Приложение Л.РПД Б1.Б.8

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
«___» _____ 2016 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

(НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ)

Направление подготовки: 09.04.03 Прикладная информатика

Магистерская программа: Информационные системы и технологии в управлении бизнес-процессами

Уровень высшего образования: магистратура

Нормативный срок обучения: 2 года

Учебный план, утвержденный 29.04.16 (год начала подготовки – 2016 г.)

Смоленск – 2016 г.

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

Целью освоения дисциплины является подготовка обучающихся к научно-исследовательской и организационно-управленческой деятельностям по направлению подготовки 09.04.03 Прикладная информатика (магистерская программа: Информационные системы и технологии в управлении бизнес–процессами) посредством обеспечения этапов формирования компетенций, предусмотренных ФГОС, 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 документах 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 защиты компьютерной информации.

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 «Методы и средства защиты компьютерной информации» направлена на формирование следующих общекультурных, общепрофессиональных, профессиональных компетенций:

ОК-2 готовностью действовать в нестандартных ситуациях, нести социальную и этическую ответственность за принятые решения

В результате изучения дисциплины студент должен:

Знать:

- основные элементы нестандартных подходов обеспечения защиты компьютерной информации;

Уметь:

- проводить анализ элементов нестандартных ситуаций при обеспечении защиты компьютерной информации;

Владеть:

- навыками действий в нестандартных ситуациях при отражении угроз информационной безопасности.

ОПК-6 способностью к профессиональной эксплуатации современного электронного оборудования в соответствии с целями основной образовательной программы магистратуры

В результате изучения дисциплины обучающийся должен:

Знать:

- основные элементы современного электронного оборудования, обеспечивающего информационную безопасность;

Уметь:

- проводить анализ элементов современного электронного оборудования;

Владеть:

- навыками эксплуатации современного электронного оборудования в соответствии с целями образовательной программы магистратуры.

ПК-2 способностью формализовывать задачи прикладной области, при решении которых возникает необходимость использования количественных и качественных оценок
В результате изучения дисциплины студент должен:
Знать:
- количественные и качественные метрики защиты информации;
Уметь:
- проводить анализ количественных и качественных оценок параметров информационной безопасности;
Владеть:
- навыками применения количественных и качественных метрик защиты информации.

ПК-3 способностью ставить и решать прикладные задачи в условиях неопределенности и определять методы и средства их эффективного решения
В результате изучения дисциплины обучающийся должен:
Знать:
- основные способы решения задач информационной безопасности для различных предметных областей в условиях неполной информации (неопределенности);
Уметь:
- проводить сравнительный анализ способов описания неопределенности;
Владеть:
- навыками использования методов и средств решения задач информационной безопасности в условиях неопределенности.

ПК-5 способностью исследовать применение различных научных подходов к автоматизации информационных процессов и информатизации предприятий и организаций
В результате изучения дисциплины обучающийся должен:
Знать:
- основные элементы технологий информатизации предприятий и организаций, обеспечивающих достаточный уровень защиты информации;
Уметь:
- обосновывать выбор технологии информатизации предприятий и организаций;
Владеть:
- навыками применения технологий автоматизации информационных процессов и информатизации предприятий, обеспечивающих достаточный уровень защиты информации.

2. Место дисциплины в структуре образовательной программы

Дисциплина относится к вариативной части блока 1 «Дисциплина (модули)» образовательной программы подготовки магистров по магистерской программе: Информационные системы и технологии в управлении бизнес–процессами направления 09.04.03 Прикладная информатика (индекс дисциплины в соответствии с учебным планом: Б1. Б. 8)

В соответствии с учебным планом по направлению 09.04.03 Прикладная информатика дисциплина «Методы и средства защиты компьютерной информации» (Б1. Б. 8) базируется на следующих дисциплинах:

«Философские проблемы науки и техники»
«Методология научного исследования»
«Моделирование информационных процессов и систем»
«Инструментальные методы поддержки решений»
«Современные информационные технологии в экономике»
«Маркетинговый анализ рынка информационных технологий»

«Современные технологии баз и банков данных»
«Алгоритмические основы мультимедийных технологий»
«Аналитические исследования в экономике»

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

«Инструментальные методы поддержки решений»
«Маркетинговый анализ рынка информационных технологий»

Знания, умения и навыки, полученные студентами в процессе изучения дисциплины, являются базой для прохождения учебной, технологической, педагогической и преддипломной практик, для выполнения научно-исследовательской работы, для прохождения государственной итоговой аттестации (выпускная квалификационная работа - магистерская диссертация).

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:	Вариативная часть	
Индекс дисциплины по учебному плану:	Б1. Б. 8	
Часов (всего) по учебному плану:	180	3 семестр
Трудоемкость в зачетных единицах (ЗЕТ)	5	3 семестр
Лекции (ЗЕТ, часов)	1 ЗЕТ, 36 час	3 семестр
Практические занятия (ЗЕТ, часов)	----------	----------
Лабораторные работы (ЗЕТ, часов)	1 ЗЕТ, 36 час	3 семестр
Курсовая работа (ЗЕТ, часов)	0,5 ЗЕТ, 18 час	3 семестр
Объем самостоятельной работы по учебному плану (ЗЕТ, часов всего)	125 ЗЕТ, 90 час	3 семестр
Зачет с оценкой (в объеме самостоятельной работы)	0,5 ЗЕТ,18 час	3 семестр
Экзамен	----------	------

Самостоятельная работа студентов

Вид работ	Трудоёмкость, ЗЕТ, час
Изучение материалов лекций (лк)	0,5 ЗЕТ, 18 час
Подготовка к практическим занятиям (пз)	----------
Подготовка к защите лабораторной работы (лаб)	1 ЗЕТ, 36 час
Выполнение расчетно-графической работы	----------
Выполнение реферата	----------
Выполнение курсовой работы	0,5 ЗЕТ, 18 час
Самостоятельное изучение дополнительных материалов дисциплины (СРС)	0,25 ЗЕТ, 9 час
Подготовка к тестированию	----------
Подготовка к зачету	0,25 ЗЕТ, 9 час
Всего (в соответствии с УП)	**2,5 ЗЕТ, 90 час**
Подготовка к экзамену	----------

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	КР	СРС	в т.ч. интеракт.
1	2	3	4	5	6	7	8	9
1	Основные положения теории информационной безопасности. Основные нормативные руководящие документы, законы РФ и т.п. касающиеся государственной тайны и защиты информации.	16	4	-	-	4	8	-
2	Защита программного обеспечения, основанная на идентификации пользователя, идентификации ПК и идентификации исполняемого модуля.	34	6	-	10	-	18	4
3	Использование криптографических методов защиты информации.	52	8	-	10	8	26	4
4	Виды вредоносных программ (компьютерных вирусов) и методы борьбы с ними.	24	4	-	8	-	12	4
5	Организация комплексной защиты автоматизированных ИС.	44	8	-	8	6	22	6
6	Таксономия нарушений информационной безопасности. Оценка надежности защитных механизмов.	10	6	-	-	-	4	-
всего по видам учебных занятий		**180**	**36**	**-**	**36**	**18**	**90**	**18**

Содержание по видам учебных занятий

Тема 1 Основные положения теории информационной безопасности. Основные нормативные руководящие документы, законы РФ и т.п. касающиеся государственной тайны и защиты информации.

Самостоятельная работа студента (СРС, 8 час)

Подготовка к лекции (2 час).

Выполнение курсовой работы (4 час)

Изучение дополнительного теоретического материала (1 час)

Подготовка к зачету (1 час)

Текущий контроль:

- устный опрос: собеседование;

- письменный опрос: конспект дополнительных материалов, проверка выполнения курсовой работы.

контроль с помощью технических средств и информационных технологий: мультимедийная презентация курсовой работы -слайды по теме.

Тема 2 Защита программного обеспечения, основанная на идентификации пользователя, идентификации ПК и идентификации исполняемого модуля.

Лабораторная работа 1-6. Защита от несанкционированного использования программ, основанная на привязке программного обеспечения к аппаратным средствам конкретного компьютера и использовании электронного ключа (12 час).

Самостоятельная работа студента (СРС, 18 час)

Подготовка к лекции (4 час).

Подготовка к защите лабораторной работы (10 час).

Изучение дополнительного теоретического материала (2 час).

Подготовка к зачету (2 час)

Текущий контроль:

- устный опрос: собеседование; защита лабораторной работы;

- письменный опрос: конспект дополнительных материалов, проверка отчета по лабораторной работе.

Тема 3 Использование криптографических методов защиты информации.

Лабораторная работа 7-12. Изучение и использование различных методов криптографии для защиты данных. (12 час).

Самостоятельная работа студента (СРС, 26 час)

Подготовка к лекции (4 час).

Подготовка к защите лабораторной работы (10 час).

Выполнение курсовой работы (8 час)

Изучение дополнительного теоретического материала (2 час).

Подготовка к зачету (2 час)

Текущий контроль:

- устный опрос: собеседование; защита лабораторной работы;

- письменный опрос: конспект дополнительных материалов, проверка выполнения курсовой работы; проверка отчета по лабораторной работе.

контроль с помощью технических средств и информационных технологий: мультимедийная презентация курсовой работы -слайды по теме.

Тема 4 Виды вредоносных программ (компьютерных вирусов) и методы борьбы с ними.

Лабораторная работа 13-18. Изучение программных средств, обеспечивающих защиту от вредоносных программ (12 час).

Самостоятельная работа студента (СРС, 12 час)

Подготовка к лекции (2 час).

Подготовка к защите лабораторной работы (8 час).

Изучение дополнительного теоретического материала (1 час).

Подготовка к зачету (1 час)

Текущий контроль:

- устный опрос: собеседование; защита лабораторной работы;

- письменный опрос: конспект дополнительных материалов, проверка отчета по лабораторной работе.

Тема 5 Организация комплексной защиты автоматизированных ИС.

Лабораторная работа 19-27. Организация комплексной защиты информационных систем (18 час).

Самостоятельная работа студента (СРС, 22 часов)

Подготовка к лекции (4 час).

Подготовка к защите лабораторной работы (8 час).

Выполнение курсовой работы (6 час)

Изучение дополнительного теоретического материала (2 час).

Подготовка к зачету (2 час)

Текущий контроль:
- устный опрос: собеседование; защита лабораторной работы;
- письменный опрос: конспект дополнительных материалов, проверка выполнения курсовой работы; проверка отчета по лабораторной работе.
контроль с помощью технических средств и информационных технологий: мультимедийная презентация курсовой работы -слайды по теме.

Тема 6 Таксономия нарушений информационной безопасности. Оценка надежности защитных механизмов.

Самостоятельная работа студента (СРС, 4 час)
Подготовка к лекции (2 час).
Изучение дополнительного теоретического материала (1 час).
Подготовка к зачету (1 час)
Текущий контроль:
- устный опрос: собеседование;
- письменный опрос: конспект дополнительных материалов.

Промежуточная аттестация по дисциплине:
Изучение дисциплины заканчивается зачетом с оценкой. Зачет 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.

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

Для обеспечения самостоятельной работы разработаны:
Учебно-методическое обеспечение аудиторной и внеаудиторной самостоятельной работы студентов, обучающихся по дисциплине «Методы и средства защиты компьютерной информации» 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: ОК-2, ОПК-6, ПК-2, ПК-3, ПК-5.
Указанные компетенции формируются в соответствии со следующими этапами:
1. Формирование и развитие теоретических знаний, предусмотренных указанными компетенциями (самостоятельная работа студентов).
2. Приобретение и развитие практических умений, предусмотренных компетенциями (лабораторные работы, самостоятельная работа студентов).
3. Закрепление теоретических знаний, умений и практических навыков, предусмотренных компетенциями, в ходе защит лабораторных работ, успешной сдачи зачета с оценкой.
Матрица соотнесения тем/разделов дисциплины и формируемых в них компетенций

Темы, разделы дисциплины	Количество часов	Код компетенции					
		ОК-2	ОПК-6	ПК-2	ПК-3	ПК-5	Σ общее количество компетенций
Тема 1. Основные положения теории информационной безопасности. Основные нормативные руководящие документы, законы РФ и т.п. касающиеся государственной тайны и защиты информации.	16	+		+			2
Тема 2. Защита программного обеспечения, основанная на идентификации пользователя, идентификации ПК и идентификации исполняемого модуля.	34		+			+	2
Тема 3. Использование криптографических методов защиты информации.	52				+		1
Тема 4. Виды вредоносных программ (компьютерных вирусов) и методы борьбы с ними.	24					+	1
Тема 5. Организация комплексной защиты автоматизированных ИС.	44	+	+				2
Тема 6. Таксономия нарушений информационной безопасности. Оценка надежности защитных механизмов.	10			+			1
Итого	**180**	2	2	2	1	2	9

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 ОК-2 «готовностью действовать в нестандартных ситуациях, нести социальную и этическую ответственность за принятые решения» преподавателем оценивается содержательная сторона и качество материалов, представленных в конспектах дополнительных материалов, в отчетах студента по лабораторным работам, в отчете по курсовой работе. Учитываются также ответы студента на вопросы по соответствующим видам занятий при текущем контроле – собеседование, защита лабораторных работ.

Принимается во внимание

- наличие знаний основных элементов нестандартных подходов к защите информации;
- наличие умений и присутствие навыков действовать в нестандартных ситуациях при обеспечении информационной безопасности.

Таблица - Показатели и критерии оценивания уровня сформированности компетенции ОК-2 «готовностью действовать в нестандартных ситуациях, нести социальную и этическую ответственность за принятые решения»

Результаты освоения (Показатели)	Уровни сформирован-ности	Критерии оценивания	Оценка (шкала оценивания)	Оцениваемая форма контроля
Знать: - основные элементы нестандартных подходов обеспечения защиты компьютерной информации; **Уметь:** - проводить анализ элементов нестандартных ситуаций при обеспечении защиты компьютерной информации; **Владеть:** - навыками действий в нестандартных ситуациях при отражении угроз информационной безопасности.	Эталонный.	1. Перечислить и дать общую характеристику основных нестандартных подходов защиты компьютерной информации. 2. Проводить анализ нестандартных подходов в области защиты информации. 3. Эффективно использовать эвристические методы защиты информации.	5	Конспект дополнительных материалов Отчёт по лабораторным работам, Защита лабораторных работ, Собеседование, Отчет по КР Зачет с оценкой
	Продвинутый	1. Перечислить и дать общую характеристику основных нестандартных подходов защиты компьютерной информации. 2. Проводить анализ нестандартных подходов в области защиты информации.	4	
	Пороговый	1. Перечислить и дать общую характеристику основных нестандартных подходов защиты компьютерной информации.	3	
	Ниже порогового	Исключительно слабо знает нестандартные походы к защите информации	2	

Для оценки уровня сформированности компетенции ОПК-6 «способностью к профессиональной эксплуатации современного электронного оборудования в соответствии с целями основной образовательной программы магистратуры» преподавателем оценивается содержательная сторона и качество материалов, представленных в конспектах дополнительных материалов, в отчетах студента по лабораторным работам, в отчетах по курсовой работе. Учитываются также ответы студента на вопросы по соответствующим видам занятий при текущем контроле – собеседование, защита лабораторных работ.

Принимается во внимание

- наличие знаний основных элементов электронного оборудования, используемого для защиты информации;
- наличие умений и присутствие навыков использования электронного оборудования для защиты информации.

Таблица - Показатели и критерии оценивания уровня сформированности компетенции ОПК-6 «способностью к профессиональной эксплуатации современного электронного оборудования в соответствии с целями основной образовательной программы магистратуры»

Результаты освоения (Показатели)	Уровни сформирован-ности	Критерии оценивания	Оценка (шкала оценивания)	Оцениваемая форма контроля
Знать: - основные элементы современного электронного оборудования, обеспечивающего информационную безопасность; **Уметь:** - проводить анализ элементов современного электронного оборудования; **Владеть:** - навыками эксплуатации современного электронного оборудования в соответствии с целями образовательной программы магистратуры.	Эталонный.	1. Перечислить и дать общую характеристику основных элементов современного электронного оборудования, обеспечивающего информационную безопасность. 2. Проводить анализ нестандартных подходов в современные электронные оборудования. 3. Эффективно использовать электронное оборудования для обеспечения защиты информации.	5	Конспект дополнительных материалов Отчёт по лабораторным работам, Защита лабораторных работ, Собеседование, Отчет по КР Зачет с оценкой
	Продвинутый	1. Перечислить и дать общую характеристику основных элементов современного электронного оборудования, обеспечивающего информационную безопасность. 2. Проводить анализ нестандартных подходов в современные электронные оборудования.	4	
	Пороговый	1. Перечислить и дать общую характеристику основных элементов современного электронного оборудования, обеспечивающего информационную безопасность	3	
	Ниже порогового	Исключительно слабо знает основные элементы электронного оборудования, обеспечивающего ИБ	2	

Для оценки уровня сформированности компетенции ПК-2 «способностью формализовывать задачи прикладной области, при решении которых возникает необходимость использования количественных и качественных оценок» преподавателем оценивается содержательная сторона и качество материалов, представленных в конспектах дополнительных материалов. Учитываются также ответы студента на вопросы по соответствующим видам занятий при текущем контроле – собеседование.

Принимается во внимание

- наличие знаний основных количественные и качественные метрики информационной безопасности;
- наличие умений и присутствие навыков применения количественных и качественных метрик информационной безопасности;

Таблица - Показатели и критерии оценивания уровня сформированности компетенции ПК-2 «способностью формализовывать задачи прикладной области, при решении которых возникает необходимость использования количественных и качественных оценок»

Результаты освоения (Показатели)	Уровни сформирован-ности	Критерии оценивания	Оценка (шкала оценивания)	Оцениваемая форма контроля
Знать: - количественные и качественные метрики защиты информации; **Уметь:** - проводить анализ количественных и качественных оценок параметров информационной безопасности; **Владеть:** - навыками применения количественных и качественных метрик защиты информации.	Эталонный.	1. Перечислить и дать общую характеристику основных количественных и качественных метрик, используемых в области информационной безопасности. 2. Проводить анализ количественных и качественных оценок параметров информационной безопасности. 3. Эффективно использовать различные метрики в таксономии надежности защитных механизмов.	5	Собеседование, Зачет с оценкой
	Продвинутый	1. Перечислить и дать общую характеристику основных количественных и качественных метрик, используемых в области информационной безопасности. 2. Проводить анализ количественных и качественных оценок параметров информационной безопасности.	4	
	Пороговый	1. Перечислить и дать общую характеристику основных количественных и качественных метрик, используемых в области информационной безопасности.	3	
	Ниже порогового	Практически не знает количественные и качественные метрики, используемые в области ИБ	2	

Для оценки уровня сформированности компетенции ПК-3 «способностью ставить и решать прикладные задачи в условиях неопределенности и определять методы и средства их эффективного решения» преподавателем оценивается содержательная сторона и качество материалов, представленных в конспектах дополнительных материалов, в отчетах студента по лабораторным работам. Учитываются также ответы студента на вопросы по соответствующим видам занятий при текущем контроле – собеседование, защита лабораторных работ.

Принимается во внимание

- наличие знаний факторов неопределенности при решении задач информационной безопасности;
- наличие умений и присутствие навыков применения методов защиты информации в условиях неопределенности.

Таблица - Показатели и критерии оценивания уровня сформированности компетенции ПК-3 «способностью ставить и решать прикладные задачи в условиях неопределенности и определять методы и средства их эффективного решения»

Результаты освоения (Показатели)	Уровни сформирован-ности	Критерии оценивания	Оценка (шкала оценивания)	Оцениваемая форма контроля
Знать: - основные способы решения задач информационной безопасности для различных предметных областей в условиях неполной информации (неопределенности); **Уметь:** - проводить сравнительный анализ способов описания неопределенности; **Владеть:** - навыками использования методов и средств решения задач информационной безопасности в условиях неопределенности.	Эталонный.	1. Перечислить и дать общую характеристику основных методов решения задачи обеспечения информационной безопасности в условиях действия факторов неопределенности. 2. Проводить анализ методов решения задачи обеспечения информационной безопасности в условиях действия факторов неопределенности. 3. Эффективно использовать методов решения задачи обеспечения информационной безопасности в условиях действия факторов неопределенности.	5	Конспект дополнительных материалов Отчёт по лабораторным работам, Защита лабораторных работ, Собеседование, Отчет по КР Зачет с оценкой
	Продвинутый	1. Перечислить и дать общую характеристику основных методов решения задачи обеспечения информационной безопасности в условиях действия факторов неопределенности. 2. Проводить анализ методов решения задачи обеспечения информационной безопасности в условиях действия факторов неопределенности.	4	
	Пороговый	1. Перечислить и дать общую характеристику основных методов решения задачи обеспечения информационной безопасности в условиях действия факторов неопределенности.	3	
	Ниже порогового	Исключительно слабо знает назначение и применение методов решения задачи информационной безопасности в условиях неопределенности	2	

Для оценки уровня сформированности компетенции ПК-5 «способностью исследовать применение различных научных подходов к автоматизации информационных процессов и информатизации предприятий и организаций» преподавателем оценивается содержательная сторона и качество материалов, представленных в конспектах дополнительных материалов, в отчетах студента по лабораторным работам. Учитываются также ответы студента на вопросы по соответствующим видам занятий при текущем контроле – собеседование, защита лабораторных работ.

Принимается во внимание

- наличие знаний о особенностях информатизации предприятий с точки зрения защиты информации;
- наличие умений и присутствие навыков применения методов защиты информации в условиях информатизации предприятий.

Таблица - Показатели и критерии оценивания уровня сформированности компетенции ПК-5 «способностью исследовать применение различных научных подходов к автоматизации информационных процессов и информатизации предприятий и организаций»

Результаты освоения (Показатели)	Уровни сформирован-ности	Критерии оценивания	Оценка (шкала оценивания)	Оцениваемая форма контроля
Знать: - основные элементы технологий информатизации предприятий и организаций, обеспечивающих достаточный уровень защиты информации; **Уметь:** - обосновывать выбор технологии информатизации предприятий и организаций; **Владеть:** - навыками применения технологий автоматизации информационных процессов и информатизации предприятий, обеспечивающих достаточный уровень защиты информации.	Эталонный.	1. Перечислить и дать общую характеристику основных технологий информатизации предприятий и организаций, обеспечивающих достаточный уровень защиты информации. 2. Проводить анализ технологий, обеспечивающих приемлемый уровень информационной безопасности. 3. Эффективно использовать современные методы и технологии защиты информации.	5	Конспект дополнительных материалов Отчёт по лабораторным работам, Защита лабораторных работ, Собеседование, Зачет с оценкой
	Продвинутый	1. Перечислить и дать общую характеристику основных технологий информатизации предприятий и организаций, обеспечивающих достаточный уровень защиты информации. 2. Проводить анализ технологий, обеспечивающих приемлемый уровень информационной безопасности.	4	
	Пороговый	1. Перечислить и дать общую характеристику основных технологий информатизации предприятий и организаций, обеспечивающих достаточный уровень защиты информации.	3	
	Ниже порогового	Исключительно слабо знает технологии информатизации предприятий, которые обеспечивают заданный уровень защиты информации	2	

Критерии оценки результатов сформированности компетенций при использовании различных форм контроля.

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 результатов уровня сформированности компетенции в процессе выполнения и защиты курсовой работы представлены в таблице.

Таблица - Критерии оценивания сформированности компетенций в процессе выполнения и защиты курсовой работы

Критерии оценки (компетенции)	Уровень освоения компетенций (оценка в баллах)				Баллы
	эталонный (5)	продвинутый (4)	пороговый (3)	ниже порогового (2)	
Актуальность темы (ПК-3)	Актуальность темы работы аргументирована.	Актуальность темы работы сравнительно аргументирована.	Актуальность темы работы недостаточно аргументирована.	Актуальность темы работы не аргументирована.	
Содержание (раскрытие темы, достижение цели, выполнение задач) (ОК-2, ОПК-6, ПК-2, ПК-3, ПК-5)	Теоретическое содержание темы полностью раскрыто; проведен полный анализ практического материала; аргументированы выводы, обоснованы предложения. Цель достигнута. Задачи выполнены.	Теоретическое содержание темы в основном раскрыто; анализ практического материала недостаточно полный; выводы недостаточно аргументированы, предложения в основном обоснованы. Цель достигнута. Задачи выполнены.	Теоретическое содержание темы раскрыто поверхностно; анализ практического материала не полный; выводы сформулированы в общей форме и не конкретны; неполное обоснование предложений. Цель достигнута частично.	Теоретическое содержание темы не раскрыто; достаточно поверхностный анализ практического материала; выводы и предложения не сформулированы. Поставленная цель не достигнута. Задачи не выполнены.	
Оформление работы (ПК-5)	Строго в соответствии с требованиями.	Допущено несколько незначительных неточностей.	Оформление с допустимыми погрешностями.	Значительные нарушения требований.	
Доклад и презентация (ОПК-6)	Доклад содержателен, логичен; отражает результаты работы, лимит времени не превышен. Студент не читает доклад с листа, показывает высокое владение профессиональным языком. Презентация не повторяет текст доклада, содержит графики, схемы, иллюстрирующие результаты работы. Информация отлично читаема с экрана; цветовое оформление не мешает восприятию информации, текст	Доклад относительно содержателен, логичен, в основном отражает результаты работы, лимит времени превышен незначительно. Студент не читает доклад с листа, хорошо владеет профессиональным языком. Презентация незначительно повторяет текст доклада, содержит графики, схемы, в основном иллюстрирующие результаты работы. Информация хорошо читаема; цветовое оформление не	Доклад логически не проработан, плохо отражает результаты работы, лимит времени превышен значительно. Студент в основном читает доклад с листа, удовлетворительно владеет профессиональным языком. Презентация значительно повторяет текст доклада, содержит графики, схемы, недостаточно полно иллюстрирующие результаты работы. Информация удовлетворительно читаема с экрана;	Доклад не содержателен, логически не выстроен, не отражает результаты работы, лимит времени превышен значительно. Студент читает доклад с листа, слабо владеет профессиональным языком. Презентация повторяет текст доклада; содержит в основном текстовые слайды слабо иллюстрирующие результаты работы. Информация плохо читаема с экрана; цветовое оформление мешает восприятию	

	не содержит ошибок.	способствует хорошему восприятию информации.	цветовое оформление неудачное.	информации, текст содержит большое количество ошибок	
Ответы на вопросы (ОК-2, ОПК-6, ПК-2, ПК-5)	Ответы правильные, полные, логичные, убедительные; высокое владение профессиональным языком, аргументированная защита своей точки зрения.	Ответы в основном правильные, полные, логичные; хорошее владение профессиональным языком, средняя аргументация и защита своей точки зрения	Не на все вопросы даны полные, логичные ответы; удовлетворительное владение профессиональным языком, низкая способность защиты своей точки зрения	Отсутствие правильных ответов на вопросы; плохое владение профессиональным языком, неспособность защиты своей точки зрения	

В результате изучения дисциплины обучающийся должен:

Сформированность уровня компетенции не ниже порогового является основанием для допуска студента к промежуточной аттестации по данной дисциплине.

Совокупный результат определяется как среднее арифметическое значение оценок по всем видам текущего контроля.

Формой промежуточной аттестации по данной дисциплине в 3 семестре является зачет с оценкой, оцениваемый по принятой в ФГБОУ ВО «НИУ «МЭИ» четырехбалльной системе: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Зачет с оценкой проводится в устной форме (собеседование). Критерии оценивания:

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, но и на дополнительные вопросы в рамках рабочей программы дисциплины, правильно выполнившему практические задания.

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, правильно выполнившему практические задания, но допустившему при этом непринципиальные ошибки.

Оценки «удовлетворительно» заслуживает студент, обнаруживший знание материала изученной дисциплины в объеме, необходимом для дальнейшей учебы и предстоящей профессиональной деятельности, справляющийся с выполнением заданий, знакомый с основной литературой, рекомендованной рабочей программой дисциплины; допустивший 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 выполнивший 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 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 дисциплине (формирования и развития компетенций, закрепленных за данной дисциплиной). Оценка «неудовлетворительно» выставляется также, если студент отказался сдавать зачет или нарушил правила сдачи зачета (списывал, подсказывал, обманом пытался получить более высокую оценку и т.д.).

Оценка по зачету выводится с учетом совокупного результата освоения всех компетенций по данной дисциплине (в соответствии с инструктивным письмом НИУ МЭИ от 14 мая 2012 года № И-23). Оценка зачета по дисциплине определяется как среднее арифметическое значение оценок по всем видам текущего контроля и оценки итогового собеседования.

В зачетную книжку студента и выписку к диплому выносится оценка зачета по дисциплине за 3 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.

Вопросы по закреплению теоретических знаний, умений и практических навыков, предусмотренных компетенциями (вопросы к зачету)

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 курсовой работы 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 курсовой работы учащийся проводит анализ конкретной предметной области. Результатом выполнения теоретического задания должен быть перечень рекомендаций для обеспечения комплексной безопасности заданной предметной области (формирование политики безопасности).

Примерная тематика заданий:

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

Практическое задание состоит в программной реализации ключа шифрования для криптографической системы (симметричный алгоритм) 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 указания для обучающихся по освоению дисциплины.

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

а) основная литература:

1 Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации [электронный ресурс] : учебное пособие / Ю.Н. Загинайлов. - М. ; Берлин : Директ-Медиа, 2015. - 253 с. Режим доступа: http://biblioclub.ru/index.php?page=book&id=276557
2 Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях [электронный ресурс] : учебное пособие / М.А. Иванов, И.В. Чугунков ; Министерство образования и науки Российской Федерации, Национальный исследовательский ядерный университет «МИФИ» ; под ред. М.А. Иванов. - М. : МИФИ, 2012. - 400 с. Режим доступа : http://biblioclub.ru/index.php?page=book&id=231673

б) дополнительная литература:

1 Федеральный закон Российской Федерации от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с исправлениями и дополнениями). Принят Государственной Думой 8 июля 2006 г., одобрен Советом Федерации 14 июля 2006 г. - Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61798/
2 Разработка моделей криптографической защиты информации [электронный ресурс] : монография / В.Г. Шубович, В.В. Капитанчук, Н.С. Знаенко, Ю.И. Титаренко ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Ульяновский государственный педагогический университет имени И.Н. Ульянова». - Ульяновск : УлГПУ, 2013. - 128 с. Режим доступа : http://biblioclub.ru/index.php?page=book&id=278070
3 Гуц А.К. Теория игр и защита компьютерных систем : методические указания / А.К. Гуц, Т.В. Вахний ; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования. «Омский Государственный университет им. Ф.М. Достоевского». - Омск : Омский государственный университет, 2013. - 160 с. Режим доступа : http://biblioclub.ru/index.php?page=book&id=237190
4 Разрушающие программные воздействия / . - М. : МИФИ, 2011. - 328 с. Режим доступа : http://biblioclub.ru/index.php?page=book&id=231881
5 Спицын В.Г. Информационная безопасность вычислительной техники : учебное пособие / В.Г. Спицын ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). - Томск : Эль Контент, 2011. - 148 с. Режим доступа : http://biblioclub.ru/index.php?page=book&id=208694
6 Фефилов А.Д. Методы и средства защиты информации в сетях [электронный ресурс] / А.Д. Фефилов. - М. : Лаборатория книги, 2011. - 105 с. Режим доступа : http://biblioclub.ru/index.php?page=book&id=140796

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

1. Лаборатория Касперского [электронный ресурс]: http://www.kaspersky.ru
2. Ассоциация предприятий компьютерных информационных технологий (АПКИТ) [электронный ресурс]: http://www.apkit.ru
3. Информационная безопасность. Защита информации [электронный ресурс]: http://all-ib.ru
4. Information Security / Информационная безопасность. Журнал [электронный ресурс]: http://www.itsec.ru/main.php
5. Энциклопедия хакера [электронный ресурс]: http://www.inattack.ru
6. Консультант плюс [электронный ресурс]: http://www.consultant.ru/online/

9. Методические указания для обучающихся по освоению дисциплины

Дисциплина предусматривает лабораторные работы. Изучение дисциплины завершается *зачетом с оценкой*.

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

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;

Содержание 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.

При подготовке к **зачету** необходимо пользоваться учебной литературой, рекомендованной к настоящей программе. При подготовке к зачету нужно изучить определения всех понятий и теоретические подходы до состояния понимания материала и самостоятельно решить несколько типовых задач из каждой темы. При решении задач всегда необходимо уметь качественно интерпретировать полученные результаты.

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 пакетов прикладных программ, средств разработки ПО и Интернет-ресурсов.

1. Пакет программ: MS Office, Антивирусные программы (Open source software – открытое ПО), Firebird (Open source software – открытое ПО), Delphi
2. Поисковые Интернет - сервера.

При выполнении **курсовой работы** студентами предусматривается использование программного обеспечения Microsoft Office.

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

Лабораторные работы по данной дисциплине проводятся в компьютерном классе № 206 (или аналогичном классе, подключенном к локальной сети), оснащенном лицензионными программно-техническими средствами, с доступом к сети Интернет; оборудованном столом для конференции, многофункциональным устройством, доской.

Авторы

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 26 августа 2016 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