МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский государственный университет имени М.В.Ломоносова»

«Утверждаю»

Декан факультета ВМК МГУ
имени М.В. Ломоносова

академик _____ Е.И. Моисеев

_____ 2018 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Информационная безопасность компьютерных систем»

Уровень высшего образования – подготовка научно-педагогических кадров в аспирантуре

Направление подготовки – 10.06.01 «Информационная безопасность»

Направленность (профиль) – «Методы и системы защиты информации, информационная безопасность» (05.13.19)

2018 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

1. НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ

Информационная безопасность компьютерных систем

2. УРОВЕНЬ ВЫСШЕГО ОБРАЗОВАНИЯ

Подготовка научно-педагогических кадров в аспирантуре.

3. НАПРАВЛЕНИЕ ПОДГОТОВКИ, НАПРАВЛЕННОСТЬ (ПРОФИЛЬ) ПОДГОТОВКИ

Направление 10.06.01 «Информационная безопасность». Направленность (профиль) «Методы и системы защиты информации, информационная безопасность» (05.13.19).

4. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина относится к специальным дисциплинам вариативной части образовательной программы и является обязательной для освоения во 2-м семестре обучения.

5. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

Дисциплина участвует в формировании следующих компетенций образовательной программы:

Формируемые компетенции	Планируемые результаты обучения
Способность обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности (ОПК-3)	З1 (ОПК-3) ЗНАТЬ принципы управления доступом в компьютерных системах, современные методы защиты информации при передаче ее по каналам связи, современные стандарты информационной безопасности У1(ОПК-3) УМЕТЬ: обосновать степень соответствия защищаемых объектов информатизации и информатизационных систем действующим стандартам в области информационной безопасности.
Способностью формулировать научные задачи в области обеспечения	З1(ОПК-1) ЗНАТЬ

информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность (ОПК-1);	научные задачи в области обеспечения информационной безопасности У1(ОПК-1) УМЕТЬ: применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность В1(ОПК-1) ВЛАДЕТЬ: Навыками внедрения полученных результатов в практическую деятельность
Владение современными методами построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также методами разработки и реализации алгоритмов их решения на основе фундаментальных знаний в области математики и информатики (ПК-1)	З1 (ПК-1) ЗНАТЬ: современные методы разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения У1 (ПК-1) УМЕТЬ: применять современные методы построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современные методы разработки и реализации алгоритмов их решения В1 (ПК-1) ВЛАДЕТЬ: навыками оптимального выбора современных методов построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современных методов разработки и реализации алгоритмов их решения
Способность разрабатывать и реализовывать алгоритмы организации работы современных вычислительных комплексов и компьютерных сетей (ПК-2)	З1 (ПК-2) ЗНАТЬ: современные методы разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения У1 (ПК-2) УМЕТЬ: применять современные методы разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения В1 (ПК-2) ВЛАДЕТЬ: навыками оптимального выбора современных методов разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения
Способность планировать и решать задачи собственного профессионального	З1(УК-5(6)) ЗНАТЬ:

и личностного развития (УК-5(6))	содержание процесса целеполагания профессионального и личностного развития, его особенности и способы реализации при решении профессиональных задач, исходя из этапов карьерного роста и требований рынка труда. У1(УК-5(6)) УМЕТЬ: формулировать цели личностного и профессионального развития и условия их достижения, исходя из тенденций развития области профессиональной деятельности, этапов профессионального роста, индивидуально-личностных особенностей.
Способность к критическому анализу и оценке современных научных достижений, генерированию новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях (УК-1)	У2 (УК-1) УМЕТЬ: при решении исследовательских и практических задач генерировать новые идеи, поддающиеся операционализации исходя из наличных ресурсов и ограничений В2(УК-1) ВЛАДЕТЬ: навыками критического анализа и оценки современных научных достижений и результатов деятельности по решению исследовательских и практических задач, в том числе в междисциплинарных областях

Оценочные средства для промежуточной аттестации приведены в Приложении.

6. ОБЪЕМ ДИСЦИПЛИНЫ

Объем дисциплины составляет 3 зачетных единицы, всего 108 часов.

40 часов составляет контактная работа с преподавателем – 32 часа занятий лекционного типа, 0 часов занятий семинарского типа (семинары, научно-практические занятия, лабораторные работы и т.п.), 0 часов индивидуальных консультаций, 4 часа мероприятий текущего контроля успеваемости, 2 часа групповых консультаций, 2 часа мероприятий промежуточной аттестации.

68 часов составляет самостоятельная работа аспиранта.

7. ВХОДНЫЕ ТРЕБОВАНИЯ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Учащиеся должны владеть знаниями по операционным системам, компьютерным сетям, базам данных, дискретной математике и основам кибернетики в объеме, соответствующем основным образовательным программам бакалавриата и магистратуры по укрупненным группам направлений и специальностей 01.00.00 «Математика и механика», 02.00.00 «Компьютерные и информационные науки».

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В процессе обучения используется программное обеспечение для подготовки слайдов лекций MS PowerPoint, средство криптографической защиты информации КриптоПро CSP.

9. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

В курсе рассматриваются основные проблемы и задачи, связанные с обеспечением информационной безопасности. Рассматриваются требования к системам и средствам защиты информации от несанкционированного доступа, основные принципы политики информационной безопасности, модели безопасности компьютерных систем. Изучаются модели взаимодействия прикладных программ и программы-злоумышленника, принципы и методы защиты от разрушающих программных воздействий, проводится классификация разрушающих программных средств. Рассматриваются основные протоколы сетевого взаимодействия, изучаются методы защиты информации при ее передаче по каналам связи.

Наименование и краткое содержание разделов и тем дисциплины (модуля), **форма промежуточной аттестации по дисциплине (модулю)**	**Всего (часы)**	В том числе								
		Контактная работа (работа во взаимодействии с преподавателем), часы из них						**Самостоятельная работа обучающегося, часы** из них		
		Занятия лекционного типа	Занятия семинарского типа	Групповые консультации	Индивидуальные	Учебные занятия, направленные на проведение текущего контроля успеваемости (коллоквиумы,	**Всего**	Выполнение домашних заданий	Подготовка рефератов и т.п..	**Всего**

						практические контрольные занятия и др)*				
Тема 1. Задачи защиты информации в автоматизированных системах Основные понятия и термины. Особенности современных автоматизированных систем. Требования к системам и средствам защиты информации от несанкционированного доступа. Классификация автоматизированных систем и требования по защите информации. Показатели защищенности средств вычислительной техники. Соответствие классов систем различным уровням конфиденциальности. Понятие модели нарушителя информационной безопасности и модели угроз информационной безопасности. Политика безопасности. Принципы построения системы защиты информации. Определение уязвимостей автоматизированных систем и выбор средств защиты. Формирование требований к построению систем защиты. Создание автоматизированных систем в защищенном	13	6	-	-	-	1	7	6	-	6

исполнении.										
Тема 2. Методы защиты информации от утечки по техническим каналам Классификация каналов утечки информации. Методы защиты речевой информации. Методы защиты информации от утечки за счет побочных электромагнитных излучений и наводок. Специальные проверки и специальные исследования оборудования. Противодействие наблюдению в оптическом диапазоне. Инженерно-техническая защита информации. Методы противодействия разведкам.	10	2	-	-	-	-	2	2	6	8
Тема 3. Управление доступом в компьютерных системах Методы контроля доступа к ресурсам компьютерной системы. Модели безопасности компьютерных систем. Дискреционные модели безопасности: модель Харрисона-Рузо-Ульмана. Модель типизированных матриц доступа. Модель take-grant. Мандатное управление доступом.	15	8	-	-	-	1	9	6	-	6

Модель Белла-Лападулы. Модель LWM. Автоматная модель невлияния. Методы поиска остаточной информации на машинных носителях. Методы гарантированного удаления информации.										
Тема 4. Разрушающие программные воздействия и защита от них Сущность разрушающих программных воздействий. Модели взаимодействия прикладных программ и программы-злоумышленника, классификация разрушающих программных средств. Компьютерные вирусы. Принципы и методы защиты от разрушающих программных воздействий. Уязвимости приложений: атаки типа переполнение буфера, стека и кучи, атаки, основанные на изменении входных данных. Атаки на web-приложения: атаки типа SQL-инъекция и межсайтовый скриптинг. Безопасность сокетов. Безопасность ActiveX-элементов, DCOM-объектов и RPC-элементов. Атаки типа «отказ в обслуживании». Требования	9	4	-	-	-	1	5	4	-	4

ФСТЭК России к программному обеспечению средств защиты и его классификация по уровню отсутствия недекларированных возможностей.										
Тема 5. Методы защиты информации при передаче ее по каналам связи Виртуальные частные сети. Криптографическая защита трафика на всех уровнях модели ISO/OSI. Криптографическая защиты сетевого уровня. Семейство протоколов IPsec и его модификации. Средства криптографической защиты прикладного уровня. Протокол SSL/TLS. Протокол RADIUS, протокол Kerberos. Проблема разграничения доступа в компьютерных сетях. Понятие межсетевого экрана. Виды межсетевых экранов. Принципы работы межсетевых экранов. Уязвимости основных протоколов сетевого взаимодействия. Понятие системы обнаружения вторжений и ее функции. Основные методы детектирования атак.	23	12	-	2	-	1	15	8	-	8

6. Промежуточная аттестация – устный экзамен	38	2	36
Итого	108	40	68

10. УЧЕБНО-МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ УЧАЩИХСЯ

Самостоятельная работа учащихся состоит в изучении лекционного материала, учебно-методической литературы, подготовки к текущему контролю и промежуточной аттестации. В рамках изучения Темы 2 учащиеся готовят реферат.

Литература для самостоятельной работы студентов в соответствии с тематическим планом (список литературы приведен в п. 11).

Тема 1 «Задачи защиты информации в автоматизированных системах»

- ✓ Борисов М.А., Заводцев И.В., Чижов И.В. Основы программно-аппаратной защиты информации, Москва: Книжный дом «Либроком», 2013.
- ✓ Официальный сайт ФСТЭК России: http://www.fstec.ru.
- ✓ "Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. ГОСТ Р 51275-2006" (утв. Приказом Ростехрегулирования от 27.12.2006 № 374-ст) // М., Стандартинформ, 2007.
- ✓ "Защита информации. Основные термины и определения. ГОСТ Р 50922-2006" (утв. Приказом Ростехрегулирования от 27.12.2006 № 373-ст) // М., Стандартинформ, 2008.

Тема 2 «Методы защиты информации от утечки по техническим каналам»

- ✓ Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: Учебное пособие. - М.: Горячая линия, 2005.
- ✓ Торокин А.А. Инженерно-техническая защита информации: Учебное пособие. - М.: Гелиос-АРВ, 2005.
- ✓ "Техническая защита информации. Основные термины и определения. Р 50.1.056-2005", (утв. приказом Ростехрегулирования от 29.12.2005 № 479-ст) // М., Стандартинформ, 2006.

Тема 3 «Управление доступом в компьютерных системах»

- ✓ Грушо А.А. Применко Э.А. Тимонина Е.Е. Теоретические основы компьютерной безопасности. – М.: Издательский центр "Академия", 2009.

✓ Девянин П.Н. Модели безопасности компьютерных систем: Учеб. пособие. – М.: Издательский центр «Академия», 2005. – 144 с.
✓ Корт С.С. Теоретические основы защиты информации: Учебное пособие. – М.: Гелиос АРВ, 2004. – 240 с.
✓ Гайдамакин Н.А. Разграничение доступа к информации в компьютерных системах. – Екатеринбург: изд-во Урал. Ун-та, 2003. – 328 с.
✓ Теория и практика обеспечения информационной безопасности / Под ред. П.Д. Зегжды. М.:Яхтсмен, 1996. - 302с

Тема 4 «Разрушающие программные воздействия и защита от них»

✓ Борисов М.А., Заводцев И.В., Чижов И.В. Основы программно-аппаратной защиты информации, Москва: Книжный дом «Либроком», 2013.
✓ "Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. ГОСТ Р 51188-98" (прин. Постановлением Госстандарта РФ от 14.07.1998 № 295) // М., Стандартинформ, 1998.

Тема 5 «Методы защиты информации при передаче ее по каналам связи»

✓ "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. ГОСТ Р.34.10-2001" (утв. Постановлением Госстандарта РФ от 12.09.2001 № 380-ст) // М., Стандартинформ, 2002.
✓ Борисов М.А., Заводцев И.В., Чижов И.В. Основы программно-аппаратной защиты информации, Москва: Книжный дом «Либроком», 2013.
✓ "Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма. ГОСТ Р.34.10-94" (утв. Постановлением Госстандарта РФ от 23.05.1994 № 154) // М., Стандартинформ, 1994.
✓ "Информационная технология. Криптографическая защита информации. Функция хэширования. ГОСТ Р.34.11-94" (утв. Постановлением Госстандарта РФ от 23.05.1994 № 154) // М., Стандартинформ, 1994.
✓ "Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. ГОСТ 28147-89" (утв. Постановлением Госстандарта РФ от 02.06.1989 № 1409) // М.: ИПК Издательство стандартов, 1998.

11. РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ

Основная литература

1. Борисов М.А., Заводцев И.В., Чижов И.В. Основы программно-аппаратной защиты информации, Москва: Книжный дом «Либроком», 2013.
2. Платонов В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей : учеб. пособие

для студ. высш. учеб. заведений / В.В.Платонов // - М.: Издательский центр "Академия", 2006.
3. Грушо А.А. Применко Э.А. Тимонина Е.Е. Теоретические основы компьютерной безопасности. – М.: Издательский центр "Академия", 2009.
4. Девянин П.Н. Модели безопасности компьютерных систем: Учеб. пособие. – М.: Издательский центр «Академия», 2005. – 144 с.

Дополнительная литература

1. Торокин А.А. Инженерно-техническая защита информации: Учебное пособие. - М.: Гелиос-АРВ, 2005.
2. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: Учебное пособие. - М.: Горячая линия, 2005.
3. "Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. ГОСТ Р 51275-2006" (утв. Приказом Ростехрегулирования от 27.12.2006 № 374-ст) // М., Стандартинформ, 2007.
4. "Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. ГОСТ 28147-89" (утв. Постановлением Госстандарта РФ от 02.06.1989 № 1409) // М.: ИПК Издательство стандартов, 1998.
5. "Информационная технология. Криптографическая защита информации. Функция хэширования. ГОСТ Р.34.11-94" (утв. Постановлением Госстандарта РФ от 23.05.1994 № 154) // М., Стандартинформ, 1994.
6. "Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма. ГОСТ Р.34.10-94" (утв. Постановлением Госстандарта РФ от 23.05.1994 № 154) // М., Стандартинформ, 1994.
7. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. ГОСТ Р.34.10-2001" (утв. Постановлением Госстандарта РФ от 12.09.2001 № 380-ст) // М., Стандартинформ, 2002.
8. "Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. ГОСТ Р 51188-98" (прин. Постановлением Госстандарта РФ от 14.07.1998 № 295) // М., Стандартинформ, 1998.
9. Теория и практика обеспечения информационной безопасности / Под ред. П.Д. Зегжды. М.:Яхтсмен, 1996. - 302с
10. Гайдамакин Н.А. Разграничение доступа к информации в компьютерных системах. – Екатеринбург: изд-во Урал. Ун-та, 2003. – 328 с.
11. Корт С.С. Теоретические основы защиты информации: Учебное пособие. – М.: Гелиос АРВ, 2004. – 240 с.
12. "Техническая защита информации. Основные термины и определения. Р 50.1.056-2005", (утв. приказом Ростехрегулирования от 29.12.2005 № 479-ст) // М., Стандартинформ, 2006.
13. "Защита информации. Основные термины и определения. ГОСТ Р 50922-2006" (утв. Приказом Ростехрегулирования от 27.12.2006 № 373-ст) // М., Стандартинформ, 2008.

14. Официальный сайт ФСТЭК России: http://www.fstec.ru.

Ресурсы информационно-телекоммуникационной сети «Интернет»

1. Официальный сайт ФСТЭК России: http://www.fstec.ru.
2. http://elibrary.ru
3. www.scopus.com

Информационные технологии, используемые в процессе обучения

1. Программное обеспечение для подготовки слайдов лекций MS PowerPoint
2. Программное обеспечение для создания и просмотра pdf-документов Adobe Reader
3. Издательская система LaTeX.
4. Средство криптографической защиты информации КриптоПро CSP.

Активные и интерактивные формы проведения занятия

№ п\п	Тип занятия или внеаудиторной работы	Вид и тематика (название) интерактивного занятия
1	Лекция 5	Лекция-конференция на тему «Техническая защита информации»
2	Лекция 16	Деловая игра «Фирма по оказанию услуг в области защиты информации»

Материально-техническая база

Для преподавания дисциплины требуется класс, оборудованный маркерной или меловой доской и проектором.

Для демонстрации современных средств защиты требуется компьютерный класс с установленным средством виртуализации «VirtualBox».

Для демонстрации аппаратных средств защиты требуется наличие компьютеров с разъёмом PCI-express.

12. ЯЗЫК ПРЕПОДАВАНИЯ

Русский

13. РАЗРАБОТЧИК ПРОГРАММЫ, ПРЕПОДАВАТЕЛИ

доцент, к.ф.-м.н. Чижов Иван Владимирович

Приложение

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

«Информационная безопасность компьютерных систем»

Средства для оценивания планируемых результатов обучения, критерии и показатели оценивания приведены ниже.

РЕЗУЛЬТАТ ОБУЧЕНИЯ по дисциплине (модулю)	**КРИТЕРИИ и ПОКАЗАТЕЛИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТА ОБУЧЕНИЯ по дисциплине (модулю)** *(критерии и показатели берутся из соответствующих карт компетенций, при этом пользуются либо традиционной системой оценивания, либо БРС)*					**ОЦЕНОЧНЫЕ СРЕДСТВА**
	1	2	3	4	5	
	Неудовлетворительно	**Неудовлетвори-тельно**	**Удовлетвори-тельно**	**Хорошо**	**Отлично**	
ЗНАТЬ: принципы управления доступом в компьютерных системах, современные методы защиты информации при передаче ее по каналам связи, современные стандарты информационной безопасности З1 (ОПК-3)	Отсутствие знаний	Фрагментарные представления о принципах управления доступом в компьютерных системах, современных методах защиты информации при передаче ее по каналам связи, современных стандартах информационной безопасности	В целом сформированные, но неполные знания о принципах управления доступом в компьютерных системах, современных методах защиты информации при передаче ее по каналам связи, современных стандартах информационной безопасности	Сформированные, но содержащие отдельные пробелы знания о принципах управления доступом в компьютерных системах, современных методах защиты информации при передаче ее по каналам связи, современных стандартах информационной безопасности	Сформированные систематические знания о принципах управления доступом в компьютерных системах, современных методах защиты информации при передаче ее по каналам связи, современных стандартах информационной безопасности	Устный экзамен
УМЕТЬ: обосновать степень соответствия	Отсутствие умений	Фрагментарные умения обоснования степени соответствия	В целом успешное, но не систематическое	Успешное, но содержащее отдельные	Сформированное умение обоснования степени соответствия	Контрольные работы

защищаемых объектов информатизации и информатизационных систем действующим стандартам в области информационной безопасности. У1(ОПК-3)		защищаемых объектов информатизации и информатизационных систем действующим стандартам в области информационной безопасности.	умение обоснования степени соответствия защищаемых объектов информатизации и информатизационных систем действующим стандартам в области информационной безопасности.	пробелы умение обоснования степени соответствия защищаемых объектов информатизации и информатизационных систем действующим стандартам в области информационной безопасности.	защищаемых объектов информатизации и информатизационных систем действующим стандартам в области информационной безопасности.	
ЗНАТЬ: современные методы построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современные методы разработки и реализации алгоритмов их решения З1 (ПК-1)	Отсутствие знаний	Фрагментарные представления о современных методах построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современных методах разработки и реализации алгоритмов их решения	В целом сформированные, но неполные знания о современных методах построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современных методах разработки и реализации алгоритмов их решения	Сформированные, но содержащие отдельные пробелы знания о современных методах построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современных методах разработки и реализации алгоритмов их решения	Сформированные систематические знания о современных методах построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современных методах разработки и реализации алгоритмов их решения	Устный экзамен
УМЕТЬ: применять	Отсутствие умений	Фрагментарные умения применять	В целом успешное, но не	Успешное, но содержащее	Сформированное умение применять	Контрольные работы

современные методы построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современные методы разработки и реализации алгоритмов их решения У1 (ПК-1)		современные методы построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современные методы разработки и реализации алгоритмов их решения	систематическое умение применять современные методы построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современные методы разработки и реализации алгоритмов их решения	отдельные пробелы умение применять современные методы построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современные методы разработки и реализации алгоритмов их решения	современные методы построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современные методы разработки и реализации алгоритмов их решения	
ВЛАДЕТЬ: навыками оптимального выбора современных методов построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современных методов разработки и реализации алгоритмов их решения В1 (ПК-1)	Отсутствие навыков	Фрагментарное владение навыками оптимального выбора современных методов построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современных методов разработки и реализации алгоритмов их решения	В целом успешное, но не полное владение навыками оптимального выбора современных методов построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современных методов	Успешное, но содержащее отдельные пробелы владение навыками оптимального выбора современных методов построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современных	Сформированное владение навыками оптимального выбора современных методов построения и анализа математических моделей, возникающих при решении естественнонаучных задач, а также современных методов разработки и реализации алгоритмов их решения	Контрольные работы, реферат

			разработки и реализации алгоритмов их решения	методов разработки и реализации алгоритмов их решения		
ЗНАТЬ: современные методы разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения Код З1 (ПК-2)	Отсутствие знаний	Фрагментарные представления о современных методах разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения	В целом сформированные, но неполные знания о современных методах разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения	Сформированные, но содержащие отдельные пробелы знания о современных методах разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения	Сформированные систематические знания о современных методах разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения	Устный экзамен
УМЕТЬ: применять современные методы разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения Код У1 (ПК-2)	Отсутствие умений	Фрагментарные умения применять современные методы разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения	В целом успешное, но не систематическое умение применять современные методы разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения	Успешное, но содержащее отдельные пробелы умение применять современные методы разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего	Сформированное умение применять современные методы разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения	Устный экзамен

				поколения		
ВЛАДЕТЬ: навыками оптимального выбора современных методов разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения Код В1 (ПК-2)	Отсутствие навыков	Фрагментарное владение навыками оптимального выбора современных методов разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения	В целом успешное, но не полное владение навыками оптимального выбора современных методов разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения	Успешное, но содержащее отдельные пробелы владение навыками оптимального выбора современных методов разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения	Сформированное владение навыками оптимального выбора современных методов разработки и реализации алгоритмов организации работы вычислительных комплексов и компьютерных сетей последнего поколения	Устный экзамен
ЗНАТЬ: научные задачи в области обеспечения информационной безопасности З1(ОПК-1)	Отсутствие знаний	Фрагментарные представления о научных задачах в области обеспечения информационной безопасности	В целом сформированные, но неполные знания о научных задачах в области обеспечения информационной безопасности	Сформированные, но содержащие отдельные пробелы о научных задачах в области обеспечения информационной безопасности	Сформированные систематические знания о научных задачах в области обеспечения информационной безопасности	Устный экзамен
УМЕТЬ: применять для задачи в области обеспечения ИБ решения методологии теоретических и экспериментальных	Отсутствие умений	Фрагментарные умения применять для задачи в области обеспечения ИБ решения методологии теоретических и экспериментальных	В целом успешное, но не систематическое умение применять для задачи в области обеспечения ИБ решения	Успешное, но содержащее отдельные пробелы умение применять для задачи в области обеспечения ИБ решения	Сформированное умение применять для задачи в области обеспечения ИБ решения методологии теоретических и экспериментальных	Устный экзамен

научных исследований, внедрять полученные результаты в практическую деятельность У1(ОПК-1)		научных исследований, внедрять полученные результаты в практическую деятельность	методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность	методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность	научных исследований, внедрять полученные результаты в практическую деятельность	
ВЛАДЕТЬ: Навыками внедрения полученных результатов в практическую деятельность В1(ОПК-1)	Отсутствие навыков	Фрагментарное владение навыками внедрения полученных результатов в практическую деятельность	В целом успешное, но не полное владение навыками внедрения полученных результатов в практическую деятельность	Успешное, но содержащее отдельные пробелы владение навыками внедрения полученных результатов в практическую деятельность	Сформированное владение навыками внедрения полученных результатов в практическую деятельность	устный экзамен
ЗНАТЬ: содержание процесса целеполагания профессионального и личностного развития, его особенности и способы реализации при решении профессиональных задач, исходя из этапов карьерного роста и требований рынка труда. З1(УК-5(6))	Не имеет базовых знаний о сущности процесса целеполагания, его особенностях и способах реализации.	Допускает существенные ошибки при раскрытии содержания процесса целеполагания, его особенностей и способов реализации.	Демонстрирует частичные знания содержания процесса целеполагания, некоторых особенностей профессионального развития и самореализации личности, указывает способы реализации, но не может обосновать	Демонстрирует знания сущности процесса целеполагания, отдельных особенностей процесса и способов его реализации, характеристик профессионального развития личности, но не выделяет критерии выбора	Раскрывает полное содержание процесса целеполагания, всех его особенностей, аргументированно обосновывает критерии выбора способов профессиональной и личностной целереализации при решении профессиональных задач.	Отчеты, доклады на научных семинарах

			возможность их использования в конкретных ситуациях.	способов целереализации при решении профессиональных задач.		
УМЕТЬ: формулировать цели личностного и профессионального развития и условия их достижения, исходя из тенденций развития области профессиональной деятельности, этапов профессионального роста, индивидуально-личностных особенностей. У1(УК-5(6))	Не умеет и не готов формулировать цели личностного и профессионального развития и условия их достижения, исходя из тенденций развития области профессиональной деятельности, этапов профессионального роста, индивидуально-личностных особенностей.	Имея базовые представления о тенденциях развития профессиональной деятельности и этапах профессионального роста, не способен сформулировать цели профессионального и личностного развития.	При формулировке целей профессионального и личностного развития не учитывает тенденции развития сферы профессиональной деятельности и индивидуально-личностные особенности.	Формулирует цели личностного и профессионального развития, исходя из тенденций развития сферы профессиональной деятельности и индивидуально-личностных особенностей, но не полностью учитывает возможные этапы профессиональной социализации.	Готов и умеет формулировать цели личностного и профессионального развития и условия их достижения, исходя из тенденций развития области профессиональной деятельности, этапов профессионального роста, индивидуально-личностных особенностей.	Отчеты, доклады на научных семинарах
УМЕТЬ: при решении исследовательских и практических задач генерировать новые идеи, поддающиеся операционализации исходя из наличных ресурсов и ограничений У2 (УК-1)	Отсутствие умений	Частично освоенное умение при решении исследовательских и практических задач генерировать идеи, поддающиеся операционализации исходя из наличных ресурсов и ограничений	В целом успешное, но не систематически осуществляемое умение при решении исследовательских и практических задач генерировать идеи, поддающиеся операционализаци и исходя из	В целом успешное, но содержащее отдельные пробелы умение при решении исследовательских и практических задач генерировать идеи, поддающиеся операционализаци и исходя из	Сформированное умение при решении исследовательских и практических задач генерировать идеи, поддающиеся операционализации исходя из наличных ресурсов и ограничений	доклады на научных семинарах

			наличных ресурсов и ограничений	наличных ресурсов и ограничений		
ВЛАДЕТЬ: навыками критического анализа и оценки современных научных достижений и результатов деятельности по решению исследовательских и практических задач, в том числе в междисциплинарных областях В2 (УК-1)	Отсутствие навыков	Фрагментарное применение технологий критического анализа и оценки современных научных достижений и результатов деятельности по решению исследовательских и практических задач.	В целом успешное, но не систематическое применение технологий критического анализа и оценки современных научных достижений и результатов деятельности по решению исследовательских и практических задач.	В целом успешное, но содержащее отдельные пробелы применение технологий критического анализа и оценки современных научных достижений и результатов деятельности по решению исследовательских и практических задач.	Успешное и систематическое применение технологий критического анализа и оценки современных научных достижений и результатов деятельности по решению исследовательских и практических задач.	доклады на научных семинарах

Фонды оценочных средств, необходимые для оценки результатов обучения

Список вопросов для устного экзамена.

1. Особенности современных автоматизированных систем.
2. Требования к системам и средствам защиты информации от несанкционированного доступа.
3. Классификация автоматизированных систем и требования по защите информации.
4. Показатели защищенности средств вычислительной техники.
5. Соответствие классов систем различным уровням конфиденциальности.
6. Понятие модели нарушителя информационной безопасности и модели угроз информационной безопасности.
7. Политика безопасности.

8. Принципы построения системы защиты информации.
9. Определение уязвимостей автоматизированных систем и выбор средств защиты.
10. Формирование требований к построению систем защиты.
11. Создание автоматизированных систем в защищенном исполнении.
12. Классификация каналов утечки информации.
13. Методы защиты речевой информации.
14. Методы защиты информации от утечки за счет побочных электромагнитных излучений и наводок.
15. Специальные проверки и специальные исследования оборудования.
16. Противодействие наблюдению в оптическом диапазоне.
17. Инженерно-техническая защита информации.
18. Методы противодействия разведкам.
19. Методы контроля доступа к ресурсам компьютерной системы.
20. Модели безопасности компьютерных систем.
21. Дискреционные модели безопасности: модель Харрисона-Рузо-Ульмана.
22. Модель типизированных матриц доступа.
23. Модель take-grant.
24. Мандатное управление доступом.
25. Модель Белла-Лападулы.
26. Модель LWM.
27. Автоматная модель невлияния.
28. Методы поиска остаточной информации на машинных носителях.
29. Методы гарантированного удаления информации.
30. Сущность разрушающих программных воздействий.
31. Модели взаимодействия прикладных программ и программы-злоумышленника, классификация разрушающих программных средств.
32. Компьютерные вирусы. Принципы и методы защиты от разрушающих программных воздействий.
33. Уязвимости приложений: атаки типа переполнение буфера, стека и кучи, атаки, основанные на изменении входных данных.
34. Атаки на web-приложения: атаки типа SQL-инъекция и межсайтовый скриптинг.
35. Безопасность сокетов.
36. Безопасность ActiveX-элементов, DCOM-объектов и RPC-элементов.
37. Атаки типа «отказ в обслуживании».

38. Требования ФСТЭК России к программному обеспечению средств защиты и его классификация по уровню отсутствия недекларированных возможностей.
39. Виртуальные частные сети. Криптографическая защита трафика на всех уровнях модели ISO/OSI.
40. Криптографическая защиты сетевого уровня. Семейство протоколов IPsec и его модификации.
41. Средства криптографической защиты прикладного уровня. Протокол SSL/TLS.
42. Протокол RADIUS, протокол Kerberos.
43. Проблема разграничения доступа в компьютерных сетях. Понятие межсетевого экрана.
44. Виды межсетевых экранов. Принципы работы межсетевых экранов.
45. Уязвимости основных протоколов сетевого взаимодействия.
46. Понятие системы обнаружения вторжений и ее функции. Основные методы детектирования атак.

Материалы для мероприятий текущего контроля.

Мероприятия текущего контроля реализуются в виде тестов с выбором вариантов ответа. Четыре набора тестов охватывают теоретический материал, относящийся соответственно к темам 1, 3, 4 и 5. Вопросы тестов соответствуют приведенным выше вопросам к устному экзамену, раскрывая их на более подробном уровне.

Примерные темы рефератов.

Реферат посвящен Теме 2. Примеры тем:

1. Методические подходы к оценке эффективности защиты речевой информации.
2. Электромагнитные низкочастотные каналы утечки информации.
3. Маскирование сигналов шумами, коррелированными с сигналами.
4. Задачи контроля каналов утечки информации в реальном масштабе времени.

Методические материалы для проведения процедур оценивания результатов обучения

Особенности организации процесса обучения

Для эффективного освоения курса рекомендуется перед каждым занятие привести в порядок конспекты лекций. После каждого занятия рекомендуется найти и прочитать дополнительную литературу по теме лекции и прочитать свои конспекты.

Система контроля и оценивания

За каждую контрольную работу и реферат выставляются баллы (максимум 10 баллов за каждый вид работы). Пусть М – максимальное число баллов, которое может набрать студент. В конце семестра баллы конвертируются в оценку О1 следующим образом:

меньше М/2 баллов: О1=2;

больше или равно М/2 баллов, но меньше 2М/3: О1=3;

больше или равно 2М/3 баллов, но меньше 5М/6: О1=4;

больше или равно 5М/6 баллов: О1=5.

На экзамене оценка О1 является стартовой. Окончательная оценка определяется исходя из оценки устного ответа студента, при этом она не может отличаться от стартовой оценки более чем на 1 балл.

Структура и график контрольных мероприятий

Контрольная работа на 3-й, 8-й, 10-й, 14-й неделях, реферат в течение семестра, устный экзамен в конце семестра.