АНО ВО «Межрегиональный открытый социальный институт»

УТВЕРЖДАЮ
Зав. кафедрой информационной
безопасности _____П.В. Никитин
Протокол заседания кафедры
№ 8 «24» марта 2017 г.

РАБОЧАЯ ПРОГРАММА

по дисциплине	Б1.В.ОД.1.1 Методы и системы защиты информации, информационная безопасность (наименование)
направление подготовки программы аспирантуры	10.06.01 Информационная безопасность
направленность подготовки программы аспирантуры (профиль)	Методы и системы защиты информации, информационная безопасность
квалификация (степень) выпускника	Исследователь. Преподаватель-исследователь
форма обучения	Очная / заочная

ПРОГРАММА РАЗРАБОТАНА

д-р техн. наук, проф.
А. В. Горохов
(должность, Ф. И. О., ученая степень, звание автора(ов) программы)

Йошкар-Ола, 2017

Содержание

1. Пояснительная записка

Цель изучения дисциплины: ознакомление с комплексом проблем информационной безопасности предпринимательских структур различных типов и направлений деятельности, построения и функционирования совокупности правовых, организационных, технических и технологических процессов, обеспечивающих информационную безопасность и формирующих структуру системы защиты ценной и конфиденциальной информации в сферах охраны интеллектуальной собственности предпринимателей и сохранности их информационных ресурсов, а также формирование знаний, умений и владений в соответствии с компетентностной моделью, представленной в основной профессиональной образовательной программе по направлению подготовки научно-педагогических кадров высшей квалификации (аспирантура).

Место дисциплины в учебном плане:

Дисциплина «Методы и системы защиты информации, информационная безопасность» относится к обязательным дисциплинам вариативной части учебного плана, программы подготовки научно-педагогических кадров в аспирантуре по направлению подготовки кадров высшей квалификации 10.06.01 Информационная безопасность.

Дисциплина «Методы и системы защиты информации, информационная безопасность» обеспечивает овладение следующими компетенциями:

Код компетенции	Наименование компетенции	Перечень планируемых результатов обучения по дисциплине
ПК-1	способность разрабатывать новые и исследовать существующие методы защиты информации при ее передаче и хранении	Знать: современные методы и средства защиты информации при ее передаче и хранении; существующие защищенные протоколы обмена информацией; современные методы исследования сетевого трафика с целью контроля целостности информации, выявления попыток несанкционированного доступа в информационные системы, обнаружения вредоносных программ; формальные модели политик безопасности, политик управления доступом и информационными потоками в информационных системах. Уметь: обосновывать выбор методов защиты информации при ее передаче и хранении, защищенные протоколы обмена информацией; выявлять возможности совершенствования научных методов и алгоритмов исследования свойств сетевого трафика с целью контроля целостности информации, выявления попыток несанкционированного доступа в информационные системы, обнаружения вредоносных программ. Владеть: навыками применения существующих защищенных протоколов обмена информацией; современными методами исследования сетевого трафика с целью контроля целостности информации, выявления попыток несанкционированного доступа в информационные системы, обнаружения вредоносных программ; современными методами и средствами защиты информации при ее передаче и хранении.
ПК-2	способность применять современные методы моделирования угроз информационной безопасности для решения	Знать: методы установки, настройки и обслуживания технических и программно-аппаратных средств защиты информации Уметь:

	профессиональных задач	осуществлять меры противодействия нарушениям информационной безопасности Владеть: навыками рационального выбора средств и методов защиты объектов информации
ПК-3	способность оценивать эффективность применяемых средств защиты информации	Знать: действующие стандарты в области информационной безопасности; критерии, устанавливающие степень соответствия защищаемых объектов стандартам информационной безопасности Уметь: применять действующие стандарты в области информационной безопасности; применять критерии, устанавливающие степень соответствия защищаемых объектов стандартам информационной безопасности; обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности. Владеть: навыками критического восприятия информации; навыками обоснования оценки степени защищенности объектов информатизации и информационных систем; навыками оценки соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности.
ПК-4	способность квалифицированно проводить научные исследования в области информационной безопасности	Знать: научные подходы к анализу методов информационной безопасности и характеристику ее составляющих. Уметь: обоснованно анализировать защищаемую информацию по критериям конфиденциальности; обоснованно классифицировать и оценивать угрозы информационной безопасности компьютерных систем; применять для решения научных задач в области обеспечения информационной безопасности методологии теоретических и экспериментальных научных исследований. Владеть: специальной профессиональной терминологией в области информационной безопасности; научно обоснованными методами анализа информационной безопасности и построения систем защиты информации от несанкционированного доступа.

Перечень компетенций с указанием этапов их формирования в процессе освоения основной образовательной программы:

Этапы формирования компетенций

Код компетенции	Формулировка компетенции	Очная / заочная форма обучения	
		Учебная дисциплина	Курс
ПК-1	способность разрабатывать новые и исследовать существующие	Научно-исследовательская деятельность и подготовка	1-4

	методы защиты информации при ее передаче и хранении	научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук	
		Методы и системы защиты информации, информационная безопасность	2
		Методы и средства защиты информации	2
		Информационная безопасность инфокоммуникационных системы	2
		Представление научного доклада об основных результатах подготовленной научно-квалификационной работы (диссертации)	3
		Подготовка к сдаче и сдача государственного экзамена	4
ПК-2	способность применять современные методы моделирования угроз информационной безопасности для решения профессиональных задач	Научно-исследовательская деятельность и подготовка научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук	1-4
		Методы и системы защиты информации, информационная безопасность	2
		Методы и средства защиты информации	2
		Информационная безопасность инфокоммуникационных системы	2
		Подготовка к сдаче и сдача государственного экзамена	4
ПК-3	способность оценивать эффективность применяемых средств защиты информации	Научно-исследовательская деятельность и подготовка научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук	1-4
		Методы и системы защиты информации, информационная безопасность	2
		Методы и средства защиты информации	2
		Информационная безопасность инфокоммуникационных системы	2
		Представление научного	3

		доклада об основных результатах подготовленной научно-квалификационной работы (диссертации)	
		Подготовка к сдаче и сдача государственного экзамена	4
ПК-4	способность квалифицированно проводить научные исследования в области информационной безопасности	Общая методология научных исследований	1
		Научно-исследовательская деятельность и подготовка научно-квалификационной работы (диссертации) на соискание ученой степени кандидата наук	1-4
		Методы и системы защиты информации, информационная безопасность	2
		Практика по получению профессиональных умений и опыта профессиональной деятельности (педагогическая практика)	3
		Представление научного доклада об основных результатах подготовленной научно-квалификационной работы (диссертации)	3
		Подготовка к сдаче и сдача государственного экзамена	4

Этапы формирования компетенций: в качестве этапов формирования компетенций в процессе освоения образовательной программы указываются курсы.

Формы текущего контроля успеваемости аспирантов: реферат
Форма промежуточной аттестации: экзамен.

2. Структура и содержания дисциплины

Трудоемкость 9 зачетные единицы, 324 часа, из них:
72 лекционных, 90 практических и 162 часа самостоятельной работы.

2.1. Тематический план учебной дисциплины

№ п/п раздела	Наименование разделов и тем	Количество часов по учебному плану				
		Всего	Виды учебной работы			
			Аудиторная работа			Самостоятельная работа
			Лекции	Практические (семинарские) занятия	Лабораторные занятия	
1	2	3	4	5	6	7
1	**Раздел I. Методы и системы защиты информации**					
2	Тема 1. Законодательные и правовые основы защиты	16	4	4		8

	компьютерной информации информационных технологий.					
3	Тема 2. Вычислительные сети и защита информации.	24	6	6		12
4	Тема 3. Проблемы защиты информации в информационных системах.	16	2	6		8
5	Тема 4. Защита локальных сетей и операционных систем.	26	6	8		12
6	Тема 5. Системы и средства защиты компьютерной информации в информационных системах.	24	6	6		12
7	Тема 6. Требования к содержанию нормативно-методических документов по защите информации.	12	4	2		6
8	Тема 7. Организационно-правовой статус службы информационной безопасности.	10	2	2		6
9	Тема 8. Программно-технические методы и средства защиты информации.	16	4	4		8
10	Тема 9. Типы несанкционированного доступа и условия работы средств защиты.	12	2	4		6
11	**Раздел II. Информационная безопасность**					
12	Тема 1. Изучение традиционных симметричных криптосистем.	18	2	6		10
13	Тема 2. Применение симметричных криптосистем для защиты компьютерной информации в информационных системах.	22	6	6		10
14	Тема 3. Применение асимметричных криптосистем для защиты компьютерной информации в информационных системах.	20	4	6		10
15	Тема 4. Методы идентификации и проверки подлинности пользователей компьютерных систем.	22	4	8		10
16	Тема 5. Защита компьютерных систем от удаленных атак через сеть Internet.	24	6	6		12
17	Тема 6. Изучение существующих аппаратно-программных средств криптографической защиты компьютерной информации серии КРИПТОН.	26	6	8		12
18	Тема 7. Компьютерные вирусы как особый класс разрушающих программных воздействий.	10	2	2		6
19	Тема 8. Комплексная защита процесса обработки информации в компьютерных системах на основе стохастической интеллектуальной информационной технологии.	18	4	4		10
20	Тема 9. Разработка транслятора исходного текста программ, обеспечивающего их защиту на логическом (алгоритмическом) и физическом уровне от НСД, программных закладок и вирусов.	8	2	2		4
	Итого по дисциплине	**324**	**72**	**90**	**-**	**162**

2.2. Тематический план лекционных занятий:

№ п/п раздела	Наименование разделов и тем	Количество часов
1	**2**	**3**
1	**Раздел I. Методы и системы защиты информации**	
2	Тема 1. Законодательные и правовые основы защиты компьютерной информации информационных технологий.	4
3	Тема 2. Вычислительные сети и защита информации.	6

4	Тема 3. Проблемы защиты информации в информационных системах.	2
5	Тема 4. Защита локальных сетей и операционных систем.	6
6	Тема 5. Системы и средства защиты компьютерной информации в информационных системах.	6
7	Тема 6. Требования к содержанию нормативно-методических документов по защите информации.	4
8	Тема 7. Организационно-правовой статус службы информационной безопасности.	2
9	Тема 8. Программно-технические методы и средства защиты информации.	4
10	Тема 9. Типы несанкционированного доступа и условия работы средств защиты.	2
11	**Раздел II. Информационная безопасность**	
12	Тема 1. Изучение традиционных симметричных криптосистем.	2
13	Тема 2. Применение симметричных криптосистем для защиты компьютерной информации в информационных системах.	6
14	Тема 3. Применение асимметричных криптосистем для защиты компьютерной информации в информационных системах.	4
15	Тема 4. Методы идентификации и проверки подлинности пользователей компьютерных систем.	4
16	Тема 5. Защита компьютерных систем от удаленных атак через сеть Internet.	6
17	Тема 6. Изучение существующих аппаратно-программных средств криптографической защиты компьютерной информации серии КРИПТОН.	6
18	Тема 7. Компьютерные вирусы как особый класс разрушающих программных воздействий.	2
19	Тема 8. Комплексная защита процесса обработки информации в компьютерных системах на основе стохастической интеллектуальной информационной технологии.	4
20	Тема 9. Разработка транслятора исходного текста программ, обеспечивающего их защиту на логическом (алгоритмическом) и физическом уровне от НСД, программных закладок и вирусов.	2
	Итого по дисциплине	**72**

Содержание лекционных занятий

Раздел I. Методы и системы защиты информации.

Тема 1. Законодательные и правовые основы защиты компьютерной информации информационных технологий.

Безопасность информационных ресурсов и документирование информации; государственные информационные ресурсы; персональные данные о гражданах; права на доступ к информации; разработка и производство информационных систем.

Тема 2. Вычислительные сети и защита информации.

Нормативно-правовая база функционирования систем защиты информации; компьютерные преступления и особенности их расследования; российское законодательство по защите информационных технологий; промышленный шпионаж и законодательство, правовая защита программного обеспечения авторским правом.

Тема 3. Проблемы защиты информации в информационных системах.

Меры по обеспечению сохранности информации и угрозы ее безопасности в информационных системах; основные задачи обеспечения безопасности информации в информационных системах.

Тема 4. Защита локальных сетей и операционных систем.

Интеграция систем защиты; Internet в структуре информационно-аналитического обеспечения информационных систем; рекомендации по защите информации в Internet.

Тема 5. Системы и средства защиты компьютерной информации в информационных системах.

Технологическая схема обработки информации. Основные каналы утечки информации при обработке на компьютерах. Аппаратные закладки. Виброаккустический канал утечки информации. Визуальный канал утечки информации. Программные и аппаратные средства защиты от несанкционированного доступа. Парольная система доступа. Защита на различных уровнях: операционная система, прикладные программы. Программные закладки. Разграничение доступа. Регистрация. Остаточная информация. Защита от копирования.

Тема 6. Требования к содержанию нормативно-методических документов по защите информации.

Научно-методологический базис, стратегическая направленность и инструментальный базис защиты информации; структура и задачи (типовой перечень) органов, выполняющих защиту информации.

Тема 7. Организационно-правовой статус службы информационной безопасности.

Организационно-технические и режимные меры; политика безопасности: организация секретного делопроизводства и мероприятий по защите информации.

Тема 8. Программно-технические методы и средства защиты информации.

Программно-аппаратные методы и средства ограничения доступа к компонентам компьютера.

Тема 9. Типы несанкционированного доступа и условия работы средств защиты.

Вариант защиты от локального несанкционированного доступа и от удаленного ИСД. Средства защиты, управляемые модемом, надежность средств защиты.

Раздел 2. Информационная безопасность.

Тема 1. Изучение традиционных симметричных криптосистем.

Основные понятия и определения; шифры перестановки; шифр перестановки «скитала»; шифрующие таблицы; применение магических квадратов; шифры простой замены; полибианский квадрат; система шифрования Цезаря; система шифрования Вижинера; шифр «двойной квадрат» Уитстона; одноразовая система шифрования; шифрование методом Вернама; роторные машины; шифрование методом гаммирования; методы генерации псевдослучайных последовательностей чисел.

Тема 2. Применение симметричных криптосистем для защиты компьютерной информации в информационных системах.

Изучение американского стандарта шифрования данных DES; основные режимы работы алгоритма DES; отечественный стандарт шифрования данных; режим простой замены; режим гаммирования; режим гаммирования с обратной связью; режим выработки имитовставки; блочные и поточные шифры.

Тема 3. Применение асимметричных криптосистем для защиты компьютерной информации в информационных системах.

Концепция криптосистемы с открытым ключом; однонаправленные функции; криптосистема шифрования данных RSA (процедуры шифрования и расшифрования в этой системе); безопасность и быстродействие криптосистемы RSA; схема шифрования Полига-Хеллмана; схема шифрования эль-Гамаля, комбинированный метод шифрования.

Тема 4. Методы идентификации и проверки подлинности пользователей компьютерных систем.

Основные понятия и концепции; идентификация и механизмы подтверждения подлинности пользователя; взаимная проверка подлинности пользователей; протоколы

идентификации с нулевой передачей знаний; упрощенная схема идентификации с нулевой передачей знаний.

Тема 5. Защита компьютерных систем от удаленных атак через сеть Internet.

Режим функционирования межсетевых экранов и их основные компоненты; маршрутизаторы; шлюзы сетевого уровня; усиленная аутентификация; основные схемы сетевой защиты на базе межсетевых экранов; применение межсетевых экранов для организации виртуальных корпоративных сетей; программные методы защиты.

Тема 6. Изучение существующих аппаратно-программных средств криптографической защиты компьютерной информации серии КРИПТОН.

Основные элементы средств защиты сети от несанкционированного доступа; устройства криптографической защиты данных; контроллер смарт-карт SCAT-200; программно-аппаратная система защиты от несанкционированного доступа (НСД) КРИПТОН-ВЕТО; защита от НСД со стороны сети; абонентское шифрование и ЭЦП; шифрование пакетов; аутентификация; защита компонентов ЛВС от НСД; защита абонентского пункта, маршрутизаторов и устройств контроля; технология работы с ключами. Методы защиты программ от изучения и разрушающих программных воздействий (программных закладок и вирусов).

Тема 7. Компьютерные вирусы как особый класс разрушающих программных воздействий.

Защита от РПВ; понятие изолированной программной среды.

Тема 8. Комплексная защита процесса обработки информации в компьютерных системах на основе стохастической интеллектуальной информационной технологии.

Возможности СИИТ для обеспечения комплексной защиты программ в момент их выполнения и данных при их обработке в компьютере.

Тема 9. Разработка транслятора исходного текста программ, обеспечивающего их защиту на логическом (алгоритмическом) и физическом уровне от НСД, программных закладок и вирусов.

Метод защиты от НСД и разрушающих программных воздействий процесса хранения, обработки информации; защита арифметических вычислений в компьютерных системах.

Литература:

1. Бурькова, Е.В. Физическая защита объектов информатизации: учебное пособие / Е.В. Бурькова; Министерство образования и науки Российской Федерации, Оренбургский государственный университет, Кафедра вычислительной техники и защиты информации. - Оренбург: Оренбургский государственный университет, 2017. - 158 с.: табл., схем. - Библиогр. в кн. - ISBN 978-5-7410-1697-8; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=481730.

2. Петренко, В.И. Защита персональных данных в информационных системах: учебное пособие / В.И. Петренко; Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет». - Ставрополь: СКФУ, 2016. - 201 с. : схем.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=459205.

3. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации: учебное пособие / Ю.Н. Загинайлов. - Москва; Берлин: Директ-Медиа, 2015. - 253 с.: ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=276557.

4. Нестандартные методы защиты информации: лабораторный практикум / Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет»; авт.-сост. В.П. Пашинцев, А.В. Ляхов. - Ставрополь: СКФУ, 2016. - 196 с.: ил. - Библиогр. в кн.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=458132.

5. Аверченков, В.И. Служба защиты информации: организация и управление: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стереотип. - Москва: Издательство «Флинта», 2016. - 186 с. - Библиогр. в кн. - ISBN 978-5-9765-1271-9; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93356.

6. Сердюк, В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учебное пособие / В.А. Сердюк; Высшая Школа Экономики Национальный Исследовательский Университет. - Москва: Издательский дом Государственного университета Высшей школы экономики, 2015. - 574 с.: ил. - Библиогр. в кн. - ISBN 978-5-7598-0698-1; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=440285.

7. Скрипник, Д.А. Общие вопросы технической защиты информации / Д.А. Скрипник. - 2-е изд., испр. - Москва: Национальный Открытый Университет «ИНТУИТ», 2016. - 425 с.: ил. - Библиогр. в кн.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=429070.

8. Комплексное обеспечение информационной безопасности автоматизированных систем: лабораторный практикум / Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет»; авт.-сост. М.А. Лапина, Д.М. Марков и др. - Ставрополь : СКФУ, 2016. - 242 с. ил. - Библиогр. в кн.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=458012.

9. Загинайлов, Ю.Н. Основы информационной безопасности: курс визуальных лекций: учебное пособие / Ю.Н. Загинайлов. - Москва; Берлин: Директ-Медиа, 2015. - 105 с.: ил. - Библиогр. в кн. - ISBN 978-5-4475-3947-4; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=362895.

10.Технологии защиты информации в компьютерных сетях / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суровов. - 2-е изд., испр. - Москва: Национальный Открытый Университет «ИНТУИТ», 2016. - 369 с. : ил.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=428820.

Интернет-ресурсы

1) Сайт журнала «Хакер» [Электронный ресурс] URL: http://xakep.ru/

2) Защита информации, управление информационной безопасностью и рисками – ISO27000.ru - [Электронный ресурс] URL: http://www.iso27000.ru/

3) Официальный сайт компании «КонсультантПлюс» [Электронный ресурс] URL: http://www.consultant.ru/

4) ФСТЭК России. Федеральная служба по техническому и экспортному контролю. Официальный сайт [Электронный ресурс] URL: http://fstec.ru/

5) ФСБ Российской Федерации. Официальный сайт [Электронный ресурс] URL: http://www.fsb.ru/

6) Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций [Электронный ресурс] URL: http://rkn.gov.ru/

2.3. Тематический план практических (семинарских) занятий:

№ п/п раздела	Наименование разделов и тем	Количество часов
1	2	3
1	**Раздел I. Методы и системы защиты информации**	
2	Тема 1. Законодательные и правовые основы защиты компьютерной информации информационных технологий.	4
3	Тема 2. Вычислительные сети и защита информации.	6
4	Тема 3. Проблемы защиты информации в информационных системах.	6
5	Тема 4. Защита локальных сетей и операционных систем.	8
6	Тема 5. Системы и средства защиты компьютерной информации в информационных системах.	6

7	Тема 6. Требования к содержанию нормативно-методических документов по защите информации.	2
8	Тема 7. Организационно-правовой статус службы информационной безопасности.	2
9	Тема 8. Программно-технические методы и средства защиты информации.	4
10	Тема 9. Типы несанкционированного доступа и условия работы средств защиты.	4
11	**Раздел II. Информационная безопасность**	
12	Тема 1. Изучение традиционных симметричных криптосистем.	6
13	Тема 2. Применение симметричных криптосистем для защиты компьютерной информации в информационных системах.	6
14	Тема 3. Применение асимметричных криптосистем для защиты компьютерной информации в информационных системах.	6
15	Тема 4. Методы идентификации и проверки подлинности пользователей компьютерных систем.	8
16	Тема 5. Защита компьютерных систем от удаленных атак через сеть Internet.	6
17	Тема 6. Изучение существующих аппаратно-программных средств криптографической защиты компьютерной информации серии КРИПТОН.	8
18	Тема 7. Компьютерные вирусы как особый класс разрушающих программных воздействий.	2
19	Тема 8. Комплексная защита процесса обработки информации в компьютерных системах на основе стохастической интеллектуальной информационной технологии.	4
20	Тема 9. Разработка транслятора исходного текста программ, обеспечивающего их защиту на логическом (алгоритмическом) и физическом уровне от НСД, программных закладок и вирусов.	2
	Итого по дисциплине	**90**

Содержание практических занятий

Раздел I. Методы и системы защиты информации.

Тема 1. Законодательные и правовые основы защиты компьютерной информации информационных технологий.

Правовое регулирование открытых информационных ресурсов. Правовая защита информационных ресурсов ограниченного доступа: а) защита информации институтом государственной тайны; б) коммерческая тайна как форма защиты информации; в) производственная, служебная и профессиональная тайна; г) личная и семейная тайна.

Тема 2. Вычислительные сети и защита информации.

Средства повышения надежности функционирования сетей. Регламентирующие документы в области безопасности вычислительных сетей. Типовые угрозы сетевой безопасности. Защита топологии сети. Методы защиты сетевого трафика и компонентов.сети.

Тема 3. Проблемы защиты информации в информационных системах.

Раскрытие конфиденциальной информации. Несанкционированный доступ к информации. Компрометация информации. Несанкционированное использование информационных ресурсов. Отказ от информации. Нарушение информационного обслуживания. Незаконное использование привилегий. «Взлом системы».

Тема 4. Защита локальных сетей и операционных систем.

Анализ потенциальных угроз оперативно-технологической информации в локальной сети. Основные цели сетевой безопасности. Модели безопасности. Виды угроз и методы защиты.

Тема 5. Системы и средства защиты компьютерной информации в информационных системах.

Защищенная информационная система и система защиты информации; принципы построения систем защиты информации и их основы; законодательная, нормативно-методическая и научная база системы защиты информации.

Тема 6. Требования к содержанию нормативно-методических документов по защите информации.

Правовые основы обеспечения информационной безопасности личности, общества и государства. Государственная политика в области обеспечения национальной безопасности. Роль и место информационной безопасности в системе национальной безопасности. Конституционные основы обеспечения безопасности. Законы РФ о безопасности личности и государства, о праве граждан на информацию. Виды нормативно-правовых актов. Иерархия нормативно-правовых актов в области защиты информации.

Тема 7. Организационно-правовой статус службы информационной безопасности.

Виды служб безопасности. Задачи и основные функции службы безопасности. Структура службы безопасности и функции основных подразделений. Плановая и контрольная работа в службе безопасности.

Тема 8. Программно-технические методы и средства защиты информации.

Классификация угроз информационной безопасности компьютерных систем. Зашита от вирусов: а) основные виды компьютерных вирусов; б) профилактика вирусного заражения; в) антивирусные программы. Защита от несанкционированного доступа с помощью стандартных и специализированных программно-технических средств.

Тема 9. Типы несанкционированного доступа и условия работы средств защиты.

Средства защита информации от несанкционированного доступа. Процедуры получения доступа к ресурсам информационной системы: идентификация, аутентификация и авторизация.

Раздел 2. Информационная безопасность.

Тема 1. Изучение традиционных симметричных криптосистем.

Принципы криптографической защиты информации: основные понятия и определения; обобщённая структура криптосистемы; классификация криптоаналитических атак. Шифры простой замены: шифрующие таблицы Трисемуса; биграммный шифр Плейфера; криптосистема Хилла. Шифры сложной замены: одноразовая система шифрования.

Тема 2. Применение симметричных криптосистем для защиты компьютерной информации в информационных системах.

Режимы работы DES: «Электронная кодовая книга», «Сцепление блоков шифра», «Обратная связь по шифру»; «Обратная связь по выходу». Области применения алгоритма DES. Комбинирование блочных алгоритмов.

Тема 3. Применение асимметричных криптосистем для защиты компьютерной информации в информационных системах.

Концепция криптосистемы с открытым ключом; однонаправленные функции; криптосистема шифрования данных RSA (процедуры шифрования и расшифрования в этой системе); безопасность и быстродействие криптосистемы RSA; схема шифрования Полига-Хеллмана; схема шифрования эль-Гамаля, комбинированный метод шифрования.

Тема 4. Методы идентификации и проверки подлинности пользователей компьютерных систем.

Проблема аутентификации данных и электронная цифровая подпись; однонаправленные хэш-функции; алгоритм безопасного деширования SHA; однонаправленные хэш-функции на основе симметричных блочных алгоритмов; отечественный стандарт хэш-функции; алгоритм

цифровой подписи RSA; алгоритм цифровой подписи эль-Гамаля (EGSA); алгоритм цифровой подписи DSA; отечественный стандарт цифровой подписи.

Тема 5. Защита компьютерных систем от удаленных атак через сеть Internet.

Особенности безопасности компьютерных сетей. Анализ сетевого трафика сети Internet. Защита от ложного ARP-сервера в сети Internet. Навязывание хосту ложного маршрута с использованием протокола ICMP с целью создания в сети Internet ложного маршрутизатора.

Тема 6. Изучение существующих аппаратно-программных средств криптографической защиты компьютерной информации серии КРИПТОН.

Классификация способов защиты; защита от отладок и дизассемблирования; способы встраивания защитных механизмов в программное обеспечение; понятие разрушающего программного воздействия; модели взаимодействия прикладной программы и программной закладки; методы перехвата и навязывания информации; методы внедрения программных закладок.

Тема 7. Компьютерные вирусы как особый класс разрушающих программных воздействий.

Вирусы. Программные «черви» - РПВ. «Троянские кони». Логические люки. Программные закладки.

Тема 8. Комплексная защита процесса обработки информации в компьютерных системах на основе стохастической интеллектуальной информационной технологии.

Метод верификации программного обеспечения для контроля корректности, реализуемости и защиты от закладок.

Тема 9. Разработка транслятора исходного текста программ, обеспечивающего их защиту на логическом (алгоритмическом) и физическом уровне от НСД, программных закладок и вирусов.

Метод защиты от НСД и разрушающих программных воздействий процесса хранения, обработки информации; защита арифметических вычислений в компьютерных системах.

Литература

1. Бурькова, Е.В. Физическая защита объектов информатизации : учебное пособие / Е.В. Бурькова; Министерство образования и науки Российской Федерации, Оренбургский государственный университет, Кафедра вычислительной техники и защиты информации. - Оренбург: Оренбургский государственный университет, 2017. - 158 с.: табл., схем. - Библиогр. в кн. - ISBN 978-5-7410-1697-8; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=481730.

2. Петренко, В.И. Защита персональных данных в информационных системах: учебное пособие / В.И. Петренко; Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет». - Ставрополь: СКФУ, 2016. - 201 с. : схем.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=459205.

3. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации: учебное пособие / Ю.Н. Загинайлов. - Москва; Берлин: Директ-Медиа, 2015. - 253 с.: ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=276557.

4. Нестандартные методы защиты информации: лабораторный практикум / Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет»; авт.-сост. В.П. Пашинцев, А.В. Ляхов. - Ставрополь : СКФУ, 2016. - 196 с.: ил. - Библиогр. в кн.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=458132.

5. Аверченков, В.И. Служба защиты информации: организация и управление: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стереотип. - Москва: Издательство «Флинта», 2016. - 186 с. - Библиогр. в кн. - ISBN 978-5-9765-1271-9; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93356.

6. Сердюк, В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учебное пособие / В.А. Сердюк; Высшая Школа Экономики Национальный Исследовательский Университет. - Москва: Издательский дом Государственного университета Высшей школы экономики, 2015. - 574 с.: ил. - Библиогр. в кн. - ISBN 978-5-7598-0698-1; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=440285.

7. Скрипник, Д.А. Общие вопросы технической защиты информации / Д.А. Скрипник. - 2-е изд., испр. - Москва: Национальный Открытый Университет «ИНТУИТ», 2016. - 425 с.: ил. - Библиогр. в кн.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=429070.

8. Комплексное обеспечение информационной безопасности автоматизированных систем: лабораторный практикум / Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет»; авт.-сост. М.А. Лапина, Д.М. Марков и др. - Ставрополь: СКФУ, 2016. - 242 с. ил. - Библиогр. в кн.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=458012.

9. Загинайлов, Ю.Н. Основы информационной безопасности: курс визуальных лекций: учебное пособие / Ю.Н. Загинайлов. - Москва; Берлин: Директ-Медиа, 2015. - 105 с.: ил. - Библиогр. в кн. - ISBN 978-5-4475-3947-4; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=362895

10.Технологии защиты информации в компьютерных сетях / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суровов. - 2-е изд., испр. - Москва: Национальный Открытый Университет «ИНТУИТ», 2016. - 369 с. : ил.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=428820

Интернет-ресурсы

1) Сайт журнала «Хакер» [Электронный ресурс] URL: http://xakep.ru/

2) Защита информации, управление информационной безопасностью и рисками – ISO27000.ru - [Электронный ресурс] URL: http://www.iso27000.ru/

3) Официальный сайт компании «КонсультантПлюс» [Электронный ресурс] URL: http://www.consultant.ru/

4) ФСТЭК России. Федеральная служба по техническому и экспортному контролю. Официальный сайт [Электронный ресурс] URL: http://fstec.ru/

5) ФСБ Российской Федерации. Официальный сайт [Электронный ресурс] URL: http://www.fsb.ru/

6) Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций [Электронный ресурс] URL: http://rkn.gov.ru/

2.3. Тематический план для самостоятельной работы

№ п/п раздела	Наименование разделов и тем	Количество часов
1	2	3
1	**Раздел I. Методы и системы защиты информации**	
2	Тема 1. Законодательные и правовые основы защиты компьютерной информации информационных технологий.	8
3	Тема 2. Вычислительные сети и защита информации.	12
4	Тема 3. Проблемы защиты информации в информационных системах.	8
5	Тема 4. Защита локальных сетей и операционных систем.	12
6	Тема 5. Системы и средства защиты компьютерной информации в информационных системах.	12
7	Тема 6. Требования к содержанию нормативно-методических документов по защите информации.	6
8	Тема 7. Организационно-правовой статус службы информационной безопасности.	6

9	Тема 8. Программно-технические методы и средства защиты информации.	8
10	Тема 9. Типы несанкционированного доступа и условия работы средств защиты.	6
11	**Раздел II. Информационная безопасность**	
12	Тема 1. Изучение традиционных симметричных криптосистем.	10
13	Тема 2. Применение симметричных криптосистем для защиты компьютерной информации в информационных системах.	10
14	Тема 3. Применение асимметричных криптосистем для защиты компьютерной информации в информационных системах.	10
15	Тема 4. Методы идентификации и проверки подлинности пользователей компьютерных систем.	10
16	Тема 5. Защита компьютерных систем от удаленных атак через сеть Internet.	12
17	Тема 6. Изучение существующих аппаратно-программных средств криптографической защиты компьютерной информации серии КРИПТОН.	12
18	Тема 7. Компьютерные вирусы как особый класс разрушающих программных воздействий.	6
19	Тема 8. Комплексная защита процесса обработки информации в компьютерных системах на основе стохастической интеллектуальной информационной технологии.	10
20	Тема 9. Разработка транслятора исходного текста программ, обеспечивающего их защиту на логическом (алгоритмическом) и физическом уровне от НСД, программных закладок и вирусов.	4
	Итого по дисциплине	**162**

Вопросы для самоконтроля

1. К видам профессиональной тайны относятся?
2. Что из приведенного ниже относится к физической защите информации?
3. К нормативно-техническому уровню государственной системы информационной безопасности относятся?
4. К организационно-правовым методам защиты информации относится?
5. К какому уровню представления нормативно-правовой базы государственной системы информационной безопасности относится Указ Президента Российской Федерации "Об утверждении Перечня сведений конфиденциального характера"?
6. Какие функции в области информационной безопасности осуществляет ФСБ России?
7. Что понимают под информационной безопасностью в узком смысле этого слова?
8. Что понимают под информационной безопасностью в широком смысле этого слова?
9. Завершите фразу правильно: "Уязвимость – это..."
10. Завершите фразу правильно: "Целостность – это..."
11. Завершите фразу правильно: "Триада безопасности – это..."
12. Завершите фразу правильно: "Политика информационной безопасности – это..."
13. Завершите фразу правильно "Конфиденциальность – это..."
14. К фукнциям ФСТЭК России в области информационной безопасности относится?
15. Выберите правильный вариант завершения фразы: "Информационная безопасность определяется способностью государства, общества, личности..."
16. Режим защиты в отношении сведений, отнесенных к государственной тайне, устанавливается?
17. Завершите фразу правильно: "Защита информации включает в себя..."
18. Система защиты персональных данных включает в себя?
19. Сколько лет составляет максимальный срок засекречивания сведений, составляющих государственную тайну?
20. Выберите правильные варианты завершения фразы: "Информационные ресурсы принято разделять с точки зрения информационной безопасности на ..."

21. Выберите правильное завершение фразы: "В соответствии с общей классификацией защищаемые объекты информатизации подразделяются на..."

22. Выберите правильное завершение фразы: "В соответствии с общей классификацией защищаемые объекты информатизации подразделяются на..."

23. Выберите правильное завершение фразы: "В соответствии с общей классификацией защищаемые объекты информатизации подразделяются на..."

24. Принцип действия каких приборов основан на интегральном методе измерения уровня электромагнитного поля в точке их размещения и на этой основе – в определении точки абсолютного уровня излучения в помещении?

25. Какие показатели необходимо учитывать, при включении угроз безопасности в модель угроз безопасности информации, необходимую для выбора мер по защите информации не содержащей государственную тайну в государственных информационных системах?

26. Какие показатели необходимо учитывать, при включении угроз безопасности в модель угроз безопасности информации, необходимую для выбора мер по защите информации не содержащей государственную тайну в государственных информационных системах?

27. Какие показатели необходимо учитывать, при включении угроз безопасности в модель угроз безопасности информации, необходимую для выбора мер по защите информации не содержащей государственную тайну в государственных информационных системах?

28. К какому уровню представления нормативно -правовой базы государственной системы информационной безопасности относится Закон Российской Федерации "О персональных данных"?

29. Выберите, что из перечисленного относится к основным техническим средствам и системам (ОТСС).

30. К какому уровню представления нормативно -правовой базы государственной системы информационной безопасности относится Постановление Правительства Российской Федерации "О сертификации средств защиты информации"?

31. К какому уровню представления нормативно -правовой базы государственной системы информационной безопасности относятся "Технические требования к универсальной электронной карте"

32. К какому уровню представления нормативно -правовой базы государственной системы информационной безопасности относится Указ Президента Российской Федерации "Об утверждении Концепции национальной безопасности Российской Федерации"?

33. Для решения задач обеспечения безопасности на первом этапе необходимо?

34. Завершите фразу правильно: "Доступность – это..."

35. Что из перечисленного является важнейшим элементом дискреционной модели разграничения доступа?

36. Сколько классов защищенности СВТ от НСД к информации установлено нормативными документами?

37. В информационной системе реализуется мандатная модель контроля доступа. Определены три уровня меток секретности. Наивысший уровень 1 - й. Какие действия будут разрешены субъекту с 1-й степенью допуска?

38. В информационной системе реализуется мандатная модель контроля доступа. Определены три уровня меток секретности. Наивысший уровень 1 - й. Какие действия будут разрешены субъекту с 3-й степенью допуска?

39. Что понимают в модели безопасности Белла -Ла Падулы под правилом запрета записи на нижний уровень?

40. Для выполнения каких действий необходима модель информационной безопасности?

41. Может ли элемент множества объектов дискреционной модели Харрисона -Рузо - Ульмана изменять множество прав доступа?

42. Какие из перечисленных характеристик используются для оценки риска информационной безопасности?

43. Какое множество должно быть определено для мандатной модели контроля доступа?

44. Какое множество должно быть определено для мандатной модели контроля доступа?

45. В информационной системе реализуется мандатная модель контроля доступа. Определены три уровня меток секретности. Наивысший уровень 1 - й. Какие действия будут разрешены субъекту со 2-й степенью допуска?

46. Какие множества должны быть определены для мандатной модели контроля доступа?

47. Выберите правильные варианты завершения фразы: "Информационные ресурсы принято разделять с точки зрения информационной безопасности на ..."

48. Завершите фразу правильно: "Техническая защита информации – это..."

49. Сколько видов усиленной ЭП определено законодательством РФ?

50. К какому уровню представления нормативно -правовой базы государственной системы информационной безопасности относится Постановление Правительства Российской Федерации "Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации о государственной тайне"?

51. Какие элементы необходимы для описания угрозы информационной безопасности?

52. Выберите что из перечисленного относится к источникам угроз информационной безопасности?

Литература

1. Бурькова, Е.В. Физическая защита объектов информатизации : учебное пособие / Е.В. Бурькова; Министерство образования и науки Российской Федерации, Оренбургский государственный университет, Кафедра вычислительной техники и защиты информации. - Оренбург: Оренбургский государственный университет, 2017. - 158 с.: табл., схем. - Библиогр. в кн. - ISBN 978-5-7410-1697-8; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=481730

2. Петренко, В.И. Защита персональных данных в информационных системах: учебное пособие / В.И. Петренко; Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет». - Ставрополь: СКФУ, 2016. - 201 с. : схем.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=459205

3. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации: учебное пособие / Ю.Н. Загинайлов. - Москва; Берлин: Директ-Медиа, 2015. - 253 с.: ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=276557

4. Нестандартные методы защиты информации: лабораторный практикум / Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет»; авт.-сост. В.П. Пашинцев, А.В. Ляхов. - Ставрополь : СКФУ, 2016. - 196 с.: ил. - Библиогр. в кн.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=458132

5. Аверченков, В.И. Служба защиты информации: организация и управление: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стереотип. - Москва: Издательство «Флинта», 2016. - 186 с. - Библиогр. в кн. - ISBN 978-5-9765-1271-9; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93356

6. Сердюк, В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий : учебное пособие / В.А. Сердюк ; Высшая Школа Экономики Национальный Исследовательский Университет. - Москва: Издательский дом Государственного университета Высшей школы экономики, 2015. - 574 с.: ил. - Библиогр. в кн. - ISBN 978-5-7598-0698-1; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=440285

7. Скрипник, Д.А. Общие вопросы технической защиты информации / Д.А. Скрипник. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 425 с.: ил. - Библиогр. в кн.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=429070

8. Комплексное обеспечение информационной безопасности автоматизированных систем: лабораторный практикум / Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет»; авт.-сост. М.А. Лапина, Д.М. Марков и др. - Ставрополь: СКФУ, 2016. - 242 с. ил. - Библиогр. в кн.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=458012

9. Загинайлов, Ю.Н. Основы информационной безопасности: курс визуальных лекций: учебное пособие / Ю.Н. Загинайлов. - Москва; Берлин: Директ-Медиа, 2015. - 105 с.: ил. -

Библиогр. в кн. - ISBN 978-5-4475-3947-4; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=362895

10.Технологии защиты информации в компьютерных сетях / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суровов. - 2-е изд., испр. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 369 с. : ил.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=428820

Интернет-ресурсы

1) Сайт журнала «Хакер» [Электронный ресурс] URL: http://xakep.ru/

2) Защита информации, управление информационной безопасностью и рисками – ISO27000.ru - [Электронный ресурс] URL: http://www.iso27000.ru/

3) Официальный сайт компании «КонсультантПлюс» [Электронный ресурс] URL: http://www.consultant.ru/

4) ФСТЭК России. Федеральная служба по техническому и экспортному контролю. Официальный сайт [Электронный ресурс] URL: http://fstec.ru/

5) ФСБ Российской Федерации. Официальный сайт [Электронный ресурс] URL: http://www.fsb.ru/

6) Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций [Электронный ресурс] URL: http://rkn.gov.ru/

Перечень тем рефератов

1. Основные симметричные шифры дошенноновского периода.
2. Криптоанализ шифров замены.
3. Криптоанализ шифров перестановки.
4. Криптоанализ шифров гаммирования и шифра Виженера.
5. Шифры DES, ГОСТ 28147-89, AES.
6. Машинные шифры.
7. Имитостойкость и надежность шифров.
8. Принципы построения и анализа алгоритмов защиты информации.
9. Криптографические хэш-функции.
10. Теоретико-автоматные модели шифров.
11. Методы шифрования с открытым ключом..
12. Безопасность и быстродействие криптосистемы RSA.
13. Методы и концепции проверки подлинности пользователей компьютерных систем.
14. Хэш-функции на основе симметричных блочных алгоритмов.
15. Алгоритм SHA и отечественный стандарт хэш-функции.
16. Цифровая подпись Эль-Гамаля (EGSA). Стандарты цифровой подписи.
17. Программно-аппаратные методы и средства ограничения доступа к компонентам компьютера.
18. Защита информации от несанкционированного копирования. Администрирование компьютерных сетей.
19. Существующие аппаратно-программные средства криптографической защиты информации серии КРИПТОН.
20. Методы генерации псевдослучайных последовательностей.
21. Избыточность языка и расстояние единственности.
22. Правовые вопросы защиты информации.
23. Стеганографическая защита информации.
24. Законодательные и правовые основы защиты компьютерной информации информационных технологий.
25. Проблемы защиты информации в информационных системах.
26. Содержание системы средств защиты компьютерной информации в информационных системах.
27. Организационно-правовой статус службы информационной безопасности.

Средство оценивания: реферат

Шкала оценивания:

Реферат оценивается по 100-балльной шкале.
Баллы переводятся в оценки успеваемости следующим образом:
86-100 баллов – «отлично»;
70- 85 баллов – «хорошо»;
51-69 баллов – «удовлетворительно;
менее 51 балла – «неудовлетворительно».

Критерии	Показатели
1. Новизна реферированного текста. Максимальная оценка – 20 баллов	– актуальность проблемы и темы; – новизна и самостоятельность в постановке проблемы, в формулировании нового аспекта выбранной для анализа проблемы; – наличие авторской позиции, самостоятельность суждений.
2. Степень раскрытия сущности проблемы. Максимальная оценка – 30 баллов	– соответствие плана теме реферата; – соответствие содержания теме и плану реферата; – полнота и глубина раскрытия основных понятий проблемы; – обоснованность способов и методов работы с материалом; – умение работать с историческими источниками и литературой, систематизировать и структурировать материал; – умение обобщать, сопоставлять различные точки зрения по рассматриваемому вопросу, аргументировать основные положения и выводы.
3. Обоснованность выбора источников и литературы. Максимальная оценка – 20 баллов.	–круг, полнота использования исторических источников и литературы по проблеме; – привлечение новейших работ по проблеме (журнальные публикации, материалы сборников научных трудов, интернет- ресурсов и т. д.).
4. Соблюдение требований к оформлению. Максимальная оценка – 15 баллов.	– правильное оформление ссылок на использованные источники и литературу; – грамотность и культура изложения; – использование рекомендованного количества исторических источников и литературы; – владение терминологией и понятийным аппаратом проблемы; – соблюдение требований к объему реферата; – культура оформления: выделение абзацев, глав и параграфов
5. Грамотность. Максимальная оценка – 15 баллов.	– отсутствие орфографических и синтаксических ошибок, стилистических погрешностей; – отсутствие опечаток, сокращений слов, кроме общепринятых; – литературный стиль.

3. Оценочные средств и методические рекомендации по проведению промежуточной аттестации

При проведении экзамена по дисциплине «Методы и системы защиты информации, информационная безопасность» может использоваться устная или письменная форма проведения.

Примерная структура экзамена по дисциплине «Методы и системы защиты информации, информационная безопасность»:

1. устный ответ на вопросы. Аспиранту на экзамене дается время на подготовку вопросов теоретического характера. Задания выполняются в течение 30 минут.

Устный ответ аспиранта на экзамене должен отвечать следующим требованиям:

• научность, знание и умение пользоваться понятийным аппаратом;

• изложение вопросов в методологическом аспектах, аргументация основных положений ответа примерами из современной практики, а также из личного опыта работы;

• осведомленность в важнейших современных проблемах в области информационной безопасности, знание классической и современной литературы, исследований ученых.

Критерии оценивания ответов

Оценка	Устный ответ
Отлично	знание учебного материала в пределах программы; логическое, последовательное изложение вопроса с опорой на разнообразные источники, с использованием знаний других наук; определение своей позиции в раскрытии различных подходов к рассматриваемой проблеме; показ значения разработки данного теоретического вопроса для педагогической практики
Хорошо	знание учебного материала в пределах программы; раскрытие различных подходов к рассматриваемой проблеме; опора при рассмотрении вопроса на обязательную литературу, включение соответствующих примеров из практики
Удовлетворительно	знание учебного материала в пределах программы на основе изучения какого–либо одного подхода к рассматриваемой проблеме
Неудовлетворительно	пробелы в знаниях основного учебно–программного материала, принципиальные ошибки в выполнении предусмотренных программой заданий

Критерии и шкала оценивания уровней освоения компетенций

Шкала оценивания	Шкала оценивания	Шкала оценивания
отлично	высокий	аспирант, овладел элементами компетенции «знать», «уметь» и «владеть», проявил всесторонние и глубокие знания программного материала по дисциплине, освоил основную и дополнительную литературу, обнаружил творческие способности в понимании, изложении и практическом использовании усвоенных знаний.
хорошо	продвинутый	аспирант овладел элементами компетенции «знать» и «уметь», проявил полное знание программного материала по дисциплине, освоил основную рекомендованную литературу, обнаружил стабильный характер знаний и умений и проявил способности к их самостоятельному применению и обновлению в ходе последующего обучения и практической деятельности.
удовлетворительно	базовый	аспирант овладел элементами компетенции «знать», проявил знания основного программного материала по дисциплине в объеме, необходимом для последующего обучения и предстоящей практической деятельности, изучил основную рекомендованную литературу, допустил неточности в ответе на экзамене, но в основном обладает необходимыми знаниями для их устранения при корректировке со стороны экзаменатора.
неудовлетворительно	компетенции не сформированы	аспирант не овладел ни одним из элементов компетенции, обнаружил существенные пробелы в знании основного программного материала по дисциплине, допустил принципиальные ошибки при применении теоретических знаний, которые не позволяют ему продолжить обучение или приступить к практической деятельности без дополнительной подготовки по данной дисциплине.

Рекомендации по проведению экзамена

1. Аспиранты должны быть заранее ознакомлены с требованиями к экзамену, критериями оценивания. В результате экзамена аспирант должен обязательно четко понять, почему он получил именно ту экзаменационную отметку, которая была ему поставлена за его ответ, а не другую.

2. Необходимо выяснить на экзамене, владеет аспирант формально или нет знаниями по данному предмету. Вопросы при ответе по билету помогут выяснить степень понимания аспирантом материала, знание им связей излагаемого вопроса с другими изучающимися им понятиями.

3. На экзамене следует выяснить, как аспирант знает программный материал, как он им овладел к моменту экзамена, как он продумал его в процессе обучения и подготовки к экзамену.

4. При устном опросе целесообразно начинать с легких, простых вопросов, ответы на которые помогут подготовить аспиранта к спокойному размышлению над дальнейшими более трудными вопросами.

Перечень вопросов к экзамену

1. Безопасность информационных ресурсов и документирование информации.
2. Государственные информационные ресурсы, ПДн.
3. Право на доступ к информации.
4. Разработка и производство информационных систем.
5. Вычислительные сети и защита информации.
6. Нормативно-правовая база функционирования систем защиты информации.
7. Промышленный шпионаж и законодательство, копирастинг ПО.
8. Меры по обеспечению сохранности информации и угрозы ее безопасности в ИС.
9. Основные задачи обеспечения безопасности информации в ИС.
10. Защита локальных сетей и операционных систем.
11. Интеграция систем защиты.
12. Рекомендации по защите информации в сети Интернет.
13. Принципы построения систем защиты и их основы.
14. Законодательная, нормативно-методическая и научная база систем защиты информации.
15. Требования к нормативным документам по ЗИ, научно-методологический базис, стратегическая направленность и инструментальный базис.
16. Структура и задачи органов выполняющих защиту информации.
17. Организационно-правовой статус службы информационной безопасности.
18. Организационно-технические и режимные меры.
19. Политика безопасности: организация секретного делопроизводства и мероприятий по ЗИ.
20. Программно-аппаратные методы и средства ограничения доступа компонентам компьютера.
21. Типы НСД и защита от них.
22. Надежность средств защиты.
23. Основные понятия и определения традиционных симметричных криптосистем.
24. Шифры перестановки.
25. Шифр перестановки "Скитала".
26. Шифрующие таблицы.
27. Магический квадрат.
28. Шифры простой замены
29. Полибианский квадрат.
30. Система шифрования Цезаря.
31. Система шифрования Вижинера.
32. Шифр двойной квадрат.
33. Одноразовая система шифрования.
34. Шифрование методом Вернама.
35. Роторные машины.
36. Шифрование методом гаммирования.
37. Методы генерации случайных последовательностей.
38. Изучение американского стандарта шифрования DES.
39. Режимы работы DES.
40. Отечественный стандарт шифрования данных.
41. Режим простой замены.
42. Режим гаммирования.

43. Гаммирование с обратной связью.
44. Режим выработки имитовставки.
45. Блочные и поточные шифры.
46. Концепция системы с открытым ключом.
47. Односторонние функции.
48. Криптосистема шифрования данных RSA.
49. Схема шифрования Полига-Хеллмана.
50. Схема шифрования Эль-Гамаля.
51. Комбинированный способ шифрования.
52. Основные понятия и концепции идентификации и проверки подлинностей пользователя.
53. Идентификация и механизмы подтверждения подлинности пользователя.
54. Взаимная проверка подлинности пользователей.
55. Протоколы идентификации с нулевой передачей знаний.
56. Проблема аутентификации данных и ЭЦП.
57. Однонаправленные хэш-функции.
58. Алгоритм безопасного дехеширования SHA.
59. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов.
60. Отечественный стандарт хэш-функции.
61. Алгоритм цифровой подписи RSA.
62. Алгоритм цифровой подписи Эль Гамаля.
63. Алгоритм DSA.
64. Отечественный стандарт цифровой подписи.
65. Режим функционирования межсетевых экранов и их основные компоненты.
66. Маршрутизаторы.
67. Шлюз сетевого уровня.
68. Усиленная аутентификация.
69. Основные схемы сетевой защиты на базе МЭ.
70. Применение межсетевых экранов для организации виртуальных корпоративных сетей.
71. Программные методы защиты.
72. Классификация способов защиты.
73. Защита от отладок и дизассемблирования.
74. Способы встраивания защитных механизмов в ПО.
75. Понятие разрушающего программного воздействия.
76. Модели взаимодействия прик. программы и прог. Закладки.
77. Методы перехвата и навязывания информации.
78. Методы внедрения программных закладок.
79. Возможности СИИТ.
80. Метод защиты от НСД и корректности ПО.
81. Защита арифметических-вычислений в КС.
82. Транслятор.
83. Основные элементы защиты сети от НСД.
84. Устройства криптограф. защиты данных.
85. Контроллер доступа ВЕТО.
86. Контроллер Скат-200.

4.Учебно-методическое и информационное обеспечение

Литература

1. Бурькова, Е.В. Физическая защита объектов информатизации: учебное пособие / Е.В. Бурькова; Министерство образования и науки Российской Федерации, Оренбургский государственный университет, Кафедра вычислительной техники и защиты информации. - Оренбург: Оренбургский государственный университет, 2017. - 158 с.: табл., схем. - Библиогр. в кн. - ISBN 978-5-7410-1697-8; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=481730.

2. Петренко, В.И. Защита персональных данных в информационных системах: учебное пособие / В.И. Петренко; Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет». - Ставрополь: СКФУ, 2016. - 201 с. : схем.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=459205.

3. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации: учебное пособие / Ю.Н. Загинайлов. - Москва; Берлин: Директ-Медиа, 2015. - 253 с.: ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=276557.

4. Нестандартные методы защиты информации: лабораторный практикум / Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет»; авт.-сост. В.П. Пашинцев, А.В. Ляхов. - Ставрополь: СКФУ, 2016. - 196 с.: ил. - Библиогр. в кн.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=458132.

5. Аверченков, В.И. Служба защиты информации: организация и управление: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стереотип. - Москва: Издательство «Флинта», 2016. - 186 с. - Библиогр. в кн. - ISBN 978-5-9765-1271-9; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93356.

6. Сердюк, В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учебное пособие / В.А. Сердюк; Высшая Школа Экономики Национальный Исследовательский Университет. - Москва: Издательский дом Государственного университета Высшей школы экономики, 2015. - 574 с.: ил. - Библиогр. в кн. - ISBN 978-5-7598-0698-1; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=440285.

7. Скрипник, Д.А. Общие вопросы технической защиты информации / Д.А. Скрипник. - 2-е изд., испр. - Москва: Национальный Открытый Университет «ИНТУИТ», 2016. - 425 с.: ил. - Библиогр. в кн.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=429070.

8. Комплексное обеспечение информационной безопасности автоматизированных систем: лабораторный практикум / Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет»; авт.-сост. М.А. Лапина, Д.М. Марков и др. - Ставрополь: СКФУ, 2016. - 242 с. ил. - Библиогр. в кн.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=458012.

9. Загинайлов, Ю.Н. Основы информационной безопасности: курс визуальных лекций: учебное пособие / Ю.Н. Загинайлов. - Москва; Берлин: Директ-Медиа, 2015. - 105 с.: ил. - Библиогр. в кн. - ISBN 978-5-4475-3947-4; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=362895.

10.Технологии защиты информации в компьютерных сетях / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суровов. - 2-е изд., испр. - Москва: Национальный Открытый Университет «ИНТУИТ», 2016. - 369 с.: ил.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=428820.

Интернет-ресурсы

1) Сайт журнала «Хакер» [Электронный ресурс] URL: http://xakep.ru/

2) Защита информации, управление информационной безопасностью и рисками – ISO27000.ru - [Электронный ресурс] URL: http://www.iso27000.ru/

3) ФСТЭК России. Федеральная служба по техническому и экспортному контролю. Официальный сайт [Электронный ресурс] URL: http://fstec.ru/

4) ФСБ Российской Федерации. Официальный сайт [Электронный ресурс] URL: http://www.fsb.ru/

5) Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций [Электронный ресурс] URL: http://rkn.gov.ru/

Перечень программного обеспечения и информационных справочных систем

1. ЭБС «Университетская библиотека онлайн»

2. Научная электронная библиотека eLIBRARY.RU

3. Информационно-образовательный портал АНО ВО «Межрегиональный открытый социальный институт»

4. Лицензионное программное обеспечение:

– «Консультант Плюс» и «Гарант» (доступ к электронным правовым системам осуществляется на основе договора о сотрудничестве от 23.09.2013 г. с ЗАО «Компьютерные технологии» (ПС Гарант), регистрационный лист зарегистрированного пользователя ЭПС «Система ГАРАНТ» от 16.02.2012 г. №12-40272-000944; договора с ООО «КонсультантПлюс Марий Эл» №2017-СВ-4 от 28.12.2016 г.).

5. Материально-техническое обеспечение дисциплины

Материально-техническую базу для проведения лекционных и практических занятий по дисциплине составляют:

Наименование специальных* помещений и помещений для самостоятельной работы	**Оснащенность специальных помещений и помещений для самостоятельной работы**
Аудитория для проведения лекционных и практических занятий, индивидуальных и групповых консультаций, промежуточной аттестации (в соответствии с расписанием)	ноутбук, мультимедийный проектор, экран
Помещение для самостоятельной работы, каб. 408, 409	9 рабочих мест ПЭВМ; Операционная система Ubuntu; Программное обеспечение: Open Office; доступ к сети Internet.
Библиотека	15 рабочих мест ПЭВМ, (15 компьютеров Asus P7H57D-VEVO Intel Core i3 540@3066 МГц), с доступом к базам данных и сети Интернет, копировальная техника.
Лаборатория программно-аппаратных средств обеспечения информационной безопасности, каб. 310.	ST-CE010MF Считыватель настольный для ввода идентификаторов Mifare; Считыватель смарт-карт ACR1252U-M1 (5шт); Программно-аппаратный комплекс Соболь 3.0; - 5шт. Программа для ЭВМ Индентификатор Rutoken S – 10 шт. Сетевой адаптер WiFi TP-Link TL-WN823N USB 2.0 (10шт); Коммутатор D-LINK DES-1016C/A1A; -1 шт. Сетевой экран Zyxel USG 40W (USG40W-RU0101F) – 1шт. Контроллер SIGUR E900I; ББП-20 Pro Tantos Источник вторичного электропитания резервированный 12В 2А (макс 3.5А) под акб.12В/7А•ч. Защита от глубокого разряда АКБ, Защита от КЗ; Аккумулятор Delta DT 1207; Извещатель, ИО 102-6, магнито-контактный, врезной на металическую дверь; Дверной замок; Считыватель PROX 13 - Reader карт формата MIFARE Classic 1k, Classic 4k, UltraLight, DESFire, с возможностью чтения кода из защищённой области карты (mad 3.0) (2шт); ПО Sigur Модуль базовый до 50 идентификаторов; Комплект Ezviz для управления Умным домом в составе: Ezviz Центр управления Умным домом (A1); Пульт дистанционного управления (K2); Ezviz Датчик движения (T1); Ezviz Датчик открытия-закрытия (T6); Ezviz Беспроводная сирена T9; Ezviz Беспроводной датчик протечки.
Лаборатория технической защиты информации, каб. 310.	Персональные компьютеры – 12 шт. Аппаратура акустической и виброакустической защиты SEL

	SP-55. Генератор шума переносной "Штора-1". Аппаратура акустической и виброакустической защиты SEL SP-55. Виброакустический электромагнитный излучатель (универсальный) SEL SP-55/V. Виброакустический электромагнитный излучатель SEL SP-55/VG. Многофункциональный прибор STO 31 "Пиранья". Нелинейный локатор "Лорнет». Осциллограф цифровой (БИТ). Алмаз обнаружитель видеокамер (БИТ). Беспроводная камера JMK. Monster 16CH. Уничтожитель информации Стек-НС1в.
Лаборатория сетей и систем передачи информации, каб. 310.	Cisco Catalist 2960. Cisco Catalist 3560. Cisco 2811. Cisco 2800. Системный блок. Монитор. Проектор и экран. Стабилизатор напряжения. Кондиционер. USB-Serial Port. Программное обеспечение: Notepad++. Cisco Packet Tracer. Bitvise SSH Client 7.39 (remove only). CCleaner. FileZilla Client. FreeCommander XE. GIMP 2.8.22. Google Chrome. HS 10.0 Express. LibreOffice 5.4 Help Pack. LibreOffice 5.4.3.2. Mozilla Firefox. MS Office 2010. NetBeans IDE. Nmap 7.60. Npcap 0.93. Oracle VM VirtualBox. Paint 3D. PuTTY. Pythol 3.6.2 (64-bit). SQL Server Browser for SQL Server 2014. VMware vSphere Client 5.1. Wireshark 2.4.2. 7-zip. Adobe Acrobat Reader DC. Adobe Flash Player.

6.Методические указания для обучающихся по освоению дисциплины

Методические указания для подготовки к практическим (семинарским) занятиям
Начиная подготовку к семинарскому занятию, необходимо, прежде всего, обратить внимание на конспект лекций, разделы учебников и учебных пособий, которые способствуют общему представлению о месте и значении темы в изучаемом курсе. Затем следует поработать с дополнительной литературой, сделать записи по рекомендованным источникам. Подготовка к семинарскому занятию включает 2 этапа:
- 1й этап - организационный;
- 2й этап - закрепление и углубление теоретических знаний. На первом этапе аспирант планирует свою самостоятельную работу, которая включает:
- уяснение задания, выданного на самостоятельную работу:
- подбор рекомендованной литературы;
- составление плана работы, в котором определяются основные пункты предстоящей подготовки.
Составление плана дисциплинирует и повышает организованность в работе. Второй этап включает непосредственную подготовку аспиранта к занятию. Начинать надо с изучения рекомендованной литературы. Необходимо помнить, что на лекции обычно рассматривается не весь материал, а только его часть. Остальная её часть восполняется в процессе самостоятельной работы. В связи с этим работа с рекомендованной литературой обязательна. Особое внимание при этом необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического приложения рассматриваемых теоретических вопросов. В процессе этой работы аспирант должен стремиться понять и запомнить основные положения рассматриваемого материала, примеры, поясняющие его, а также разобраться в иллюстративном материале. Заканчивать подготовку следует составлением плана (конспекта) по изучаемому материалу (вопросу). Это позволяет составить концентрированное, сжатое представление по изучаемым

вопросам. В процессе подготовки к занятиям рекомендуется взаимное обсуждение материала, во время которого закрепляются знания, а также приобретается практика в изложении и разъяснении полученных знаний, развивается речь. При необходимости следует обращаться за консультацией к преподавателю. Готовясь к консультации, необходимо хорошо продумать вопросы, которые требуют разъяснения.

В начале занятия аспиранты под руководством преподавателя более глубоко осмысливают теоретические положения по теме занятия, раскрывают и объясняют основные положения выступления.

Записи имеют первостепенное значение для самостоятельной работы обучающихся. Они помогают понять построение изучаемого материала, выделить основные положения и проследить их логику. Ведение записей способствует превращению чтения в активный процесс, мобилизует, наряду со зрительной, и моторную память, Следует помнить: у аспиранта, систематически ведущего записи, создается свой индивидуальный фонд подсобных материалов для быстрого повторения прочитанного, для мобилизации накопленных знаний. Особенно важны и полезны записи тогда, когда в них находят отражение мысли, возникшие при самостоятельной работе. Важно развивать умение сопоставлять источники, продумывать изучаемый материал.

Большое значение имеет совершенствование навыков конспектирования. Преподаватель может рекомендовать аспирантам следующие основные формы записи план (простой и развернутый), выписки, тезисы. Результаты конспектирования могут быть представлены в различных формах.

План - это схема прочитанного материала, краткий (или подробный) перечень вопросов, отражающих структуру и последовательность материала. Подробно составленный план вполне заменяет конспект.

Конспект - это систематизированное, логичное изложение материала источника. Различаются четыре типа конспектов.

План-конспект - это развернутый детализированный план, в котором достаточно подробные записи приводятся по тем пунктам плана, которые нуждаются в пояснении.

Текстуальный конспект – это воспроизведение наиболее важных положений и фактов источника.

Свободный конспект - это четко и кратко сформулированные (изложенные) основные положения в результате глубокого осмысливания материала. В нем могут присутствовать выписки, цитаты, тезисы; часть материала может быть представлена планом.

Тематический конспект составляется на основе изучения ряда источников и дает более или менее исчерпывающий ответ по какой-то схеме (вопросу).

Ввиду трудоемкости подготовки к семинару следует продумать алгоритм действий, еще раз внимательно прочитать записи лекций и уже готовый конспект по теме семинара, тщательно продумать свое устное выступление.

На семинаре каждый его участник должен быть готовым к выступлению по всем поставленным в плане вопросам, проявлять максимальную активность при их рассмотрении Выступление должно строиться свободно, убедительно и аргументировано Необходимо следить, чтобы выступление не сводилось к репродуктивному уровню (простому воспроизведению текста), не допускать и простое чтение конспекта. Необходимо, чтобы выступающий проявлял собственное отношение к тому, о чем он говорит, высказывал свое личное мнение, понимание, обосновывал его и мог сделать правильные выводы из сказанного.

Выступления других обучающихся необходимо внимательно и критически слушать, подмечать особенное в суждениях обучающихся, улавливать недостатки и ошибки. При этом обратить внимание на то, что еще не было сказано, или поддержать и развить интересную мысль, высказанную выступающим аспирантом. Изучение аспирантами фактического материала по теме практического занятия должно осуществляться заблаговременно. Под фактическим материалом следует понимать специальную

литературу по теме занятия, систему нормативных правовых актов, а также арбитражную практику по рассматриваемым проблемам. Особое внимание следует обратить на дискуссионные теоретические вопросы в системе изучаемого вопроса: изучить различные точки зрения ведущих ученых, обозначить противоречия современного законодательства. Для систематизации основных положений по теме занятия рекомендуется составление конспектов.

Обратить внимание на:

- составление списка нормативных правовых актов и учебной и научной литературы по изучаемой теме;
- изучение и анализ выбранных источников;
- изучение и анализ арбитражной практики по данной теме, представленной в информационно- справочных правовых электронных системах и др.;
- выполнение предусмотренных программой заданий в соответствии с тематическим планом;
- выделение наиболее сложных и проблемных вопросов по изучаемой теме, получение разъяснений и рекомендаций по данным вопросам с преподавателями кафедры на их еженедельных консультациях;
- проведение самоконтроля путем ответов на вопросы текущего контроля знаний, решения представленных в учебно-методических материалах кафедры задач, тестов, написания рефератов и эссе по отдельным вопросам изучаемой темы;

Семинарские занятия завершают изучение наиболее важных тем учебной дисциплины. Они служат для закрепления изученного материала, развития умений и навыков подготовки докладов, сообщений, приобретения опыта устных публичных выступлений, ведения дискуссии, аргументации и защиты выдвигаемых положений, а также для контроля преподавателем степени подготовленности обучающихся по изучаемой дисциплине.

Методические указания для обучающихся по освоению дисциплины дли самостоятельной работы

Методика организации самостоятельной работы аспирантов зависит от структуры, характера и особенностей изучаемой дисциплины, объема часов на ее изучение, вида заданий для самостоятельной работы аспирантов, индивидуальных особенностей аспирантов и условий учебной деятельности.

При этом преподаватель назначает аспирантам варианты выполнения самостоятельной работы, осуществляет систематический контроль выполнения аспирантами графика самостоятельной работы, проводит анализ и дает оценку выполненной работы.

Самостоятельная работа обучающихся осуществляется в аудиторной и внеаудиторной формах. Самостоятельная работа обучающихся в аудиторное время может включать:

- конспектирование (составление тезисов) лекций, выполнение контрольных работ;
- решение задач;
- работу со справочной и методической литературой;
- работу с нормативными правовыми актами;
- выступления с докладами, сообщениями на семинарских занятиях;
- защиту выполненных работ;
- участие в оперативном (текущем) опросе по отдельным темам изучаемой дисциплины;
- участие в собеседованиях, деловых (ролевых) играх, дискуссиях, круглых столах, конференциях;
- участие в тестировании и др.

Самостоятельная работа обучающихся во внеаудиторное время может состоять из:

- повторение лекционного материала;
- подготовки к семинарам (практическим занятиям);
- изучения учебной и научной литературы;
- изучения нормативных правовых актов (в т.ч. в электронных базах данных);
- решения задач, выданных на практических занятиях;

- подготовки к контрольным работам, тестированию и т.д.;
- подготовки к семинарам устных докладов (сообщений);
- подготовки рефератов, эссе и иных индивидуальных письменных работ по заданию преподавателя;
- выполнения курсовых работ, предусмотренных учебным планом;
- выделение наиболее сложных и проблемных вопросов по изучаемой теме, получение разъяснений и рекомендаций по данным вопросам с преподавателями кафедры на их еженедельных консультациях;
- проведение самоконтроля путем ответов на вопросы текущего контроля знаний, решения представленных в учебно-методических материалах кафедры задач, тестов;
- написания рефератов и эссе по отдельным вопросам изучаемой темы.
- подготовки к семинарам устных докладов (сообщений);
- подготовки рефератов, эссе и иных индивидуальных письменных работ по заданию преподавателя;
- выполнения курсовых работ, предусмотренных учебным планом;
- выполнения выпускных квалификационных работ и др.
- выделение наиболее сложных и проблемных вопросов по изучаемой теме, получение разъяснений и рекомендаций по данным вопросам с преподавателями кафедры на их еженедельных консультациях;
- проведение самоконтроля путем ответов на вопросы текущего контроля знаний, решения представленных в учебно-методических материалах кафедры задач, тестов;
- написания рефератов и эссе по отдельным вопросам изучаемой темы.