Приложение 3.РПД Б1.В.ДВ.2.2

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 научной работе
_____ М.И. Дли
«31» 08 2015 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

(НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ)

Направление подготовки: 38.06.01 Экономика

Направленность: Математические и инструментальные методы экономики

Уровень высшего образования: подготовка кадров высшей квалификации

Нормативный срок обучения: 3 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 научно-исследовательской деятельности в экономике по направлению подготовки 38.06.01 Экономика (направленность «Математические и инструментальные методы экономики») посредством обеспечения этапов формирования компетенций, предусмотренных ФГОС, в части представленных ниже знаний, умений и навыков.

Задачами дисциплины является получение обучающимися:

- знаний о современных тенденциях угроз информационной безопасности, о нормативных правовых документах по защите информации, а так же о современных методах и средствах обеспечения информационной безопасности в экономических информационных системах;
- умений выявлять угрозы информационной безопасности, использовать нормативные правовые документы по защите информации, исследовать, использовать и развивать современные методы и средства обеспечения информационной безопасности;
- навыков владения приемами разработки политики безопасности предприятия и навыками использования методов и средств обеспечения информационной безопасности в социально-экономических информационных системах (СЭИС).

То есть, задачами дисциплины является изучение основных теоретических положений и методов, формирование умений и привитие навыков применения теоретических знаний для решения прикладных задач, а также развитие новых подходов к обеспечению информационной безопасности в сфере экономики.

Дисциплина «Информационная безопасность» направлена на формирование следующих компетенций:

ОПК-1 способностью самостоятельно осуществлять научно-исследовательскую деятельность в соответствующей профессиональной области с использованием современных методов исследования и информационно-коммуникационных технологий

В результате изучения дисциплины аспирант должен:

Знать:

- современные методы научных исследований и информационно-коммуникационных технологий в области организации информационной безопасности социально-экономических информационных систем (СЭИС);

Уметь:

- проводить сравнительную оценку эффективности различных методов научных исследований и информационно-коммуникационных технологий в области организации информационной безопасности СЭИС;

Владеть:

- навыками оценки эффективности использования информационно-коммуникационных технологий в области организации информационной безопасности.

ПК-1 готовностью к решению сложных задач в области математического анализа экономических процессов

В результате изучения дисциплины аспирант должен:

Знать:

- основные математические методы, используемые для организации защиты информации в экономических процессах;

Уметь:

- проводить анализ эффективности математических методов, применяемых для организации защиты информации в экономических процессах;

Владеть:

- навыками оценки эффективности математических методов, применяемых для организации защиты информации в экономических процессах.

ПК-4 способностью развивать методы обеспечения информационной безопасности в социально-экономических системах

В результате изучения дисциплины аспирант должен:

Знать:

- основные организационно-административные методы управления информационной безопасностью;
- основные тенденции развития организационно-административных методов обеспечения информационной безопасности;

Уметь:

- развивать организационно-административные методы защиты информации;

Владеть:

- навыками оценки эффективности организационно-административных методов защиты информации в социально-экономических системах.

2. Место дисциплины в структуре образовательной программы

Дисциплина относится к дисциплинам по выбору направления 38.06.01 Экономика, направленность «Математические и инструментальные методы экономики» (индекс дисциплины в соответствии с учебным планом: Б1.В.ДВ. 2.2).

В соответствии с учебным планом по направлению 38.06.01 Экономика дисциплина «Информационная безопасность» (Б1.В.ДВ.2.2) базируется на дисциплинах «Системный анализ в экономике», «Имитационное моделирование экономических процессов».

Знания, умения и навыки, полученные аспирантами в процессе изучения дисциплины, являются базой для изучения дисциплин «Методы аккумулирования знаний», «Математические и инструментальные методы экономики», «Системы поддержки принятия решений в экономике», «Иностранный язык».

Знания, умения и навыки, полученные аспирантами в процессе изучения дисциплины, являются базой для выполнения научных исследований и государственной итоговой аттестации.

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	Курс (семестр)
Часть цикла:	Вариативная часть	
Индекс дисциплины по учебному плану:	Б1.В. ДВ. 2.2	
Часов (всего) по учебному плану:	144	2 курс (3 семестр)
Трудоемкость в зачетных единицах (ЗЕТ)	4	2 курс (3 семестр)
Лекции (ЗЕТ, часов)	0,5 ЗЕТ, 18 час.	2 курс (3 семестр)
Практические занятия (ЗЕТ, часов)	-	-
Лабораторные работы (ЗЕТ, часов)	-	-
Объем самостоятельной работы по учебному плану (ЗЕТ, часов всего)	3 ЗЕТ, 108 час.	2 курс (3 семестр)
Зачет с оценкой	0,5 ЗЕТ, 18 час.	2 курс (3 семестр)
Экзамен	-	-

Самостоятельная работа аспирантов

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)	-
Самостоятельное изучение дополнительных материалов дисциплины (СРС)	1,78 ЗЕТ, 64 час
Подготовка материалов для участия в групповой дискуссии	0,72 ЗЕТ 26 час
Всего (в соответствии с УП)	**3 ЗЕТ, 108 час**
Подготовка к зачету	0,5 ЗЕТ, 18 час
Подготовка к экзамену	-

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

№ п/п	Темы дисциплины	Всего часов на тему	Виды учебной занятий, включая самостоятельную работу аспирантов и трудоемкость (в часах) (*в соответствии с УП*)				
			лк	пр	лаб	СРС	Контроль (зачет)
1	2	3	4	5	6	8	9
1	Современная нормативно-законодательная база обеспечения информационной безопасности.	22	2	-	-	18	2
2	Анализ возможных нарушений и атак в социально-экономических информационных системах (СЭИС). Исследование влияния и противодействие вредоносным программам в СЭИС.	28	4	-	-	20	4
3	Анализ возможностей методов криптографии, которые могут быть использованы в целях защиты данных. Применение крипто-графических систем шифрования данных.	32	4	-	-	24	4
4	Исследование эффективности методов защиты информации в корпоративных вычисли-ельных сетях (Интранет) и глобальной сети Интернет.	32	4	-	-	24	4
5	Аудит информационной безопасности. Анализ информационных рисков.	30	4	-	-	22	4
	всего по видам учебных занятий	**144**	**18**	**-**	**-**	**108**	**18**

Содержание по видам учебных занятий

Тема 1. Современная нормативно-законодательная база обеспечения информационной безопасности.

Лекция 1. Современная нормативно-законодательная база обеспечения информационной безопасности (2 час).

Самостоятельная работа (СРС, 18 час)

Подготовка к лекции (2 час).

Изучение дополнительного теоретического материала (12 час).

Подготовка материалов для участия в групповой дискуссии (4 час)

Подготовка к зачету (2 часа)

Текущий контроль:

- устный опрос: собеседование; групповая дискуссия на тему «Государственная тайна».

Тема 2. Анализ возможных нарушений и атак в социально-экономических информационных системах. Исследование влияния и противодействие вредоносным программам в СЭИС.

Лекция 2. Анализ возможных нарушений и атак в социально-экономических информационных системах (СЭИС) (2 час).

Лекция 3. Исследование влияния и противодействие вредоносным программам в СЭИС (2 час).

Самостоятельная работа (СРС, 20 час)

Подготовка к лекции (4 час).

Изучение дополнительного теоретического материала (12 час).

Подготовка материалов для участия в групповой дискуссии (4 час)

Подготовка к зачету (4 час)

Текущий контроль:

- **устный опрос:** собеседование; групповая дискуссия на тему «Оценка эффективности способов защиты флеш - памяти от компьютерных вирусов».

Тема 3. Анализ возможностей методов криптографии, которые могут быть использованы в целях защиты данных. Применение криптографических систем шифрования данных.

Лекция 4. Анализ возможностей методов криптографии, которые могут быть использованы в целях защиты данных (2 час).

Лекция 5. Применение криптографических систем шифрования данных (2 час).

Самостоятельная работа (СРС, 24 час)

Подготовка к лекции (4 час).

Изучение дополнительного теоретического материала (14 час).

Подготовка материалов для участия в групповой дискуссии (6 час)

Подготовка к зачету (4 час)

Текущий контроль:

- **устный опрос:** собеседование; групповая дискуссия на тему «Электронная цифровая подпись (ЭЦП): достоинства и недостатки. Оценка доверия к ЭЦП»

Тема 4. Исследование эффективности методов защиты информации в корпоративных вычислительных сетях (Интранет) и глобальной сети Интернет.

Лекция 6. Исследование эффективности методов защиты информации в корпоративных вычислительных сетях (Интранет) (2 час).

Лекция 7. Исследование эффективности методов защиты информации в глобальной сети Интернет (2 час).

Самостоятельная работа (СРС, 24 час)

Подготовка к лекции (4 час).

Изучение дополнительного теоретического материала (14 час).

Подготовка материалов для участия в групповой дискуссии (6 час)

Подготовка к зачету (4 час)

Текущий контроль:

- **устный опрос:** собеседование; групповая дискуссия на тему «Источники угроз информационной безопасности в глобальной сети Интернет».

Тема 5. Аудит информационной безопасности. Анализ информационных рисков.

Лекция 8. Аудит информационной безопасности (2 час).

Лекция 9. Анализ информационных рисков (2 час).

Самостоятельная работа (СРС, 22 час)

Подготовка к лекции (4 час).

Изучение дополнительного теоретического материала (12 час).

Подготовка материалов для участия в групповой дискуссии (6 час)

Подготовка к зачету (4 час)

Текущий контроль:

- **устный опрос:** собеседование; групповая дискуссия на тему «Сценарии анализа информационных рисков»

Промежуточная аттестация по дисциплине:

Изучение дисциплины заканчивается зачетом с оценкой. Зачет с оценкой проводится в соответствии с Положением о порядке организации и проведения промежуточной аттестации обучающихся по программам подготовки научно-педагогических кадров в аспирантуре (ред.2 утверждена директором филиала ФГБОУ ВО «НИУ «МЭИ» в г. Смоленске А.С. Федуловым 08.09.2015 г.). Зачет с оценкой 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 к самостоятельной работе аспирантов.

Учебно-методическое обеспечение аудиторной и внеаудиторной самостоятельной работы аспирантов, 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, ПК-1, ПК-4.

Указанные компетенции формируются в соответствии со следующими этапами:

1. Формирование и развитие теоретических знаний, предусмотренных указанными компетенциями (лекционные занятия, самостоятельная работа аспирантов).
2. Приобретение и развитие практических умений, предусмотренных компетенциями (самостоятельная работа аспирантов).
3. Закрепление теоретических знаний, умений и практических навыков, предусмотренных компетенциями в ходе успешной сдачи зачета с оценкой.

Матрица соотнесения тем/разделов дисциплины и формируемых в них компетенций

Темы, разделы дисциплины	Количество часов	Код компетенции			
		ОПК-1	ПК-1	ПК- 4	Σ общее количество компетенций
Тема 1. Современная нормативно-законодательная база обеспечения информационной безопасности.	22			+	1
Тема 2. Анализ возможных нарушений и атак в социально-экономических информационных системах (СЭИС). Исследование влияния и противодействие вредоносным программам в СЭИС.	28	+		+	2
Тема 3. Анализ возможностей методов криптографии, которые могут быть использованы в целях защиты данных. Применение криптографических систем шифрования данных.	32	+	+		2
Тема 4. Исследование эффективности методов защиты информации в корпоративных вычислительных сетях (Интранет) и глобальной сети Интернет.	32			+	1
Тема 5. Аудит информационной безопасности. Анализ информационных рисков.	30		+		1
Итого	**144**	2	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.

При оценке уровня сформированности компетенции ОПК-1 «способностью самостоятельно осуществлять научно-исследовательскую деятельность в соответствующей профессиональной области с использованием современных методов исследования и информационно-коммуникационных технологий» в рамках данной дисциплины учитываются ответы аспиранта на вопросы при собеседовании, а также его активное и эффективное участие в групповых дискуссиях.

Кроме этого, во время проведения зачета аспирант должен уметь развернуто и аргументированно отвечать на следующие вопросы:

1. Потенциальные угрозы безопасности в корпоративных вычислительных сетях (Интранет). Методы защиты информации в Интранет.
2. Потенциальные угрозы безопасности в Интернет (и в частности в электронной коммерции). Методы защиты информации в сети Интернет.
3. Формирование политики безопасности предприятия (организации).
4. Основные методы и средства защиты информации, применяемые в корпоративных экономических информационных системах (КЭИС).
5. Защита информации в компьютерных сетях. Объекты защиты информации в сети.
6. Использование межсетевых экранов для обеспечения информационной безопасности в Интернет.
7. Частные виртуальные сети (VPN). Классификация VPN.

Таблица - Показатели и критерии оценивания уровня сформированности компетенции ОПК-1 «способностью самостоятельно осуществлять научно-исследовательскую деятельность в соответствующей профессиональной области с использованием современных методов исследования и информационно-коммуникационных технологий»

Результаты освоения (Показатели)	Уровни сформирован-ности	Критерии оценивания	Оценка (шкала оценивания)	Оцениваемая форма контроля
Знать: - современные методы научных исследований и информационно-коммуникационных технологий в области организации информационной безопасности социально-экономических информационных систем (СЭИС);	Эталонный.	1. Перечислить и дать общую характеристику современных методов научных исследований и информационно-коммуникационных технологий в области организации информационной безопасности социально-экономических информационных систем 2. Дать оценку возможностей использования современных методов научных исследований	5	Собеседование, Групповая дискуссия, Зачет с оценкой

Уметь: - проводить сравнительную оценку эффективности различных методов научных исследований и информационно-коммуникационных технологий в области организации информационной безопасности СЭИС; **Владеть:** - навыками оценки эффективности использования информационно-коммуникационных технологий в области организации информационной безопасности.		и информационно-коммуникационных технологий в области организации информационной безопасности. 3. Эффективно проводить оценку использования информационно-коммуникационных технологий для решения задач информационной безопасности СЭИС.		
	Продвинутый	1. Перечислить и дать общую характеристику современных методов научных исследований и информационно-коммуникационных технологий в области организации информационной безопасности социально-экономических информационных систем 2. Дать оценку возможностей использования современных методов научных исследований и информационно-коммуникационных технологий в области организации информационной безопасности.	4	
	Пороговый	1. Перечислить и дать общую характеристику современных методов научных исследований и информационно-коммуникационных технологий в области организации информационной безопасности социально-экономических информационных систем	3	
	Ниже порогового	Исключительно плохо ориентируется в современных информационно-коммуникационных технологиях, обеспечивающих приемлемый уровень информационной безопасности.	2	

При оценке сформированности в рамках данной дисциплины компетенции ПК-1 «готовностью к решению сложных задач в области математического анализа экономических процессов» в рамках данной дисциплины учитываются ответы аспиранта на вопросы при собеседовании, а также его активное и эффективное участие в групповых дискуссиях.

Кроме этого, во время проведения зачета аспирант должен уметь развернуто и аргументированно отвечать на следующие вопросы:

1. Количественный подход к информационной безопасности. Оценка защищенности механизмов защиты.
2. Аудит информационной безопасности.
3. Управление информационными рисками.
4. Идентификация пользователей, аутентификация пользователей и авторизация пользователей (назначение и способы реализации).
5. Криптографические методы защиты информации. Математическое и алгоритмическое обеспечение криптографических методов защиты информации.
6. Симметричные и асимметричные криптосистемы.

Таблица - Показатели и критерии оценивания уровня сформированности компетенции ПК-1 «готовностью к решению сложных задач в области математического анализа экономических процессов»

Результаты освоения (Показатели)	Уровни сформирован-ности	Критерии оценивания	Оценка (шкала оценивания)	Оцениваемая форма контроля
Знать: - основные математические методы, используемые для организации защиты информации в экономических процессах; **Уметь:** - проводить анализ эффективности математических методов, применяемых для организации защиты информации в экономических процессах; **Владеть:** - навыками оценки эффективности математических методов, применяемых для организации защиты информации в экономических процессах.	Эталонный.	1. Перечислить и дать общую характеристику математических методов, используемых для организации защиты информации в экономических процессах. 2. Дать оценку эффективности математических методов, применяемых для организации защиты информации в экономических процессах. 3. Прогнозировать возможные пути развития математических методов защиты информации.	5	Собеседование, Групповая дискуссия, Зачет с оценкой
	Продвинутый	1. Перечислить и дать общую характеристику математических методов, используемых для организации защиты информации в экономических процессах. 2. Дать оценку эффективности математических методов, применяемых для организации защиты информации в экономических процессах.	4	
	Пороговый	1. Перечислить и дать общую характеристику математических методов, используемых для организации защиты информации в экономических процессах.	3	
	Ниже порогового	Исключительно плохо ориентируется в основных принципах построения систем защиты информации	2	

При оценке уровня сформированности компетенции ПК-4 «способностью развивать методы обеспечения информационной безопасности в социально-экономических системах» в рамках данной дисциплины в рамках данной дисциплины учитываются ответы аспиранта на вопросы при собеседовании, а также его активное и эффективное участие в групповых дискуссиях.

Кроме этого, во время проведения зачета аспирант должен уметь развернуто и аргументированно отвечать на следующие вопросы:

1. Организационно-административные методы защиты, применяемые в социально-экономических информационных системах.
2. Электронная цифровая подпись. Использование ЭЦП в экономических системах.
3. Использование электронных ключей для организации информационной безопасности в КЭИС.
4. Основные понятия и определения информационной безопасности. Особенности защиты информации в социально-экономических информационных системах (СЭИС)
5. Методы защиты от вредоносных программ в СЭИС.

6. Правовые меры обеспечения информационной безопасности в социально-экономических информационных системах (СЭИС).

7. Законодательные и нормативные акты Российской Федерации в области защиты информации.

Таблица - Показатели и критерии оценивания уровня сформированности компетенции ПК-4 «способностью развивать методы обеспечения информационной безопасности в социально-экономических системах»

Результаты освоения (Показатели)	Уровни сформированности	Критерии оценивания	Оценка (шкала оценивания)	Оцениваемая форма контроля
Знать: - основные организационно-административные методы управления информационной безопасностью; - основные тенденции развития организационно-административных методов обеспечения информационной безопасности; **Уметь:** - развивать организационно-административные методы защиты информации; **Владеть:** - навыками оценки эффективности организационно-административных методов защиты информации в социально-экономических системах.	Эталонный.	1. Перечислить и дать общую характеристику современных организационно-административных методов защиты информации 2. Оценивать организационно-административные методы защиты информации. 3. Прогнозировать возможные пути совершенствования организационно-административные методов защиты информации.	5	Собеседование, Групповая дискуссия, Зачет с оценкой
	Продвинутый	1. Перечислить и дать общую характеристику современных организационно-административных методов защиты информации 2. Оценивать организационно-административные методы защиты информации.	4	
	Пороговый	1. Перечислить и дать общую характеристику современных организационно-административных методов защиты информации.	3	
	Ниже порогового	Исключительно плохо ориентируется в основных требованиях к организации защиты информации	2	

Критерии оценки результатов сформированности компетенций при использовании различных форм контроля.

Критерии оценивания собеседования (устного опроса):

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

Критерии оценивания групповой дискуссии:

- оценки «отлично» заслуживает аспирант, который подготовил необходимые материалы к групповой дискуссии и активно участвует в ней. При этом он аргументированно отстаивает свою точку зрения и предлагает креативные методы решения выявленных проблем.

- оценки «хорошо» заслуживает аспирант, который подготовил необходимые материалы к групповой дискуссии и активно участвует в ней. При этом он отстаивает свою точку зрения, но не предлагает способов решения выявленных проблем.

- оценки «удовлетворительно» заслуживает аспирант, который подготовил необходимые материалы к групповой дискуссии и участвует в ней.

- оценки «неудовлетворительно» заслуживает аспирант, не подготовившийся к групповой дискуссии и не принимающий в ней активного участия.

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

Формой промежуточной аттестации по данной дисциплине является зачет с оценкой. Зачет с оценкой проводится в устной форме (собеседование).

Критерии оценивания:

Оценки «отлично» заслуживает аспирант, 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 аспирант, 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 аспирант, 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 аспиранту, 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 аспирантам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине (формирования и развития компетенций, закрепленных за данной дисциплиной). Оценка «неудовлетворительно» выставляется также, если аспирант отказался сдавать зачет или нарушил правила сдачи зачета (списывал, 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 Положением о порядке организации и проведения промежуточной аттестации обучающихся по программам подготовки научно-педагогических кадров в аспирантуре (ред.2 утверждена директором филиала ФГБОУ ВО «НИУ «МЭИ» в г. Смоленске А.С. Федуловым 08.09.2015 г.)).

Оценка зачета по дисциплине определяется как среднее арифметическое значение оценок по всем видам текущего контроля и оценки итогового собеседования.

В зачетную книжку аспиранта 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.

Примерный перечень вопросов по закреплению теоретических знаний, умений и практических навыков, предусмотренных компетенциями

1. Основные понятия и определения информационной безопасности. Особенности защиты информации в социально-экономических информационных системах (СЭИС)
2. Основные методы и средства защиты информации, применяемые в корпоративных экономических информационных системах (КЭИС).
3. Правовые меры обеспечения информационной безопасности в социально-экономических информационных системах (СЭИС).
4. Законодательные и нормативные акты Российской Федерации в области защиты информации.
5. Использование электронных ключей для организации информационной безопасности в КЭИС.
6. Организационно-административные методы защиты, применяемые в социально-экономических информационных системах.
7. Формирование политики безопасности предприятия (организации).
8. Идентификация пользователей, аутентификация пользователей и авторизация пользователей (назначение и способы реализации).
9. Криптографические методы защиты информации. Математическое и алгоритмическое обеспечение криптографических методов защиты информации.
10. Симметричные и асимметричные криптосистемы.
11. Электронная цифровая подпись. Использование ЭЦП в экономических системах.
12. Защита информации в компьютерных сетях. Объекты защиты информации в сети.
13. Потенциальные угрозы безопасности в Интранет. Методы защиты информации в Интранет.
14. Потенциальные угрозы безопасности в Интернет (и в частности в электронной коммерции). Методы защиты информации в сети Интернет.
15. Использование межсетевых экранов для обеспечения информационной безопасности в Интернет.
16. Частные виртуальные сети (VPN). Классификация VPN.
17. Количественный подход к информационной безопасности. Оценка защищенности механизмов защиты.
18. Методы защиты от вредоносных программ в СЭИС.
19. Аудит информационной безопасности.
20. Управление информационными рисками.

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

По дисциплине «Информационная безопасность» предусмотрен зачет с оценкой в 3 семестре. Билет к зачету содержит два теоретических вопроса и один практический. Вопрос практического характера позволяет выявить умение практического использования полученных знаний.

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 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
2 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
3 Мельников В.П. Защита информации: Учебное пособие /В.П.Мельников, А.И.Куприянов, А.Г.Схиртладзе. – М: Академия, 2014. – 304с.

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 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
3 Анисимов А.А. Менеджмент в сфере информационной безопасности \ курс лекций [электронный ресурс]. М.: Интернет университет информационных технологий, 2009 -176с. Режим доступа: http://biblioclub.ru/index.php?page=book&id=232981&sr=1
4 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

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

1 Лаборатория Касперского [электронный ресурс]: http://www.kaspersky.ru
2 Information Security / Информационная безопасность. Журнал [электронный ресурс]: http://www.itsec.ru/main.php
3 Энциклопедия хакера [электронный ресурс]: http://www.inattack.ru
4 Консультант плюс [электронный ресурс]: http://www.consultant.ru/online/

9. Методические указания для обучающихся по освоению дисциплины

Дисциплина предусматривает лекции. Изучение курса завершается *зачетом с оценкой*.

Успешное изучение курса требует посещения лекций, выполнения всех учебных заданий преподавателя, ознакомления с основной и дополнительной литературой.

Во время лекции аспирант 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.

При подготовке к **зачету с оценкой** в дополнение к изучению конспектов лекций, необходимо пользоваться учебной литературой, рекомендованной к настоящей программе. При подготовке к зачету 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 аспирантов (СРС) по дисциплине играет важную роль в ходе всего учебного процесса. Методические материалы и рекомендации для обеспечения СРС готовятся преподавателем и выдаются аспиранту.

Методические материалы и рекомендации для обеспечения самостоятельной работы аспирантов представлены в приложении.

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

При проведении **лекционных занятий** предусматривается использование Интернет-ресурсы.

1. Поисковые Интернет - сервера.

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

Лекционные занятия:

Для проведения лекционных занятий необходим класс ПЭВМ (№206 либо аналогичный), подключенный к локальной сети. Учебная аудитория должна соответствовать требованиям пожарной безопасности и охраны труда по освещенности, количеству рабочих (посадочных) мест аспирантов. Учебные лаборатории и кабинеты должны быть оснащены необходимым лабораторным оборудованием (компьютеры), обеспечивающими проведение предусмотренного учебным планом лабораторного практикума (практических занятий) по дисциплине. Освещенность рабочих мест должна соответствовать действующим СНиПам.

Автор
канд. техн. наук, доцент  Окунев Борис Васильевич

Зав. кафедрой МИТЭ
д-р техн. наук, профессор  Дли Максим Иосифович

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