Приложение 3.РПД Б1.В.ОД.10

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

УТВЕРЖДАЮ
Зам. директора
филиала ФГБОУ ВО «НИУ «МЭИ»
в г. Смоленске
по учебно-методической работе
_____ В.В. Рожков
«____» _____ 2016 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ЗАЩИТА ИНФОРМАЦИИ

(НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ)

Направление подготовки: 09.03.01 Информатика и вычислительная техника

Профиль подготовки: Вычислительные машины, комплексы, системы и сети

Уровень высшего образования: бакалавриат

Нормативный срок обучения: 4 года

Форма обучения: очная

Смоленск – 2016 г.

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

Целью дисциплины «Защита информации» является подготовка обучающихся по направлению подготовки 09.03.01 "Информатика и вычислительная техника" посредством обеспечения этапов формирования компетенций, предусмотренных ФГОС, в части представленных ниже знаний, умений и навыков.

Задачами дисциплины являются:

- дать знания студентам по основным угрозам безопасности компьютерных систем;
- дать знания основных стандартов безопасности компьютерных систем;
- дать знания моделей безопасности компьютерных систем;
- дать знания основных криптографических систем;
- дать знания основ администрирования сетей и защиты информации в сетях.

Дисциплина направлена на формирование следующих общепрофессиональных и профессиональных компетенций:

- ОПК-1. Способностью инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем.
- ОПК-2. Способностью осваивать методики использования программных средств для решения практических задач.
- ОПК-4. Способностью участвовать в настройке и наладке программно-аппаратных комплексов.
- ОПК-5. способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
- ПК-3. способностью обосновывать принимаемые проектные решения, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности.

В результате освоения дисциплины обучающийся должен знать:

- актуальность и важность проблемы информационной безопасности (ОПК-5)
- цели, задачи, принципы и основные направления обеспечения информационной безопасности (ОПК-5, ПК-3);
- знать основные положения законодательства в области современного авторского права и защиты информации (ОПК-2);
- эволюцию, тенденцию и перспективы развития методов и средств защиты компьютерной информации (ОПК-2);
- основные методы защиты конфиденциальной компьютерной информации (ОПК-5, ПК-3, ОПК-1);
- основные понятия, используемые в сфере защиты информации (ОПК-5);
- угрозы информационной безопасности и классификацию каналов несанкционированного доступа к информации (ОПК-5);
- современные подходы к построению систем защиты информации (ПК-3, ОПК-4, ОПК-5);

В результате освоения дисциплины обучающийся должен уметь:

- анализировать информационную инфраструктуру (ОПК-2);
- пользоваться современной научно-технической информацией по исследуемым проблемам и задачам (ОПК-2);

- принимать адекватные решения при выборе средств защиты информации на основе анализа угроз (ОПК-5, ПК-3);
- выбирать и анализировать показатели качества систем и отдельных методов и средств защиты информации (ОПК-2);
- осуществлять поиск и анализировать научно-техническую литературу и выбирать необходимые материалы (ОПК-2, ОПК-4);
- определять и анализировать угрозы безопасности информации в зависимости от среды эксплуатации продуктов информационных технологий (ОПК-1, ОПК-5, ПК-3);
- разрабатывать модели компонентов систем защиты информации (ОПК-5, ПК-3)
- использовать современные программные средства для шифрования и сокрытия информации (ПК-3)
- выбирать оптимальные методы защиты конфиденциальной информации (ОПК-5).
- применять полученные знания при выполнении курсовых проектов и выпускных квалификационных работ, а также в ходе научных исследований (ПК-3)
- анализировать информацию на предмет сокрытия в ней данных (ОПК-1, ПК-3);
- разрабатывать и создавать типовые схемы защиты информации на основе современных средств обеспечения информационной безопасности (ОПК-5, ПК-3);

В результате освоения дисциплины обучающийся должен владеть:

- навыками дискуссии по профессиональной тематике (ОПК-4);
- терминологией в области защиты информации (ОПК-2).
- навыками создания защищенной среды с помощью аппаратно-программных средств защиты (ОПК-1, ОПК-2, ОПК-4, ПК-3) ;
- навыками разработки защищенных приложений (ОПК-5, ПК-3)
- навыками самостоятельного проектирования систем защиты информации (ОПК-5, ПК-3)

2 Место дисциплины в структуре образовательной программы

Дисциплина «Защита информации» относится к вариативной части профессионального цикла Б.1.В.ОД.10 основной образовательной программы подготовки бакалавров по профилям "Вычислительные машины, системы и сети" и "Автоматизированные системы обработки информации и управления" направления 09.03.01 "Информатика и вычислительная техника".

В соответствии с учебным планом по направлению "Информатика и вычислительная техника" дисциплина «Защита информации» базируется на следующих дисциплинах:

- Б1.Б.7 Информатика
- Б1.В.ОД.1 Программирование
- Б1.Б.8 Инженерная графика
- Б1.Б.14 Высшая математика
- Б1.Б.5 Физика
- Б2.У.1 Практика по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности
- Б2.У.2 Исполнительская практика
- Б1.Б.9 ЭВМ и периферийные устройства
- Б1.В.ОД.4 Операционные системы
- Б1.В.ОД.5 Компьютерная графика
- Б1.В.ОД.6 Технология программирования
- Б1.В.ДВ.3.1 Введение в оптимизацию

- Б1.В.ДВ.3.2 Теория систем
- Б1.Б.6 Теория вероятностей и математическая статистика
- Б1.Б.15 Вычислительная математика
- Б1.В.ОД.3 Теория алгоритмов
- Б1.В.ОД.2 Дискретная математика
- Б2.П.1 Практика по получению профессиональных умений и опыта профессиональной деятельности
- Б2.П.3 Технологическая практика
- Б1.Б.10 Базы данных
- Б1.В.ОД.16 Конструирование и технологии средств вычислительной техники
- Б1.В.ОД.7 Сети и телекоммуникации
- Б1.В.ОД.11 Теория автоматов
- Б1.В.ОД.13 Основы теории управления
- Б1.В.ОД.15 Сопровождение разработки программного обеспечения
- Б1.В.ОД.17 Инженерное проектирование и САПР
- Б1.В.ДВ.5.1 Прикладная статистика
- Б1.В.ДВ.5.2 Методы анализа данных
- Б1.Б.13 Правоведение
- Б1.Б.18 Схемотехника

.

Знания, полученные по освоению дисциплины «Защита информации», необходимы при выполнении бакалаврской выпускной квалификационной работы и для освоения следующих дисциплин направления подготовки 09.03.01:

- Б1.В.ОД.14 Тестирование программного обеспечения
- Б1.В.ОД.8 Сетевые технологии
- Б1.В.ОД.9 Микропроцессорные системы
- Б1.В.ОД.12 Моделирование
- Б1.В.ДВ.6.1 Аппаратная реализация алгоритмов
- Б1.В.ДВ.6.2 Технология проектирования устройств на ПЛИС
- Б1.В.ДВ.7.1 Теория передачи информации
- Б1.В.ДВ.7.2 Методы и средства цифровой связи
- Б1.В.ДВ.9.1 Проектирование информационных систем
- Б1.В.ДВ.9.2 Информационные технологии
- Б1.В.ДВ.10.1 Корпоративные и ведомственные сети
- Б1.В.ДВ.10.2 Технологические сети для сбора данных и управления
- Б1.В.ДВ.8.1 Основы теории надежности
- Б1.В.ДВ.8.2 Надежность и диагностика технических средств
- Б1.В.ДВ.11.1 Интернет-технологии
- Б1.В.ДВ.11.2 Проектирование Web-приложений
- Б1.В.ДВ.4.1 Введение в цифровую обработку сигналов
- Б1.В.ДВ.4.2 Теория сигналов
- Б2.П.4 Преддипломная практика
- Б3 Государственная итоговая аттестация

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

Общая трудоемкость дисциплины составляет 5 зачетных единиц, 180 часов.

Аудиторная работа

Цикл:	Б1	Семестр
Часть цикла:	Вариативная Обязательная дисциплина	
Индекс дисциплины по учебному плану	Б1.В.ОД.10	
Часов всего по учебному плану	180	7 семестр
Трудоемкость в зачетных единицах (ЗЕТ)	5	7 семестр
Лекции (ЗЕТ/ часов)	1/36	7 семестр
Лабораторные работы (ЗЕТ/ часов)	1/36	7 семестр
Объем самостоятельной работы по учебному плану (ЗЕТ/ часов всего)	2/72	7 семестр
Экзамен	1/36	7 семестр

Самостоятельная работа студента

Вид работ	Трудоёмкость	
	ЗЕТ	*час*
Подготовка к лекции	0,39	14
Изучение дополнительного теоретического материала	0,33	12
Подготовка к сеансу тестирования	0,31	11
Подготовка к контрольной работе	0,22	8
Подготовка к выполнению и защите лабораторных работ (лаб)	0,75	27
Всего:	**2**	**72**

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

№ п/п	Темы дисциплины	Общая трудоемкость, всего	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)					
			Аудиторные занятия			Экзамен	Самостоятельная работа	Занятия в интерактивной форме
			Всего	Лекции	Лабораторные работы			
1	Источники, риски и формы атак на компьютерные системы.	19	10	6	4		9	
2	Модели безопасности информационных систем	9	4	4			5	
3	Стандарты безопасности. Законодательные меры защиты информации	8	2	2			6	
4	Криптографические модели и методы защиты информации	41	22	10	12		19	
5	Защита информации в современных операционных системах	38	20	4	16		18	
6	Защита информации в сети	29	14	10	4		15	
Экзамен		36				36		
Всего		**180**	**72**	**36**	**36**	**36**	**72**	

Тема 1. Источники, риски и формы атак на компьютерные системы

Лекция 1 (2 часа)

Функции и задачи защиты информации. Методы и системы защиты информации. Основные виды угроз безопасности. Классификация атак на вычислительные системы. Сетевые атаки. Кодификатор компьютерных преступлений интерпола.

Лекция 2 (2часа)

Компьютерные вирусы. Классификация вирусов. Алгоритмы вирусов. Признаки проявления вируса. Методы защиты. Классы антивирусных программ.

Лекция 3 (2 часа)

Услуги информационной безопасности. Механизмы безопасности. Соотношение между услугами безопасности и механизмами обеспечения безопасности. Методы обеспечения безопасности.

Лабораторная работа № 1 (4 часа)

Перехват и анализ сетевых пакетов.

Цель работы: Изучить возможности библиотеки WinPcap, Изучить возможности библиотеки SharpPcap; осуществить перехват и анализ сетевых пакетов на сетевом транспортном и прикладном уровнях модели OSI.

Самостоятельная работа

Тема учебной дисциплины	Вид самостоятельной работы студента (курсовой проект, курсовая работа, реферат, расчетно-графическая работа, др.)	Всего часов
Тема 1. Источники, риски и формы атак на компьютерные системы.	Изучение дополнительного теоретического материала	2
	Подготовка к сеансу тестирования	3
	Оформление и подготовка к защите лабораторной работы	3
	Подготовка к лекции (3 лекции)	1
	ИТОГО:	9

Текущий контроль – устные опросы по материалам лекции 1 и самостоятельно изученным разделам, тестирование по теме 1.

Тестирование

Цель тестирования - проверка знаний, полученных при изучении общих вопросов компьютерной безопасности.

Коды формируемых компетенций: ОПК-2, ОПК-5, ПК-3,ПК-4

Результаты освоения

ОПК-2: владеть терминологией в области защиты информации.

ОПК-5: знать актуальность и важность проблемы информационной безопасности, знать угрозы информационной безопасности и классификацию каналов несанкционированного доступа к информации, определять и анализировать угрозы безопасности информации в зависимости от среды эксплуатации продуктов информационных технологий.

ПК-3: знать цели, задачи, принципы и основные направления обеспечения информационной безопасности, уметь принимать адекватные решения при выборе средств защиты информации на основе анализа угроз.

ПК-4: владеть навыками дискуссии по профессиональной тематике.

Тема 2. Модели безопасности информационных систем

Лекция 4 (2 часа)

Виды политик безопасности. Дискреционные модели. Мандатные модели. Модель ролевого доступа. Модели мандатного разграничения доступа (модель Белла-ЛаПадула, модель Биба, мандатная модель защиты от угроз отказа в обслуживании).

Лекция 5 (2 часа)

Математические модели информационной безопасности. Модели на основе дискретных компонент (Харрисона-Руззо-Ульмана, модель распространения прав доступа Take-Grant). Базовая модель ролевого разграничения доступа.

Самостоятельная работа

Тема учебной дисциплины	Вид самостоятельной работы студента (курсовой проект, курсовая работа, реферат, расчетно-графическая работа, др.)	Всего часов
Тема 2. Модели безопасности информационных систем	Изучение дополнительного теоретического материала	2
	Подготовка к контрольной работе	2
	Подготовка к лекции (2 лекции)	1
	ИТОГО:	5

Текущий контроль – устные опросы по материалам лекции 2 и самостоятельно изученным разделам, контрольная работа.

Контрольная работа

Цель контрольной работы – определение соответствия некоторой вычислительной системы принятой математической модели информационной безопасности. Студентам предлагается вариант вычислительной системы и математическая модель. Требуется определить, нарушают ли действия пользователя правила предложенной модели информационной безопасности.

Коды формируемых компетенций: ОПК-2, ОПК-4,

Результаты освоения

ОПК-2: анализировать информационную инфраструктуру, пользоваться современной научно-технической информацией по исследуемым проблемам и задачам.

ОПК-4: знать современные подходы к построению систем защиты информации.

Тема 3. Стандарты безопасности. Законодательные меры защиты информации

Лекция 6 (2 часа)

Роль стандартов информационной безопасности. Международные стандарты информационной безопасности (Стандарты ISO/IEC 17799:2002, Международный стандарт ISO 15408 «Общие критерии безопасности информационных систем», Стандарты для беспроводных сетей, Стандарты информационной безопасности в Internet). Отечественные стандарты безопасности информационных технологий (материалы Гостехкомиссии РФ, ГОСТ Р ИСО/МЭК 15408-1, ГОСТ Р ИСО/МЭК 15408-2, ГОСТ Р ИСО/МЭК 15408-3).

Самостоятельная работа

Тема учебной дисциплины	Вид самостоятельной работы студента (курсовой проект, курсовая работа, реферат, расчетно-графическая работа, др.)	Всего часов
Тема 3. Стандарты безопасности. Законодательные меры защиты информации	Изучение дополнительного теоретического материала	2
	Подготовка к контрольной работе	2
	Подготовка к лекции	2
	ИТОГО:	6

Текущий контроль – устные опросы по материалам лекции 3 и самостоятельно изученным разделам, контрольная работа.

Контрольная работа

Цель контрольной работы – закрепление знаний по законодательным мерам информационной безопасности (знания материалов Гостехкомиссии России и ГОСТ Р ИСО/МЭК 15408-Х)

Коды формируемых компетенций: ОПК-1, ОПК-2, ОПК-5.

Результаты освоения

ОПК-1: знает основные положения законодательства в области современного авторского права и защиты информации, основные методы защиты конфиденциальной компьютерной информации.

ОПК-2: знает эволюцию, тенденцию и перспективы развития методов и средств защиты компьютерной информации. Знает основные положения законодательства в области современного авторского права и защиты информации.

ОПК-5: знает основные понятия, используемые в сфере защиты информации

Тема 4. Криптографические модели и методы защиты информации

Лекция 7 (2 часа)

Классическая криптография. Математика криптографии (модульная арифметика, матрицы, вычисления в полях Галуа). Симметричные криптосистемы. Стандарт шифрования DES. Усовершенствованный стандарт шифрования AES. Отечественный стандарт шифрования

ГОСТ 28147-89. режимы работы ГОСТ 28147-89 – простой замены, гаммирования, гаммирования с обратной связью и генерации имитовставки. Криптостойкость шифра ГОСТ 28147-89.

Лекция 8 (2 часа)

Асимметричные криптосистемы. Математика криптографии (простые числа, определение простоты числа, однонаправленные функции, разложение на множители, квадратичное сравнение, возведение в степень и логарифмы). Криптосистема RSA. Криптосистема Эль-Гамаля. Криптосистемы на основе эллиптических кривых.

Лекция 9 (2 часа)

Хэширование информации и электронная цифровая подпись. Проблема аутентификации данных. Однонаправленные хэш-функции, Алгоритм безопасного хэширования SHA, Отечественный стандарт хэш-функции ГОСТ Р 34.11-2012. Алгоритм электронной цифровой подписи RSA. Алгоритм цифровой подписи DSA. Отечественный стандарт цифровой подписи ГОСТ Р 34.10-2012.

Лекция 10 (2 часа)

Безопасное распределение ключей. Алгоритм Диффи-Хеллмана. Технологии аутентификации – методы аутентификации, использующие пароли и PIN-коды, биометрическая аутентификация пользователя. Протоколы идентификации с нулевой передачей знаний.

Лекция 11 (2 часа)

Инфраструктура управления открытыми ключами PKI. Принципы функционирования PKI. Логическая структура и компоненты PKI.

Лабораторная работа № 2 (4 часа)

Современные симметричные криптосистемы.

Цель работы: Изучение принципов работы симметричных криптосистем, многие из которых являются национальными или ведомственными стандартами; Изучение реализаций симметричной криптографии в среде .NET Framework; Программная реализация существующих симметричных криптоалгоритмов.

Лабораторная работа № 3 (4 часа)

Современные асимметричные криптосистемы.

Цель работы: Изучение принципов работы асимметричных криптосистем; Изучение реализаций асимметричной криптографии в среде .NET Framework; Реализация существующих асимметричных криптоалгоритмов.

Лабораторная работа № 4 (4 часа)

Хэширование и электронная цифровая подпись.

Цель работы: Изучение методов формирования дайджеста сообщения (хэш-функции) и электронной цифровой подписи (ЭЦП); Изучение реализаций хэш-функций и ЭЦП в среде .NET Framework; Реализация существующих хэш-функций и алгоритмов ЭЦП.

Самостоятельная работа

Тема учебной дисциплины	Вид самостоятельной работы студента (курсовой проект, курсовая работа, реферат, расчетно-графическая работа, др.)	Всего часов
Тема 4. Криптографические модели и методы защиты информации	Оформление и подготовка к защите лабораторных работ (3 лабораторные работы)	9
	Изучение дополнительного теоретического материала	2
	Подготовка к лекции (5 лекций)	4
	Подготовка к сеансу тестирования	4
	ИТОГО:	19

Текущий контроль – устные опросы по материалам лекций 4, 5, 6, 7 и самостоятельно изученным разделам, тестирование.

Тестирование

Тестирование проводится по материалам лекций 4, 5, 6, 7 и самостоятельно изученным разделам. Является итоговым по теме «Криптографические модели и методы защиты информации». В ходе проведения тестирования проверяются знания студентов в области симметричной и асимметричной криптографии, хэширования, формирования электронной - цифровой подписи, идентификации и аутентификации пользователей, безопасного распределения ключей и инфраструктуры открытых ключей PKI.

Коды формируемых компетенций: ПК-3, ОПК-5, ОПК-1.

Результаты освоения

ОПК-1: умеет анализировать информацию на предмет сокрытия в ней данных.

ОПК-5: умеет выбирать оптимальные методы защиты конфиденциальной информации.

ПК-3: умеет разрабатывать модели компонентов систем защиты информации, использовать современные программные средства для шифрования и сокрытия информации. Умеет применять полученные знания при выполнении курсовых проектов и выпускных квалификационных работ, а также в ходе научных исследований.

ПК-5: умеет выбирать оптимальные методы защиты конфиденциальной информации

ПК-9: умеет анализировать информацию на предмет сокрытия в ней данных

ПК-11: умеет устанавливать и настраивать системы защиты информации

Тема 5. Защита информации в современных операционных системах

Лекция 12 (2 часа)

Проблема обеспечения безопасности операционных систем (ОС). Угрозы безопасности ОС. Понятие защищенной ОС. Архитектура подсистемы защиты ОС (основные функции подсистемы защиты ОС, идентификация, аутентификация и авторизация, разграничение доступа к объектам ОС, аудит).

Лекция 13 (2 часа)

Защита информации в ОС Windows. Защита информации в ОС Linux. Система Kerberos.

Лабораторная работа № 5 (4 часа)

Изучение методов работы с системными журналами. Отслеживание событий записи в системные журналы. Перехват системных событий. Анализ записей системных журналов.

Лабораторная работа № 6 (4 часа)

Отслеживание событий изменения файловой системы (создание, удаление, переименование и изменение выбранных файлов и папок). Отслеживание событий изменения аппаратной конфигурации компьютера.

Лабораторная работа № 7 (4 часа)

Удаленный доступ к ресурсам операционной системы с использованием технологии WMI. Знакомство с утилитой командной строки wmic.

Лабораторная работа № 8 (4 часа)

Исследование методов контроля доступа к ресурсам операционной системы. Обеспечение безопасности доступа кода (утверждение и отклонение полномочий). Управление политиками безопасности.

Самостоятельная работа

Тема учебной дисциплины	Вид самостоятельной работы студента (курсовой проект, курсовая работа, реферат, расчетно-графическая работа, др.)	Всего часов
Тема 5. Защита информации в современных операционных системах	Изучение дополнительного теоретического материала	2
	Подготовка к контрольной работе	2
	Оформление и подготовка к защите лабораторной работы (4 лабораторные работы)	12
	Подготовка к лекции (2 лекции)	2
	ИТОГО:	18

Текущий контроль – устные опросы по материалам лекции 8 и самостоятельно изученным разделам, контрольная работа.

Контрольная работа

При подготовке к контрольной работе студенты должны повторить лекционный материал по защите операционных систем. Особое внимание в контрольной работе уделяется вопросам защиты конкретных операционных систем (Windows и Linux).

Коды формируемых компетенций: ОПК-1, ОПК-2, ОПК-4

Результаты освоения

ОПК-1: умеет устанавливать и настраивать системы защиты информации

ОПК-2: умеет выбирать и анализировать показатели качества систем и отдельных методов и средств защиты информации.

ОПК-4: умеет выбирать оптимальные методы защиты конфиденциальной информации в соответствии с особенностями конкретной ОС, осуществлять поиск и анализировать научно-техническую литературу и выбирать необходимые материалы.

Тема 6. Защита информации в сети

Лекция 14 (2 часа)

IPSec. Защита информации на транспортном уровне семиуровневой модели ISO/OSI. Режимы работы протокола IPSec (транспортный и туннельный). Протоколы безопасности IPSec – заголовок аутентификации (AH)и режим инкапсуляции полезной нагрузки (ESP). Стратегия безопасности протокола IPSec. Обмен ключами по протоколу IPSec (протокол интернет - обмена ключамиIKE).

Лекция 15 (2часа)

Протокол SSL/TLS. Защита информации на прикладном уровне семиуровневой модели ISO/OSI. SSL-архитектура. Форматы сообщений SSL.

Лекция 16 (2 часа)

Протокол SMIME и система PGP.

Лекция 17 (2 часа)

Межсетевые экраны (МЭ). Функции межсетевых экранов. Особенности функционирования МЭ на различных уровнях модели OSI. Схемы сетевой защиты на базе МЭ.

Лекция 18 (2 часа)

Система отслеживания вторжений (IDS). Технология анализа защищенности. Технологии обнаружения атак. Классификация систем IDS. Архитектура IDS. Аудит и мониторинг безопасности

Лабораторная работа № 9 (4 часа)

Безопасное распределение ключей. Алгоритм Диффи-Хеллмана.

Самостоятельная работа

Тема учебной дисциплины	Вид самостоятельной работы студента (курсовой проект, курсовая работа, реферат, расчетно-графическая работа, др.)	Всего часов
Тема 6. Защита информации в сети	Оформление и подготовка к защите лабораторной работы	3
	Подготовка к контрольной работе	2
	Подготовка к лекции (5 лекций)	4
	Подготовка к тестированию	4
	Изучение дополнительного теоретического материала	2
	ИТОГО:	15

Текущий контроль – устные опросы по материалам лекций 9, 10 и самостоятельно изученным разделам, контрольная работа.

Контрольная работа

При подготовке к контрольной работе студенты повторяют лекционный материал по следующим темам: протокол IPSec, протокол Kerberos, протокол PGP, протокол S/MIME, протокол SSL/TLS, метод шифрования электронной почты base64, метод шифрования электронной почты quoted printable, система отслеживания вторжений.

Коды формируемых компетенций: ОПК-1, ОПК-2, ОПК-4, ОПК-5, ПК-3

Результаты освоения

ОПК-1: владеет навыками создания защищенной среды с помощью аппаратно-программных средств защиты.

ПК-3: владеет навыками разработки защищенных приложений и навыками самостоятельного проектирования систем защиты информации.

ОПК-5: разрабатывать и создавать типовые схемы защиты информации на основе современных средств обеспечения информационной безопасности

ОПК-4: способен участвовать в настройке и наладке систем защиты вычислительных комплексов и автоматизированных систем в сети, умеет сопрягать аппаратные и программные средства в составе информационных и автоматизированных систем

ОПК-1: умеет устанавливать и настраивать системы защиты информации в сети, выполнять аудит и мониторинг безопасности

Промежуточная аттестация по дисциплине: экзамен.

Изучение дисциплины заканчивается экзаменом. Экзамен проводится в соответствии с Положением о зачетной и экзаменационной сессиях в НИУ МЭИ и инструктивным письмом от 14.05.2012 г. № 21-23.

5 Самостоятельная работа студента

Для обеспечения самостоятельной работы разработаны:

1. Конспект лекций по дисциплине (см. приложение З.РПД Б1.В.ОД.10 (лк));
2. Методические указания к выполнению лабораторных работ (см. приложение З.РПД Б1.В.ОД.10 (лб));
3. Методические указания к самостоятельной работе студентов (см. приложение З.РПД Б1.В.ОД.10 (срс)).

6 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

6.1 Перечень компетенций с указанием этапов их формирования

При освоении дисциплины формируются следующие компетенции:

- общепрофессиональные ОПК-1, ОПК-2, ОПК-4, ОПК-5;
- профессиональные ПК-3.

Указанные компетенции формируются в соответствии со следующими этапами:

1. Формирование и развитие теоретических знаний, предусмотренных указанными компетенциями (лекционные занятия, самостоятельная работа студентов).
2. Приобретение и развитие практических умений, предусмотренных компетенциями (практические занятия, лабораторные работы, выполнение расчетно-графической работы, самостоятельная работа студентов).
3. Закрепление теоретических знаний, умений и практических навыков, предусмотренных компетенциями, в ходе защит лабораторных работ, выполнения расчетно-графической работы, а также решения конкретных технических задач на практических занятиях, успешной сдачи экзамена.

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

Формы текущего контроля по темам дисциплины

№№пп	Наименование темы дисциплины	Формы текущего контроля
1.	Тема 1	Тест
2.	Тема 2	Контрольная работа
3.	Тема 3	Контрольная работа
4.	Тема 4	Тест
5.	Тема 5	Контрольная работа
6	Тема 6	Контрольная работа, Тест

Виды контроля самостоятельной работы студентов и оценочные средства

№ п/п	№ семестра	Тема учебной дисциплины	Виды контроля	Оценочные средства
1	7	Тема 2, 3, 5, 6	Контрольная работа	«3»- Пороговый уровень освоения компетенции «4»- Продвинутый уровень освоения компетенции «5»- Высокий уровень освоения компетенции
2	7	Тема 1, 4, 6	Тест	«50%»Пороговый уровень освоения компетенции «70%»- Продвинутый уровень освоения компетенции «90%»- Высокий уровень освоения компетенции

Образовательные технологии, обеспечивающие результаты освоения дисциплины в форме компетенций

Код компетенции	Компонентный состав компетенции (дескрипторы)	Технологии формирования	Средства оценки
ОПК-1	Знать: основные положения законодательства в области современного авторского права и защиты информации	лекции,	Тест
	Уметь: разрабатывать модели компонентов систем защиты информации	Домашнее задание	Тест
	Владеть: терминологией в области защиты информации. Владеть методами инсталляции программного и аппаратного обеспечения для информационных и автоматизированных систем защиты	Домашнее задание	Тест
ОПК-2	Знать: основные методы защиты конфиденциальной компьютерной информации	лекции,	Опрос, контрольные работы
	Уметь: разрабатывать защищенные приложения, организовывать защиту вычислительных комплексов и автоматизированных систем	Домашнее задание	Опрос, Контрольная работа

	Владеть: навыками дискуссии по профессиональной тематике. Владеть технологиями разработки и внедрения средств защиты	Домашнее задание	Опрос, Контрольная работа
ОПК-4	Знать: основные понятия, используемые в сфере защиты информации, основные виды угроз сохранности информации и методы борьбы с ними. Знать основные модели обеспечения компьютерной безопасности	лекции, лабораторные занятия	Опрос, контрольные работы
	Уметь: организовывать систему защиты информации в глобальных компьютерных сетях. Уметь разрабатывать модели систем защиты информации вычислительных комплексов и автоматизированных систем	лабораторные занятия	Опрос
	Владеть: методами защиты вычислительных комплексов и автоматизированных систем в глобальных сетях	лабораторные занятия	Опрос
ОПК-5	Знать: технологии разработки бизнес-планов и технических заданий на оснащение отделов, лабораторий и офисов средствами защиты информации	лекции,	Тест
	Уметь: разрабатывать модели систем защиты информации. Уметь выбирать оптимальные методы защиты конфиденциальной информации в сети и на отдельном компьютере соответствии с особенностями конкретной ОС	Домашнее задание	Тест
	Владеть: технологиями администрирования и защиты сетевых приложений. Владеть программными технологиями, используемыми для создания защищенных приложений. Владеть практикой создания защищенных приложений	Домашнее задание	Тест
ПК-3	Знать: современные программные средства разработки систем защиты, защищенных приложений, методов аудита безопасности и отслеживания вторжений. Знать основные инструментальные средства и программные технологии, используемые для защиты информации в сети и на отдельном компьютере	лекции, лабораторные занятия	Опрос, контрольные работы,
	Уметь: использовать современные программные средства для шифрования и сокрытия информации, для защиты операционных систем, для защиты информации в сети	лабораторные занятия	Опрос, контрольные работы
	Владеть: практикой создания защищенных приложений, систем защиты, систем отражения атак	лабораторные занятия	Опрос, контрольные работы, тест

Оценка уровней сформированности компетенций в результате освоения учебной дисциплины

Коды компетенций	Уровни сформированности компетенции	Основные признаки уровня
Общепрофессиональные компетенции - ОПК		
ОПК-1	Пороговый уровень освоения компетенции	Знает: основные положения законодательства в области современного авторского права и защиты информации
	Продвинутый уровень освоения компетенции	Дополнительно умеет: разрабатывать модели компонентов систем защиты информации
	Высокий уровень освоения компетенции	Дополнительно владеет: терминологией в области защиты информации. Владеет методами инсталляции программного и аппаратного обеспечения для информационных и автоматизированных систем защиты
ОПК-2	Пороговый уровень освоения компетенции	Знает: основные методы защиты конфиденциальной компьютерной информации
	Продвинутый уровень освоения компетенции	Дополнительно умеет: разрабатывать защищенные приложения, организовывать защиту вычислительных комплексов и автоматизированных систем
	Высокий уровень освоения компетенции	Дополнительно владеет: навыками дискуссии по профессиональной тематике, владеет технологиями разработки и внедрения средств защиты
ОПК-4	Пороговый уровень освоения компетенции	Знает: основные понятия, используемые в сфере защиты информации, основные виды угроз сохранности информации и методы борьбы с ними. Знает основные модели обеспечения компьютерной безопасности
	Продвинутый уровень освоения компетенции	Дополнительно умеет: организовывать систему защиты информации в глобальных компьютерных сетях
	Высокий уровень освоения компетенции	Дополнительно владеет: методами защиты вычислительных комплексов и автоматизированных систем в глобальных сетях
ОПК-5	Пороговый уровень освоения компетенции	Знает: технологии разработки бизнес-планов и технических заданий на оснащение отделов, лабораторий и офисов средствами защиты информации
	Продвинутый уровень освоения компетенции	Дополнительно умеет: разрабатывать модели систем защиты информации. Умеет выбирать оптимальные методы защиты конфиденциальной информации в сети и на отдельном компьютере соответствии с особенностями конкретной ОС
	Высокий уровень освоения компетенции	Дополнительно владеет: технологиями администрирования и защиты сетевых приложений. Владеет программными технологиями, используемыми для создания защищенных приложений. Владеет прак-

		тикой создания защищенных приложений
Профессиональные компетенции – ПК		
ПК-3	Пороговый уровень освоения компетенции	Знает: современные программные средства разработки систем защиты, защищенных приложений, методов аудита безопасности и отслеживания вторжений. Знает основные инструментальные средства и программные технологии, используемые для защиты информации в сети и на отдельном компьютере
	Продвинутый уровень освоения компетенции	Дополнительно умеет: использовать современные программные средства для шифрования и сокрытия информации, для защиты операционных систем, для защиты информации в сети
	Высокий уровень освоения компетенции	Дополнительно владеет: практикой создания защищенных приложений, систем защиты, систем отражения атак

6.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Вопросы к экзамену:

1. Защита информации. Основные понятия. Угрозы и меры защиты.
2. Виды атак. Сетевые атаки.
3. Виды политик информационной безопасности
4. Математические модели информационной безопасности. Модель Бела-Лападула
5. Математические модели информационной безопасности. Модель Биба
6. Математические модели информационной безопасности. Мандатная модель защиты от угроз ОВО
7. Математические модели информационной безопасности. Модель Харрисона-Руззо-Ульмана
8. Стандарты информационной безопасности. Материалы Гостехкомиссии России
9. Классификация компьютерных преступлений по кодификатору Интерпола.
10. Криптография. Основные термины и определения. Задачи криптографии.
11. Этапы развития криптографии
12. Стеганография
13. Шифрование данных. Основные термины и определения. Классификация алгоритмов шифрования.
14. Роторные машины.
15. Американский стандарт шифрования DES.
16. Режимы работы алгоритма DES
17. Российский стандарт шифрования ГОСТ 28147-89.
18. Симметричная криптосистема AES
19. Асимметричные системы шифрования. Основной принцип работы. Однонаправленные функции
20. Система шифрования RSA.
21. Хэш-функции. Основные требования и примеры построения.
22. Алгоритм хэширования SHA
23. Электронная цифровая подпись RSA.

24. Генерация ключей
25. Хранение ключей.
26. Алгоритм безопасного распределения ключей Диффи-Хэллмана
27. Сертификаты открытых ключей
28. Протокол Kerberos
29. Технологии аутентификации
30. Защита информации в сети. Семиуровневая модель OSI. Стек TCP/IP
31. Протокол IPSec. Режимы работы
32. Протокол IPSec. Стратегия безопасности
33. Защита информации в сети. Протокол SSL/TLS
34. Защита информации на прикладном уровне. Протокол PGP
35. Защита информации на прикладном уровне. Протокол S/MIME
36. Система отслеживания вторжений

Примеры контрольных работ

Контрольная работа по теме 2

1. Имеется некоторая вычислительная система, построенная в соответствии с мандатной моделью безопасности Бела –Лападулла. Пользователь, работающий в данной системе и имеющий уровень доступа «С» (СЕКРЕТНО), пытается прочитать файл, имеющий уровень секретности «К» (КОНФИДЕНЦИАЛЬНО). Возможна ли данная операция? И если не возможна, то какое правило модели Бела-Лападулла она нарушает. Если возможна, то, в соответствии с каким правилом.
2. Имеется некоторая вычислительная система, построенная в соответствии с мандатной моделью безопасности Бела –Лападулла. Пользователь, работающий в данной системе, пытается удалить в корзину какой-либо файл, имеющий уровень секретности «СС». Возможна ли данная операция? И если не возможна, то, какое правило модели Бела-Лападулла она нарушает. Если возможна, то, в соответствии с каким правилом.
3. Имеется некоторая вычислительная система, построенная в соответствии с мандатной моделью целостности Биба. Пользователь, работающий в данной системе, пытается записать в папку с уровнем целостности «С» какой-либо файл, имеющий уровень целостностии «СС». Возможна ли данная операция? И если не возможна, то, какое правило модели Биба она нарушает. Если возможна, то, в соответствии с каким правилом.
4. Имеется некоторая вычислительная система, построенная в соответствии с мандатной моделью целостности Биба. Пользователь, работающий в данной системе и имеющий уровень доступа «С» (СЕКРЕТНО), пытается прочитать (запустить на выполнение) файл, имеющий уровень целостности «К» (КОНФИДЕНЦИАЛЬНО). Возможна ли данная операция? И, если не возможна, то какое правило модели Биба она нарушает. Если возможна, то, в соответствии с каким правилом.

Контрольная работа по теме 3

1. Начиная с какого класса защищенности СВТ требуется руководство пользователя
2. Начиная с какого класса требований ГТК РФ к защите информации в автоматизированных многопользовательских системах с различным доступом требуется интерактивное оповещение администраторов системы о попытках несанкционированного доступа
3. Начиная с какого класса защищенности СВТ требуется взаимодействие пользователя с комплексом средств защиты
4. Начиная с какого класса требований ГТК РФ к защите информации в автоматизированных многопользовательских системах с различным доступом требуется учет и регистрация изменений полномочий субъектов доступа

5. Начиная с какого класса требований ГТК РФ к защите информации в автоматизированных многопользовательских системах с одинаковыми полномочиями доступа требуется очистка освобождаемых областей оперативной памяти
6. Начиная с какого класса защищенности СВТ требуется мандатный принцип контроля доступа
7. Начиная с какого класса требований ГТК РФ к защите информации в автоматизированных многопользовательских системах с различным доступом требуется шифрование конфиденциальной информации
8. Начиная с какого класса требований ГТК РФ к защите информации в автоматизированных многопользовательских системах с одинаковым доступом требуется наличие администратора (службы) защиты информации в АС
9. Начиная с какого класса защищенности СВТ требуется регистрация
10. Начиная с какого класса требований ГТК РФ к защите информации в автоматизированных многопользовательских системах с различным доступом требуется использование сертифицированных криптографических средств

Контрольная работа по теме 5

1. В ОС UNIX права доступа к некоторому файлу заданы числом 765. Какие права имеют остальные пользователи на доступ к этому файлу
2. Какая команда ОС UNIX позволяет избранным пользователям выполнять некоторые программы на правах суперпользователя, причем у обратившегося к этой команде пользователя запрашивается не пароль суперпользователя, а его собственный пароль
3. Команда su (ОС UNIX) получила свое название, как аббревиатура словосочетания
4. Каждая запись файла etc\passwd (ОС UNIX) состоит из семи полей, разделенных символом
5. Журнал безопасности ОС Windows расположен в файле
6. В ОС Windows для запуска программы от имени другой учетной записи используется команда

Контрольная работа по теме 6

1. Структура протокола IPv4
2. Структура протокола IPv6
3. Структура протокола TCP
4. Структура протокола UDP
5. Структура протокола ICMP
6. Структура протокола HTTP
7. Атаки на протокол IP
8. Атаки на протокол ICMP
9. Атаки на протокол TCP
10. Атаки на протокол HTTP
11. Атаки на протокол ARP

Примеры тестов

Тест по теме 1

1) Угроза нарушения конфиденциальности вычислительной системы (ВС) означает:
   a) Искажение информации, хранящейся в компьютерной системе или передаваемой по каналу связи
   b) Разглашение секретной информации;
   c) Создание таких ситуаций, когда определенные преднамеренные действия либо снижают работоспособность ВС, либо блокируют доступ к некоторым ее ресурсам;
   d) Информация становится известной лицам, которые не должны иметь к ней доступ.
2) Угроза нарушения целостности информации означает:

a) Искажение информации, хранящейся в компьютерной системе или передаваемой по каналу связи
b) Разглашение секретной информации;
c) Санкционированное изменение информации, которое выполняется полномочными лицами;
d) Создание таких ситуаций, когда определенные преднамеренные действия либо снижают работоспособность ВС, либо блокируют доступ к некоторым ее ресурсам.

3) Угроза нарушения работоспособности вычислительной системы (ВС) означает:
a) Разглашение конфиденциальной или секретной информации;
b) Искажение информации, хранящейся в компьютерной системе или передаваемой по каналу связи
c) Блокирование доступа к ресурсу;
d) Создание таких ситуаций, когда определенные преднамеренные действия либо снижают работоспособность ВС, либо блокируют доступ к некоторым ее ресурсам.

4) «Компьютерный вирус» - это программа, которая :
a) Может заражать другие программы, модифицируя их посредством включения в них своей, возможно, измененной копии, причем последняя сохраняет способность к дальнейшему размножению;
b) Осуществляет перехват паролей
c) Наряду с действиями, описанными в ее документации, выполняет некоторые другие действия, ведущие к нарушению безопасности системы и деструктивным результатам
d) выполняет какие-либо действия одним пользователем от имени другого пользователя, обладающего соответствующими полномочиями.

5) Причинами случайных разрушающих воздействий при работы ВС могут быть:
a) Ошибки в работе ВС;
b) Отказы и сбой аппаратуры;
c) Помехи в линиях связи из-за воздействия внешней среды
d) Результат работы компьютерного вируса или троянской программы.

6) Угрозами безопасности вычислительной системы (ВС) являются:
a) Вмешательство человека в работу ВС;
b) Аппаратно-техническое вмешательство в работу ВС
c) Администрирование ВС со стороны администратора;
d) Разрушающее воздействие на программные компоненты ВС с помощью программных средств.

7) Атака на компьютерную систему:
a) Действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости системы;
b) Оценка производительности системы;
c) Реализация угрозы безопасности;
d) Тестирование ВС;

8) К разрушающим программным средствам относятся:
a) Анализаторы протоколов;
b) Компьютерные вирусы;
c) Серверы приложений;
d) Троянские программы.

9) «Троянский конь» - это программа, которая :
a) Может заражать другие программы, модифицируя их посредством включения в них своей, возможно, измененной копии, причем последняя сохраняет способность к дальнейшему размножению;
b) Осуществляет перехват паролей

c) Наряду с действиями, описанными в ее документации, выполняет некоторые другие действия, ведущие к нарушению безопасности системы и деструктивным результатам
d) выполняет какие-либо действия одним пользователем от имени другого пользователя, обладающего соответствующими полномочиями.

10) «Маскарад» - это программа, которая :
a) Может заражать другие программы, модифицируя их посредством включения в них своей, возможно, измененной копии, причем последняя сохраняет способность к дальнейшему размножению;
b) Осуществляет перехват паролей
c) Наряду с действиями, описанными в ее документации, выполняет некоторые другие действия, ведущие к нарушению безопасности системы и деструктивным результатам
d) выполняет какие-либо действия одним пользователем от имени другого пользователя, обладающего соответствующими полномочиями.

11) Комплексный подход» в обеспечению безопасности ВС:
a) Ориентирован на создание защищенной среды обработки информации в ВС, объединяющий в единый комплекс разнородные меры противодействия угрозам;
b) Направлен на противодействие четко определенным угрозам в заданных условиях;
c) Не создает единую защищенную среду обработки информации;
d) Гарантирует определенный уровень безопасности ВС в целом.

12) Политика безопасности может быть:
a) Манчестерской;
b) Дискреционной;
c) Мандатной;
d) Паспортной.
e) Ролевой

13) В материалах Гостехкомиссия (ГТК) при Президенте Российской федерации (РФ) основное внимание уделяется вопросам:
a) Обеспечения целостности
b) Обеспечения конфиденциальности
c) Обеспечения работоспособности
d) Обеспечения аутентификации
e) Обеспечения регистрации

Тест по теме 4

Тест 4.1 Симметричная криптография

1. Фундаментальное правило криптоанализа, заключающееся в том, что стойкость шифра должна определяться только секретностью ключа, сформулировано:
   a. Режевским
   b. Керкхоффом
   c. Шамиром
   d. Шенноном

2. Какой из режимов работы алгоритма DES можно использовать для формирования электронной цифровой подписи
   a. ECB
   b. CBC
   c. CFB
   d. OFB
3. Какой из режимов работы алгоритма DES используется в телекоммуникационных системах
   a. ECB

b. CBC
c. CFB
d. OFB

4. Размер блока в DES:
5. Размер ключа в DES:
6. Размер ключа раунда в DES:
7. Покажите результат прохождения 110111 через S-блок 3:
8. Покажите результат прохождения 001100 через S-блок 4:
9. Покажите результат прохождения 000000 через S-блок 7:
10. Покажите результат прохождения 111111 через S-блок 2:
11. Найдите результат следующей операции $(01001101) \oplus (01001101)$:
12. Найдите результат следующей операции $(01001101) \oplus (10110010)$:
13. Назовите размер блока, размер ключа и число раундов для AES-128:
14. Назовите размер блока, размер ключа и число раундов для AES-192:
15. Назовите размер блока, размер ключа и число раундов для AES-256:

Тест 4.2 Асимметричная криптография

1. Какие из перечисленных функций относятся к однонаправленным:
   a. Вычисление определителя квадратной матрицы
   b. Разложение на множители большого целого числа т.е. нахождение делителей P и Q большого целого числа N = P*Q
   c. Разложение периодической функции с периодом $2*\pi$ в ряд по тригонометрическим функциям: $f(x)=a_0/2+\sum(a_k*\cos(kx)+b_k*\sin(kx))$ (Ряд Фурье)
   d. Задача дискретного логарифмирования, то есть для известных целых A, N и Y нахождение целого числа X, такого, что $A^x \bmod N = Y$
2. Хэш-функция предназначена для
   a. Аутентификации текстов, передаваемых по телекоммуникационным каналам
   b. Шифрования передаваемой информации
   c. Увеличения скорости передачи данных
   d. Сжатия подписываемого документа до нескольких десятков или сотен бит
3. Какой из перечисленных алгоритмов является алгоритмом хэширования:
   a. SHA
   b. RSA
   c. Эль-Гамаля
   d. DSA

Тест по теме 6

1) Протокол безопасности AH IPSec обеспечивает следующие виды защиты
   a) Защиту конфиденциальности данных
   b) Защиту целостности данных
   c) Защиту работоспособности
   d) Сжатие информации с паролем
   e) Скрэмблирование
2) Протокол безопасности ESP IPSec обеспечивает следующие виды защиты
   a) Защиту конфиденциальности
   b) Защиту целостности
   c) Защиту работоспособности
   d) Скрэмблирование

   e) Защиту сжатием информации с паролем
3) Какую информацию защищает протокол IPSec в транспортном режиме
   a) Заголовок протокола IP
   b) Информацию транспортного уровня
   c) Сертификат
   d) Псевдозаголовок протокола IP
   e) Дополнительную информацию, необходимую для аутентификации
4) Протокол IPSec в транспортном режиме защищает данные на участке
   a) хост - хост
   b) хост - маршрутизатор
   c) маршрутизатор - хост
   d) маршрутизатор - маршрутизатор
5) Протокол IPSec в туннельном режиме защищает данные на участке
   a) хост - хост
   b) хост - маршрутизатор
   c) маршрутизатор - хост
   d) маршрутизатор - маршрутизатор
6) Для каких целей служит поле "индекс параметров обеспечения безопасности" протокола IPSec
   a) для хранения ключей
   b) для определения режима работа протокола IPSec
   c) для идентификации виртуального канала
   d) для определения алгоритмов шифрования
7) Какой алгоритм использует протокол IPSec для передачи ключей
   a) Kerberos
   b) DES в режиме OFB
   c) RSA
   d) Диффи-Хеллмана
8) Какие из перечисленных протоколов сетевой безопасности обеспечивает предварительное сжатие передаваемой информации
   a) PGP
   b) S/MIME
   c) SSL
   d) TLS
   e) IPSec
   f) Kerberos
9) Передаваемый по электронной почте текст на русском языке имеет длину - 136 символов. текст шифруется методом base64. Определите размер текста после шифрования
   a) 138
   b) 408
   c) 184
   d) 180
   e) 211
   f) 410
10) Передаваемый по электронной почте текст на русском языке имеет длину - 200 символов. текст шифруется методом quoted printable. Определите размер текста после шифрования
   a) 400
   b) 268
   c) 600
   d) размер передаваемого текста не изменится
   e) 100

f) 350

11) Протокол IPSec обеспечивает защиту от атак на
   a) физическом уровне
   b) канальном уровне
   c) сетевом уровне
   d) транспортном уровне
   e) сеансовом уровне
   f) уровне представления
   g) прикладном уровне
12) Служба сетевой аутентификации Kerberos представляет собой
   a) Систему агент-менеджер
   b) Систему клиент-сервер
   c) Систему запрос-ответ
   d) Систему распределенных вычислений
13) В протоколе SSL для шифрования трафика используются следующие протоколы (выберите правильный ответ):
   a) FORTEZZA
   b) IDEA
   c) DES
   d) RSA
   e) AES
   f) MD5
   g) SHA-1
14) компонентами СОА являются:
   a) модуль выявления атак
   b) модуль реагирования
   c) сервер базы данных
   d) модуль сканирования сети
   e) модуль анализа сетевых журналов
   f) модули -датчики
   g) модуль хранения данных

15) Криптосистема RSA. $\varphi(N)=7$. Открытый ключ - 4. Укажите возможные значения секретного ключа
   a. 1
   b. 2
   c. 5
   d. 9
   e. 11
   f. 13
16) Концепция асимметричных криптографических систем с открытым ключом основана на применении:
   a. Рядов Фурье
   b. Расширенной теоремы Евклида
   c. Однонаправленных функций
   d. Теоремы Найквиста-Котельникова
   e. Полей Галуа
17) Какие утверждения верны для хэш-функции
   a. Длина хэш-функции не зависит от длины исходного сообщения
   b. Длина хэш-функции меняется в зависимости от длины исходного сообщения

c. хэш-функция должна быть чувствительна к всевозможным изменениям в тексте , таким как вставки, выбросы, перестановки и т.п.
d. хэш-функция должна обладать свойством необратимости, то есть задача подбора документа, который обладал бы требуемым значением хэш-функции, должна быть вычислительно неразрешима
e. для вычисления значения хэша можно использовать симметричные криптостистемы

18) Определите возможные значения открытого ключа алгоритма RSA, если P=3, Q=11
   a. 7
   b. 11
   c. 13
   d. 6
   e. 9
   f. 4
19) Криптосистема RSA. P=3, Q=11. Открытый ключ равен 7. Выберите ответ с правильными значениями N, φ(N) и секретного ключа
   a. 33, 20, 9
   b. 20, 34, 5
   c. 33, 20, 3
   d. 11, 9, 3
20) Для числа N=7*11 с помощью функции Эйлера φ(N) определите количество положительных целых чисел, меньших N и взаимно простых с N
   a. 77
   b. 60
   c. 1
   d. 5
   e. 11
   f. 7
21) В протоколе Диффи-Хеллмана G=7, P=23, x=3 и y=6. Какое значение имеет симметричный ключ
   a. 75
   b. 12
   c. 18
   d. 4
   e. 11
   f. 74
22) Для каких целей служит стандарт X509
   a. новый стандарт шифрования асимметричных криптосистем, предложенный агентством национальной безопасности соединенных штатов
   b. стандарт в области PKI
   c. стандарт шифрования данных в виртуальных частных сетях (VPN)
   d. стандарт ЭЦП США, на основе хэш-функции SHA1

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

Процедуры оценивания я знаний, умений, навыков, характеризующих этапы формирования компетенций , изложены в:

1. Конспект лекций по дисциплине (см. приложение 3.РПД Б1.В.ОД.10 (лк));

2. Методические указания к выполнению лабораторных работ (см. приложение 3.РПД Б1.В.ОД.10 (лб));
3. Методические указания к самостоятельной работе студентов (см. приложение 3.РПД Б1.В.ОД.10 (срс)).

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

Основная учебная литература

1. Бирюков, А.А. Информационная безопасность: защита и нападение. [Электронный ресурс] : учебник. — Электрон. дан. — М. : ДМК Пресс, 2012. — 474 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=39990
2. Беломойцев, Д.Е. Основные методы криптографической обработки данных: учеб. пособие [Электронный ресурс] : / Д.Е. Беломойцев, Т.М. Волосатова, С.В. Родионов. — Электрон. дан. — М. : МГТУ им. Н.Э. Баумана (Московский государственный технический университет имени Н.Э. Баумана), 2014. — 80 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=58438
3. Петров, А.А. Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс] : . — Электрон. дан. — М. : ДМК Пресс, 2008. — 451 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=3027
4. Шаньгин, В.Ф. Информационная безопасность [Электронный ресурс] : учебное пособие. — Электрон. дан. — М. : ДМК Пресс, 2014. — 702 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=50578

Дополнительная учебная литература

5. Герасимов, А.А. Защита информации от несанкционированного доступа: методические указания к выполнению лабораторной работы по курсу «Аттестация объектов информатизации» [Электронный ресурс] : учебно-методическое пособие / А.А. Герасимов, А.В. Мозговой. — Электрон. дан. — М. : МГТУ им. Н.Э. Баумана (Московский государственный технический университет имени Н.Э. Баумана), 2012. — 28 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=62003
6. Дипломное проектирование по спец. Комплексное обеспечение информационной безопасности автоматизированных систем [Электронный ресурс] : . — Электрон. дан. — М. : МГТУ им. Н.Э. Баумана (Московский государственный технический университет имени Н.Э. Баумана), 2011. — 80 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=52421
7. Ховард М. 19 смертных грехов, угрожающих безопасности программ. Как не допустить типичных ошибок [Электронный ресурс] : учебное пособие / Ховард М., Лебланк Д., Виега Д. — Электрон. дан. — М. : ДМК Пресс, 2009. — 288 с. — Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=1118

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

1. http://base.consultant.ru - Гостехкомиссия России. Руководящий документ. Концепция защиты средств вычислительной техники от несанкционированного доступа к информации, Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации, Руководящий документ. Автоматизированные системы. Защита от несанкционированного

доступа к информации. Классификация автоматизированных систем и требования по защите информации.

2. http://gostexpert.ru - Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.
3. http://standartgost.ru/g/ГОСТ_Р_34.10-2012 - Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи
4. http://standartgost.ru/g/ГОСТ_Р_34.11-2012 - Информационная технология. Криптографическая защита информации. Функция хэширования.
5. http://docs.cntd.ru/document/gost-28147-89 - Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

9. Методические указания для обучающихся по освоению дисциплины

Дисциплина предусматривает лекции раз в неделю, и лабораторные работы раз в две недели. Изучение курса завершается экзаменом.

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

Во время **лекции** студент должен вести краткий конспект.

Работа с конспектом лекций предполагает просмотр конспекта в тот же день после занятий. При этом необходимо пометить материалы конспекта, которые вызывают затруднения для понимания. При этом обучающийся должен стараться найти ответы на затруднительные вопросы, используя рекомендуемую литературу. Если ему самостоятельно не удалось разобраться в материале, необходимо сформулировать вопросы и обратится за помощью к преподавателю на консультации или на ближайшей лекции.

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

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

Выполнение студентами лабораторных работ направлено на:

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

формирование необходимых профессиональных умений и навыков;

Содержание лабораторных работ фиксируется в РПД в разделе 4 настоящей программы.

При планировании лабораторных работ следует учитывать, что наряду с ведущей целью - подтверждением теоретических положений - в ходе выполнения заданий у студентов формируются практические умения и навыки обращения с лабораторным оборудованием, аппаратурой и пр., которые могут составлять часть профессиональной практической подготовки, а также исследовательские умения (наблюдать, сравнивать, анализировать, устанавливать зависимости, делать выводы и обобщения, самостоятельно вести исследование, оформлять результаты).

Состав заданий для лабораторной работы +спланирован с таким расчетом, чтобы за отведенное время они могли быть качественно выполнены большинством студентов.

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

Помимо собственно выполнения работы для каждой лабораторной работы предусмотрена процедура защиты, в ходе которой преподаватель проводит устный или письменный опрос студентов для контроля понимания выполненных ими измерений, правильной интерпретации полу-

ченных результатов и усвоения ими основных теоретических и практических знаний по теме занятия.

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

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

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

При проведении **лабораторных работ** предусматривается использование персональных компьютеров, оснащенных необходимым комплектом лицензионного программного обеспечения. – Viusual Studio 2010 по подписке Dream Spark.

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

Лекционные занятия:
Аудитория.

Лабораторные работы по данной дисциплине проводятся в компьютерных классах, оснащенных необходимым комплектом программного обеспечения.

Автор
канд. техн. наук, доцент — Е.А. Панкратова

Зав. кафедрой ВТ
д-р техн. наук, профессор — А.С. Федулов

Программа одобрена на заседании кафедры 31 августа 2016 года, протокол № 01.