования.

29. Реализация алгоритмов шифрования.
30. Электронная цифровая подпись.
31. Виды атак на электронную цифровую подпись.
32. Основные типы криптоаналитических атак.
33. Защита информации в компьютерных сетях.
34. Объекты защиты информации в сети.
35. Уровни сетевых атак согласно эталонной модели взаимодействия открытых систем OSI.
36. Потенциальные угрозы безопасности в Internet.
37. Методы защиты информации в сети Internet.
38. Использование межсетевых экранов для обеспечения информационной безопасности в Internet.
39. Классификация межсетевых экранов.
40. Схемы подключения межсетевых экранов.
41. Частные виртуальные сети (VPN).
42. Классификация VPN.
43. Защита информации на уровне межсетевого протокола Internet Protocol (IP). Протокол IPSecurity.
44. Количественный подход к информационной безопасности. Оценка защищенности механизмов защиты.
45. Методы защиты от вредоносных программ («червей», «троянских программ» и т.д.).
46. Анализ рынка антивирусных программ.
47. Комплексная защита информационных систем.
48. Управление доступом. Избирательное управление доступом.
49. Управление доступом. Полномочное (мандатное) управление доступом.
50. Организация защиты программного обеспечения от исследования.

В ходе выполнения расчетно-графической работа необходимо выполнить два задания: теоретическое и практическое.

Теоретическое задание состоит в анализе и формировании рекомендаций по построению системы защиты АИС для заданной предметной области.

Во время выполнения расчетно-графической работы учащийся проводит анализ конкретной предметной области. Результатом выполнения теоретического задания должен быть перечень рекомендаций для обеспечения комплексной безопасности заданной предметной области.

Примерная тематика заданий:

1. Система информационной безопасности для ИС для учета движения товаров на складе мелкооптовой торговли.
2. Система информационной безопасности для ИС для автоматизации обработки платежных поручений.
3. Система информационной безопасности для ИС для учета расчетов по кредитам физических лиц коммерческого банка.
4. Система информационной безопасности для ИС составления сметы на ремонтно-строительные работы.
5. Система информационной безопасности для ИС агентства трудоустройства.

Практическое задание состоит в программной реализации криптографического метода (ассиметричный алгоритм RSA) защиты.

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

Процедуры оценивания знаний, умений, навыков, характеризующих этапы формирования компетенций, изложены в п.6.1 и 6.2 настоящей программы и в методических указаниях для обучающихся по освоению дисциплины.

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

а) основная литература:

1 Шаньгин В.Ф. Информационная безопасность [электронный ресурс]: учебное пособие/ Шаньгин В.Ф. - М. Изд. «ДМК Пресс», 2014. – 702с. Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=50578
2 Андрианов В.В., Зефиров С.Л. и др. Обеспечение информационной безопасности бизнеса [электронный ресурс]. М.: Альпина Паблишерз, 2011 – 373 с. Режим доступа: http://biblioclub.ru/index.php?page=book&id=235577&sr=1

б) дополнительная литература:

1 Аверченков В.И. Аудит информационной безопасности [электронный ресурс]: учебное пособие/ В.И. Аверченков. М. :Флинта, 2011 – 269с. Режим доступа: http://biblioclub.ru/index.php?page=book&id=93245&sr=1
2 Беломойцев Д.Е., Волосатова Т.М., Радионов С.В. Основные методы криптографической обработки данных [электронный ресурс]: учебное пособие / Беломойцев Д.Е. – М. Изд. МГТУ им. Н.Э. Баумана (Московский государственный технический университет имени Н.Э. Баумана), 2014. – 76с. Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=58438
3 Бирюков А.А. Информационная безопасность: защита и нападение [электронный ресурс]: учебник / Бирюков А.А. – М. Изд. «ДМК Пресс», 2012. – 474с. Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=39990

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» необходимых для освоения дисциплины

1 Лаборатория Касперского [электронный ресурс]: http://www.kaspersky.ru
2 Информационная безопасность. Защита информации [электронный ресурс]: http://all-ib.ru
3 Information Security / Информационная безопасность. Журнал [электронный ресурс]: http://www.itsec.ru/main.php
4 Консультант плюс [электронный ресурс]: http://www.consultant.ru/online/

9. Методические указания для обучающихся по освоению дисциплины

Дисциплина предусматривает лекции и лабораторные работы, а также выполнение расчетно-графической работы. Изучение курса завершается *экзаменом*.

Успешное изучение курса требует посещения лекций, активной работы на лабораторных работах, выполнения всех учебных заданий преподавателя, ознакомления с основной и дополнительной литературой.

Во время лекции студент должен вести краткий конспект. Работа с конспектом лекций предполагает просмотр конспекта в тот же день после занятий. При этом необходимо пометить

материалы конспекта, которые вызывают затруднения для понимания. При этом обучающийся должен стараться найти ответы на затруднительные вопросы, используя рекомендуемую литературу. Если ему самостоятельно не удалось разобраться в материале, необходимо сформулировать вопросы и обратится за помощью к преподавателю на консультации или ближайшей лекции.

Обучающемуся необходимо регулярно отводить время для повторения пройденного материала, проверяя свои знания, умения и навыки по контрольным вопросам.

Лабораторные работы составляют важную часть профессиональной подготовки студентов. Они направлены на экспериментальное подтверждение теоретических положений и формирование учебных и профессиональных практических умений.

Выполнение студентами лабораторных работ направлено на:

- обобщение, систематизацию, углубление, закрепление полученных теоретических знаний по конкретным темам дисциплин;

- формирование необходимых профессиональных умений и навыков;

Названия лабораторных работ фиксируется в разделе 4 настоящей рабочей программы.

Необходимыми структурными элементами лабораторной работы, помимо самостоятельной деятельности студентов, являются инструктаж, проводимый преподавателем, а также организация обсуждения итогов выполнения лабораторной работы.

Выполнению лабораторных работ предшествует проверка знаний студентов – их теоретической готовности к выполнению задания.

Развитие и закрепление теоретических знаний, умений и практических навыков, предусмотренных компетенциями, закрепленными за дисциплиной, осуществляется в ходе самостоятельного выполнения обучающимися заданий расчетно-графической работы (РГР).

При подготовке к **экзамену** в дополнение к изучению конспектов лекций и учебных пособий, необходимо пользоваться учебной литературой, рекомендованной в настоящей программе. При подготовке к экзамену нужно изучить теорию: определения всех понятий и подходы к оцениванию до состояния понимания материала и самостоятельно решить по нескольку типовых задач из каждой темы. При решении задач всегда необходимо уметь качественно интерпретировать итог решения.

Самостоятельная работа студентов (СРС) по дисциплине играет важную роль в ходе всего учебного процесса. Методические материалы и рекомендации для обеспечения СРС готовятся преподавателем и выдаются студенту.

Методические материалы и рекомендации для обеспечения самостоятельной работы студентов представлены в методических указаниях для обучающихся по освоению дисциплины.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

При проведении **лабораторных работ** предусматривается использование пакетов прикладных программ, средств разработки ПО и Интернет-ресурсы.

Пакет программ: MS Office, Антивирусные программы (Kaspersky Endpoint Security), Delphi

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Лекционные занятия проводятся в обычной аудитории, оснащенной учебной мебелью и доской (№218 либо аналогичная).

Лабораторные работы по данной дисциплине проводятся в компьютерном классе № А317 оборудованным компьютерами с современными лицензионными программно-

технологическими средствами, с доступом к сети Интернет, столом для конференций, доской, многофункциональными устройствами.

Автор:

канд. техн. наук, доцент  Б.В. Окунев

Зав. кафедрой МИТЭ

д-р техн. наук, профессор  М.И. Дли

Программа одобрена на заседании кафедры Менеджмента и информационных технологий в экономике от 28 августа 2015 года, протокол № 1.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Номер изменения	Номера страниц				Всего страниц в документе	Наименование и № документа, вводящего изменения	Подпись, Ф.И.О. внесшего изменения в данный экземпляр	Дата внесения изменения в данный экземпляр	Дата введения изменения
	измененных	замененных	новых	аннулированных					
1	2	3	4	5	6	7	8	9	10