Приложение З.РПД Б3.Б.8

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

УТВЕРЖДАЮ
Зам. директора
филиала ФГБОУ ВО «НИУ «МЭИ»
в г. Смоленске
по учебно-методической работе
_____ В.В. Рожков
«31» 08 2015 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ЗАЩИТА ИНФОРМАЦИИ

(НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ)

Направление подготовки: 09.03.01 Информатика и вычислительная техника

Профиль подготовки: Автоматизированные системы обработки информации и управления

Уровень высшего образования: бакалавриат

Нормативный срок обучения: 4 года

Форма обучения: очная

Смоленск – 2015 г.

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

Целью дисциплины «Защита информации» является изучение основных направлений защиты компьютерной информации; изучение организационных и административных методов защиты информации; изучение программно-аппаратных средств защиты компьютерных систем; обзор готовых решений по обеспечению информационной безопасности, разработка программных средств аудита безопасности, выявления вторжений и программных средств криптографической защиты информации.

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 общекультурных и профессиональных компетенций:

- ОК-11: осознает сущность и значение информации в развитии современного общества; владеет основными методами, способами и средствами получения, хранения, переработки информации;
- ОК-12: имеет навыки работы с компьютером как средством управления информацией;
- ОК-13: способен работать с информацией в глобальных компьютерных сетях;
- ПК-1: проектно-конструкторская деятельность: умеет разрабатывать бизнес-планы и технические задания на оснащение отделов, лабораторий, офисов компьютерным и сетевым оборудованием;
- ПК-2: способен осваивать методики использования программных средств для решения практических задач
- ПК5: проектно-технологическая деятельность: умеет разрабатывать компоненты программных комплексов и баз данных, использовать современные инструментальные средства и технологии программирования
- ПК-9: монтажно-наладочная деятельность: способен участвовать в настройке и наладке программно-аппаратных комплексов.
- ПК-10: умеет сопрягать аппаратные и программные средства в составе информационных и автоматизированных систем;
- ПК-11: сервисно-эксплуатационная деятельность: умеет инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем

В результате освоения дисциплины обучающийся должен знать:

- актуальность и важность проблемы информационной безопасности(ОК-11)
- цели, задачи, принципы и основные направления обеспечения информационной безопасности (ОК-11, ПК-2, ПК-5);
- знать основные положения законодательства в области современного авторского права и защиты информации (ОК-11);
- эволюцию, тенденцию и перспективы развития методов и средств защиты компьютерной информации (ОК-11);
- основные методы защиты конфиденциальной компьютерной информации (ОК-12, ПК-2, ПК-9,ПК-10);

- основные понятия, используемые в сфере защиты информации (ОК-13);
- угрозы информационной безопасности и классификацию каналов несанкционированного доступа к информации (ОК-13);
- современные подходы к построению систем защиты информации (ПК-1, ПК-2, ПК-9, ПК-11);

В результате освоения дисциплины обучающийся должен уметь:

- анализировать информационную инфраструктуру (ОК-11);
- пользоваться современной научно-технической информацией по исследуемым проблемам и задачам (ОК-11);
- принимать адекватные решения при выборе средств защиты информации на основе анализа угроз (ОК-12, ПК-2);
- выбирать и анализировать показатели качества систем и отдельных методов и средств защиты информации (ОК-13);
- осуществлять поиск и анализировать научно-техническую литературу и выбирать необходимые материалы (ОК-11);
- определять и анализировать угрозы безопасности информации в зависимости от среды эксплуатации продуктов информационных технологий (ОК-13);
- разрабатывать модели компонентов систем защиты информации (ПК-1)
- использовать современные программные средства для шифрования и сокрытия информации (ПК-2)
- выбирать оптимальные методы защиты конфиденциальной информации (ПК-5).
- применять полученные знания при выполнении курсовых проектов и выпускных квалификационных работ, а также в ходе научных исследований(ПК-5)
- анализировать информацию на предмет сокрытия в ней данных (ПК-9);
- разрабатывать и создавать типовые схемы защиты информации на основе современных средств обеспечения информационной безопасности (ПК-10, ПК-11);

В результате освоения дисциплины обучающийся должен владеть:

- навыками дискуссии по профессиональной тематике (ОК-12);
- терминологией в области защиты информации (ОК-11).
- навыками создания защищенной среды с помощью аппаратно-программных средств защиты (ОК-13, ПК-2, ПК-10) ;
- навыками разработки защищенных приложений (ПК-9, ПК-11)
- навыками самостоятельного проектирования систем защиты информации(ПК-1, ПК-5)

2 Место дисциплины в структуре ООП ВПО направления 09.03.01 бакалавр техники и технологий по направлению «Информатика и вычислительная техника»

Дисциплина «Защита информации» относится к базовой части профессионального цикла Б.3.Б.8 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:

- Б3.Б.5 Сети и телекоммуникации
- Б3.Б.7 Базы данных
- Б3.В.ОД.3 Основы теории управления

- Б3.В.ОД.4 Микропроцессорные системы
- Б3.В.ОД.8 Теория передачи информации
- Б3.В.ДВ.5.1 Информационные технологии
- Б2.Б.1 Математика
- Б2.Б.2 Физика
- Б2.Б.3 Информатика
- Б2.В.ОД.4 Теория вероятностей и математическая статистика
- Б2.В.ОД.5 Прикладная статистика
- Б2.В.ДВ.1.1 Теория принятия решений
- Б3.Б.1 Электротехника, электроника и схемотехника
- Б3.Б.3 Операционные системы
- Б3.Б.4 Инженерная и компьютерная графика
- Б3.Б.9 ЭВМ и периферийные устройства
- Б3.Б.10 Метрология, стандартизация и сертификация
- Б3.В.ОД.1 Компьютерная графика
- Б3.В.ОД.5 Системное программное обеспечение
- Б3.В.ОД.6 Технология программирования
- Б3.В.ОД.7 Электронные цепи ЭВМ
- Б3.В.ОД.9 Проектирование АСОИУ
- Б3.В.ДВ.1.1 Теоретические основы автоматизированного управления
- Б3.В.ДВ.2.1 Аппаратные и программные средства АСОИУ
- Б3.В.ДВ.3.1 Сетевые технологии
- Б3.В.ДВ.6.1 Надежность, эргономика и качество АСОИУ
- Б3.В.ДВ.7.1 Учебный практикум по моделированию систем
- Б1.Б.4 Экономика
- Б2.Б.4 Экология
- Б2.В.ОД.1 Математическая логика и теория алгоритмов
- Б2.В.ОД.2 Дискретная математика
- Б2.В.ДВ.2.1 Введение в оптимизацию
- Б3.Б.2 Программирование
- Б2.Б.4 Экология
- Б5.У.1 Учебная практика
- Б5.П.1 Производственная практика

.

Знания, полученные по освоению дисциплины «Защита информации», необходимы при выполнении бакалаврской выпускной квалификационной работы и изучении дисциплин направления магистерской подготовки «Информатика и вычислительная техника», связанных с разработкой программного обеспечения.

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 4 зачетных единицы, 144 часа.
Объем занятий, проводимых в интерактивной форме, 10 часов

Аудиторная работа

Цикл:	Б3 Профессиональный цикл	Семестр
Часть цикла:	Базовая	
Индекс дисциплины по учебному плану	Б3.Б8	
Часов всего по учебному плану	144	8 семестр
Трудоемкость в зачетных единицах (ЗЕТ)	4	8 семестр
Лекции (ЗЕТ/ часов)	0,55/20	8 семестр
Практические занятия (ЗЕТ/ часов)	0,55/20	8 семестр
Объем самостоятельной работы по учебному плану (ЗЕТ/ часов всего)	1,89/68	8 семестр
Зачет с оценкой (в объеме самостоятельной работы)	-	8 семестр
Экзамен	1/36	8 семестр

Самостоятельная работа студента

Вид работ	Трудоёмкость	
	ЗЕТ	*час*
Подготовка к лекции	0,22	8
Изучение дополнительного теоретического материала	0,67	24
Подготовка к сеансу тестирования	0,22	8
Подготовка к контрольной работе	0,22	8
Подготовка к выполнению и защите лабораторных работ (лаб)	0,56	20
Всего:	**1,89**	**68**

Распределение трудоемкости дисциплины по семестрам и видам учебной работы

№ п/п	Разделы и темы дисциплины	Семестр	Неделя семестра	Общая трудоемкость, всего	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)									Занятия в интерактивной форме	Формы текущего контроля успеваемости *(по каждой теме)* Форма промежуточной аттестации *(по семестрам: зачет с оценкой, экзамен)*
					Аудиторные занятия				Экзамен	Самостоятельная работа					
					Всего	Лекции	Практические занятия	Лабораторные работы		Всего	Реферат, РГР	Курсовая работа/проект	Другая		
1	Источники, риски и формы атак на компьютерные системы.	8	1	14	2	2			2	10			10		Тест, Изучен.доп.материала, Подготовка к лекц.
2	Модели безопасности информационных	8	2	14	2	2			4	8			8		Контр. Работа, Изучен.доп.матер

	систем														иала, Подготовка к лекц.
3	Стандарты безопасности. Законодательные меры защиты информации	8	3	14	2	2			4	8			8		Контр. Работа, Изучен.доп.материала, Подготовка к лекц.
4	Криптографические модели и методы защиты информации	8	4	56	20	8		12	16	20			20	5	Тест, Изучен.доп.материала,
5	Защита информации в современных операционных системах	8	15	22	6	2		4	4	12			12	3	Контр. Работа, Изучение доп. Материала, подгот к лекц.
6	Защита информации в сети	8	16	24	8	4		4	6	10			10	2	Контр. Работа, Изучение доп. материала
Всего		**часов**		**144**	**40**	**20**		**20**	**36**	**68**			**68**	**10**	
		ЗЕТ		4	1,2	0,6		0,6	1	1,8			1,8	0,3	

Матрица соотнесения тем/разделов дисциплины и формируемых в них общекультурных и профессиональных компетенций

Темы, разделы дисциплины	**Количество часов**	**Код компетенции**											
		ОК-11	**ОК-12**	**ОК-13**	**ПК-1**	**ПК-2**	**ПК-5**	**ПК-9**	**ПК-10**	**ПК-11**	**…**	**…**	**Σ общее количество компетенций**
Тема 1	**14**	***X***			***X***								***2***
Тема 2	**14**				***X***								***1***
Тема 3	**14**	***X***	***X***										***2***
Тема 4	**56**					***X***	***X***	***X***		***X***			***4***
Тема 5	**22**					***X***	***X***	***X***		***X***			***4***
Тема 6	**24**			***X***		***X***	***X***	***X***	***X***	***X***			***6***
Итого	**144**	***2***	***1***	***1***	***2***	***3***	***3***	***3***	***1***	***3***			***19***

4 Содержание дисциплины, структурированное по темам

№№ пп	Наименование раздела, темы дисциплины	Содержание	Коды формируемых компетенций	Результаты освоения
1	Тема 1. Источники, риски и формы атак на компьютерные системы	Функции и задачи защиты информации. Методы и системы защиты информации. Основные виды угроз безопасности. Классификация атак на вычислительные системы. Сетевые атаки. Компьютерные вирусы и антивирусные программы. Кодификатор компьютерных преступлений интерпола	ОК-11, ПК-1	ОК-11: осознает сущность и значение информации в развитии современного общества; владеет основными методами, способами и средствами получения, хранения, переработки информации. Владеет терминологией в области защиты информации ПК-1: умеет разрабатывать бизнес-планы и технические задания на оснащение отделов, лабораторий, офисов средствами защиты информации
2	Тема 2. Модели безопасности информационных систем	Виды политик безопасности. Дискреционные модели. Мандатные модели. Модель ролевого доступа	ПК-1	ПК-1: умеет выбирать оптимальные методы защиты конфиденциальной информации, разрабатывать систему защиты вычислительных комплексов
3	Тема 3. Стандарты безопасности. Законодательные меры защиты информации	Материалы Гостехкомиссии РФ. Единые критерии безопасности информационных технологий	ОК-11, ОК-12	ОК-11: знает основные положения законодательства в области современного авторского права и защиты информации ОК-12: знает основные методы защиты конфиденциальной компьютерной информации

4	Тема 4. Криптографические модели и методы защиты информации	Классическая криптография. Симметричные криптосистемы. Асимметричные криптосистемы. Хэширование информации и электронная цифровая подпись. Безопасное распределение ключей. Инфраструктура управления открытыми ключами.	ПК-2, ПК-5, ПК-9, ПК-11	ПК-2: умеет использовать современные программные средства для шифрования и сокрытия информации 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
5	Тема 5. Защита информации в современных операционных системах	Защита информации в ОС Windows. Защита информации в ОС Linux. Система Kerberos.	ПК-2, ПК-5, ПК-9, ПК-11	ПК-2: умеет использовать современные программные средства для защиты информации ПК-5: умеет выбирать оптимальные методы защиты конфиденциальной информации в соответствии с особенностями конкретной ОС ПК-9: способен участвовать в настройке и наладке систем защиты вычислительных комплексов и автоматизированных систем ПК-11: умеет устанавливать и настраивать системы защиты информации

6	Тема 6. Защита информации в сети	IPSec. Защита информации на транспортном уровне семиуровневой модели ISO/OSI. Протокол SSL/TLS. Защита информации на прикладном уровне семиуровневой модели ISO/OSI. Протокол SMIME и система PGP. Межсетевые экраны. Система отслеживания вторжений Аудит и мониторинг безопасности	ОК-13, ПК-2, ПК-5, ПК-9, ПК-10, ПК-11	ОК-13: способен организовывать систему защиты информации в глобальных компьютерных сетях ПК-2: умеет использовать современные программные средства для защиты информации в сети ПК-5: умеет выбирать оптимальные методы защиты конфиденциальной информации в вычислительной сети ПК-9: способен участвовать в настройке и наладке систем защиты вычислительных комплексов и автоматизированных систем в сети ПК-10: умеет сопрягать аппаратные и программные средства в составе информационных и автоматизированных систем ПК-11: умеет устанавливать и настраивать системы защиты информации в сети, выполнять аудит и мониторинг безопасности

Лекционные занятия (в количестве 20 часов) проводятся в интерактивной форме (используются технологии типа «лекция-провокация», т.е. в процессе лекции делается преднамеренная ошибка с последующим опросом студентов на следующей лекции и организацией диалога «преподаватель-студент», «студент-студент» с целью выявления ошибки и установления истины

Лабораторные работы

№ семестра	Раздел учебной дисциплины	Наименование практических занятий	Трудоемкость, часы
8	Тема 4. Криптографические модели и методы защиты информации	Лабораторная работа № 1. Современные симметричные криптосистемы	4
		Лабораторная работа № 2. Современные асимметричные криптосистемы	4
		Лабораторная работа № 3. Хэширование и электронная цифровая подпись	4
8	Тема 5. Защита информации в современных операционных системах	Лабораторная работа № 4. Контроль доступа к ресурсам операционной системы, отслеживание событий ОС и анализ системных журналов	4
8	Тема 6. Защита информации в сети	Лабораторная работа № 5. Перехват и анализ сетевых пакетов.	4
		Итого	20

Лабораторные работы (20 часов) проводятся в интерактивной форме. Каждому студенту выдается индивидуальное задание. Затем организуется активный диалог студентов с преподавателем и между собой для подведения итогов решения задания и определения его практической значимости.

5 Самостоятельная работа студента

Для обеспечения самостоятельной работы разработаны:

1. Конспект лекций по дисциплине (см. приложение З.РПД Б3.Б.8 (лк));
2. Методические указания к выполнению лабораторных работ (см. приложение З.РПД Б3.Б.8 (лб));
3. Методические указания к самостоятельной работе студентов (см. приложение З.РПД Б.3.Б.8 (срс)).

Самостоятельная работа студентов по темам дисциплины в часах

№ п/п	№ семестра	Раздел, тема учебной дисциплины	Вид самостоятельной работы студента (курсовой проект, курсовая работа, реферат, расчетно-графическая работа, др.)	Всего часов
1	8	Тема 1. Источники, риски и формы атак на компьютерные системы.	Изучение дополнительного теоретического материала	4
			Подготовка к сеансу тестирования	4
			Подготовка к лекции	2
2	8	Тема 2. Модели безопасности информационных систем	Изучение дополнительного теоретического материала	4
			Подготовка к контрольной работе	2
			Подготовка к лекции	2
3	8	Тема 3. Стандарты безопасности. Законодательные меры защиты информации	Изучение дополнительного теоретического материала	4
			Подготовка к контрольной работе	2
			Подготовка к лекции	2
4	8	Тема 4. Криптографические модели и методы защиты информации	Оформление и подготовка к защите лабораторных работ (3 лабораторные работы)	12
			Изучение дополнительного теоретического материала	4
			Подготовка к сеансу тестирования	4
5	8	Тема 5. Защита информации в современных операционных системах	Изучение дополнительного теоретического материала	4
			Подготовка к контрольной работе	2
			Оформление и подготовка к защите лабораторной работы	4
			Подготовка к лекции	2
6	8	Тема 6. Защита информации в сети	Оформление и подготовка к защите лабораторной работы	4
			Подготовка к контрольной работе	2
			Изучение дополнительного теоретического материала	4
			ИТОГО:	68

Для обеспечения самостоятельной работы разработаны методические указания по самостоятельной работе при подготовке к лабораторным работам.

Виды контроля самостоятельной работы студентов и оценочные средства

№ п/п	№ семестра	Раздел, тема учебной дисциплины	Виды контроля	Оценочные средства
1	8	Тема 2,3, 5, 6	Контрольная работа	«3»- Пороговый уровень освоения компетенции «4»- Продвинутый уровень освоения компетенции «5»- Высокий уровень освоения компетенции
2	8	Тема 1, 4	Тест	«50%»Пороговый уровень освоения компетенции «70%»- Продвинутый уровень освоения компетенции «90%»- Высокий уровень освоения компетенции

Самостоятельная работа студентов по темам дисциплины
Самостоятельная работа студентов по Теме 1.
Контрольные вопросы

1. Что такое информационная безопасность и ее основные аспекты?
2. Какая система называется безопасной и какая надежной?
3. Что такое персональные данные?
4. Что такое служебная тайна?
5. Что такое государственная тайна?
6. Что представляют персональные данные?
7. Дайте определение компьютерной атаки

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

Самостоятельная работа студентов по теме 2

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.

Самостоятельная работа студентов по теме 3

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

Самостоятельная работа студентов по теме 4

Задания к лабораторной работе № 1

Цель работы;

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

Современные симметричные криптосистемы

Номер варианта	Алгоритм
1	Алгоритм шифрования DES. Режим ECB. Реализовать приложение в виде исполняемого файла (*.exe).
2	Алгоритм шифрования DES. Режим CBC. Реализовать приложение в виде исполняемого файла (*.exe).
3	Алгоритм шифрования DES. Режим CFB. Реализовать приложение в виде исполняемого файла (*.exe).
4	Алгоритм шифрования DES. Режим OFB. Реализовать приложение в виде исполняемого файла (*.exe).
5	Алгоритм шифрования TripleDES. Режим ECB. Реализовать приложение в виде исполняемого файла (*.exe).
6	Алгоритм шифрования TripleDES. Режим CBC. Реализовать приложение в виде исполняемого файла (*.exe).

7	Алгоритм шифрования TripleDES. Режим CFB. Реализовать приложение в виде исполняемого файла (*.exe).
8	Алгоритм шифрования TripleDES. Режим OFB. Реализовать приложение в виде исполняемого файла (*.exe).
9	Алгоритм шифрования RC2. Реализовать приложение в виде исполняемого файла (*.exe).
10	Алгоритм шифрования LOKI91. Реализовать приложение в виде исполняемого файла (*.exe).
11	Алгоритм шифрования IDEA. Реализовать приложение в виде исполняемого файла (*.exe).
12	Алгоритм шифрования Blowfish. Реализовать приложение в виде исполняемого файла (*.exe).
13	Отечественный стандарт шифрования данных ГОСТ 28147-89. Режим простой замены. Реализовать приложение в виде исполняемого файла (*.exe).
14	Отечественный стандарт шифрования данных ГОСТ 28147-89. Режим гаммирования. Реализовать приложение в виде исполняемого файла (*.exe).
15	Отечественный стандарт шифрования данных ГОСТ 28147-89. Режим гаммирования с обратной связью. Реализовать приложение в виде исполняемого файла (*.exe).
16	Алгоритм шифрования 3-WAY. Реализовать приложение в виде исполняемого файла (*.exe).
17	Алгоритм шифрования DES. Режим ECB. Реализовать приложение в виде динамически компонуемой библиотеки (*.dll).
18	Алгоритм шифрования DES. Режим CBC. Реализовать приложение в виде динамически компонуемой библиотеки (*.dll).
19	Алгоритм шифрования DES. Режим CFB. Реализовать приложение в виде динамически компонуемой библиотеки (*.dll).
20	Алгоритм шифрования DES. Режим OFB. Реализовать приложение в виде динамически компонуемой библиотеки (*.dll).
21	Алгоритм шифрования TripleDES. Режим ECB. Реализовать приложение в виде динамически компонуемой библиотеки (*.dll).
22	Алгоритм шифрования TripleDES. Режим CBC. Реализовать приложение в виде динамически компонуемой библиотеки (*.dll).
23	Алгоритм шифрования TripleDES. Режим CFB. Реализовать приложение в виде динамически компонуемой библиотеки (*.dll).
24	Алгоритм шифрования TripleDES. Режим OFB. Реализовать приложение в виде динамически компонуемой библиотеки (*.dll).
25	Алгоритм шифрования RC2. Реализовать приложение в виде динамически компонуемой библиотеки (*.dll).
26	Алгоритм шифрования LOKI91. Реализовать приложение в виде динамически компонуемой библиотеки (*.dll).
27	Алгоритм шифрования IDEA. Реализовать приложение в виде динамически компонуемой библиотеки (*.dll).

28	Алгоритм шифрования Blowfish. Реализовать приложение в виде динамически компонуемой библиотеки (*.dll).
29	Отечественный стандарт шифрования данных ГОСТ 28147-89. Режим простой замены. Реализовать приложение в виде динамически компонуемой библиотеки (*.dll).
30	Отечественный стандарт шифрования данных ГОСТ 28147-89. Режим гаммирования. Реализовать приложение в виде динамически компонуемой библиотеки (*.dll).
31	Отечественный стандарт шифрования данных ГОСТ 28147-89. Режим гаммирования с обратной связью. Реализовать приложение в виде динамически компонуемой библиотеки (*.dll).
32	Алгоритм шифрования 3-WAY. Реализовать приложение в виде динамически компонуемой библиотеки (*.dll).

Контрольные вопросы к лабораторной работе № 1

1. Каков размер блока и ключа в алгоритме DES?
2. Каков размер блока и ключа в алгоритме DES?
3. Что такое двукратный DES? Какая атака делает двукратный DES бесполезным?
4. Почему режим OFB (Output Feed Back – Обратная связь по выходу) алгоритма DES применяют для шифрования в спутниковых системах связи?
5. Каков размер блока и ключа в алгоритме ГОСТ 28147-89?
6. Каков размер циклового ключа в алгоритме ГОСТ 28147-89?
7. Какой режим работы алгоритма ГОСТ 28147-89 можно использовать при формировании ЭЦП?
8. Перечислите параметры (размер блока, размер ключа и число раундов) для трех версий AES?
9. Сколько преобразований имеется в каждой версии AES? Сколько ключей необходимо для каждой версии?

Задания к лабораторной работе № 2

Цель работы:

1. Изучение принципов работы асимметричных криптосистем;
2. Изучение реализаций асимметричной криптографии в среде .NET Framework;
3. Реализация существующих асимметричных криптоалгоритмов

Асимметричные криптосистемы

Номер варианта	Задание
1	Алгоритм Меркла-Хеллмана. Секретный и открытый ключи сохранять в текстовом файле. Шифровать (дешифрировать) содержимое файла.
2	Алгоритм Меркла-Хеллмана. Для шифрования и дешифрирования использовать различные приложения. Секретный и открытый ключ отображать в окне приложения.
3	Алгоритм RSA. Секретный и открытый ключи сохранять в текстовом файле. Шифровать (дешифрировать) содержимое файла.
4	Алгоритм RSA. Для шифрования и дешифрирования использовать различные приложения. Секретный и открытый ключ отображать в окне приложения.
5	Алгоритм Полига-Хеллмана. Секретный и открытый ключи сохранять в текстовом файле. Шифровать (дешифрировать) содержимое файла.
	Алгоритм Полига-Хеллмана. Для шифрования и дешифрирования использовать

6	различные приложения. Секретный и открытый ключ отображать в окне приложения.
7	Алгоритм Рабина. Секретный и открытый ключи сохранять в текстовом файле. Шифровать (дешифрировать) содержимое файла
8	Алгоритм Рабина. Для шифрования и дешифрирования использовать различные приложения. Секретный и открытый ключ отображать в окне приложения
9	Алгоритм Вильямса. Секретный и открытый ключи сохранять в текстовом файле. Шифровать (дешифрировать) содержимое файла
10	Алгоритм Вильямса. Для шифрования и дешифрирования использовать различные приложения. Секретный и открытый ключ отображать в окне приложения
11	Алгоритм Эль Гамаля. Секретный и открытый ключи сохранять в текстовом файле. Шифровать (дешифрировать) содержимое файла
12	Алгоритм Эль Гамаля. Для шифрования и дешифрирования использовать различные приложения. Секретный и открытый ключ отображать в окне приложения
13	Алгоритм Месси-Омуры. Секретный и открытый ключи сохранять в текстовом файле. Шифровать (дешифрировать) содержимое файла
14	Алгоритм Месси-Омуры. Для шифрования и дешифрирования использовать различные приложения. Секретный и открытый ключ отображать в окне приложения
15	Алгоритм МакЭлиса. Секретный и открытый ключи сохранять в текстовом файле. Шифровать (дешифрировать) содержимое файла
16	Алгоритм МакЭлиса. Для шифрования и дешифрирования использовать различные приложения. Секретный и открытый ключ отображать в окне приложения

Контрольные вопросы к лабораторной работе № 2

1. Приведите примеры однонаправленных функций.
2. Для числа a=5 найдите обратное число по модулю n=7. Имеет ли данная задача решение? Приведите примеры криптосистем, использующих правила модулярной арифметики.
3. Для числа a=72 найдите обратное число по модулю n=8. Имеет ли данная задача решение? Приведите примеры криптосистем, использующих правила модулярной арифметики.
4. Для числа N=7*11 с помощью функции Эйлера φ(N) определите количество положительных целых чисел, меньших N и взаимно простых с N. В каких криптосистемах используется функция Эйлера?
5. Определите хотя бы одно возможное значение открытого ключа алгоритма RSA, если P=3, Q=11.
6. Определите значение закрытого ключа для алгоритма RSA, если открытый ключ E=7, а функция Эйлера имеет значение φ(N)=20
7. В криптосистеме RSA дано N=221 и E=5, найдите D.
8. В криптосистеме RSA дано N=3937 и E=17, найдите D.
9. В криптосистеме RSA дано P=19, Q=23 и E=3, найдите N, φ(N) и D.
10. В криптосистеме RSA дано E=13 и N=100. Зашифруйте сообщение «HOW ARE YOU», кодируя английский алфавит числами от 00 до 25 и используя число 26 для пробела. Используйте различные блоки, чтобы сделать P<N.

Задания к лабораторной работе № 3

Цель работы:

1. Изучение методов формирования дайджеста сообщения (хэш-функции) и электронной цифровой подписи (ЭЦП);

2. Изучение реализаций хэш-функций и ЭЦП в среде .NET Framework;
3. Реализация существующих хэш-функций и алгоритмов ЭЦП.

Электронная цифровая подпись

Создайте клиент-серверное приложение. Клиент передает подписанное письмо. Сервер его получает и верифицирует ЭЦП. Пусть для передачи используются файлы. Сообщение должно быть зашифровано. Для шифрования/дешифрирования и формирования ЭЦП используются функции из пространства имен System.Security.Cryptography.

Номер варианта	Задание
1	2
1	Для шифрования использовать алгоритм DES, для формирования ЭЦП – алгоритм RSA (методы SignHash и VerifyHash)
2	Для шифрования использовать алгоритм TripleDES, для формирования ЭЦП – алгоритм RSA (методы SignHash и VerifyHash)
3	Для шифрования использовать алгоритм Rijndael, для формирования ЭЦП – алгоритм RSA (методы SignHash и VerifyHash)
4	Для шифрования использовать алгоритм RC2, для формирования ЭЦП – алгоритм RSA (методы SignHash и VerifyHash)
5	Для шифрования использовать алгоритм DES, для формирования ЭЦП – алгоритм DSA (методы SignHash и VerifyHash)
6	Для шифрования использовать алгоритм TripleDES, для формирования ЭЦП – алгоритм DSA (методы SignHash и VerifyHash)
7	Для шифрования использовать алгоритм Rijndael, для формирования ЭЦП – алгоритм DSA (методы SignHash и VerifyHash)
8	Для шифрования использовать алгоритм RC2, для формирования ЭЦП – алгоритм DSA (методы SignHash и VerifyHash)
9	Для шифрования использовать алгоритм DES, для формирования ЭЦП – алгоритм RSA (метод SignData)
10	Для шифрования использовать алгоритм TripleDES, для формирования ЭЦП – алгоритм RSA (метод SignData)
11	Для шифрования использовать алгоритм Rijndael, для формирования ЭЦП – алгоритм RSA (метод SignData)
12	Для шифрования использовать алгоритм RC2, для формирования ЭЦП – алгоритм RSA (метод SignData)
13	Для шифрования использовать алгоритм DES, для формирования ЭЦП – алгоритм DSA (метод SignData)
14	Для шифрования использовать алгоритм TripleDES, для формирования ЭЦП – алгоритм DSA (метод SignData)
15	Для шифрования использовать алгоритм Rijndael, для формирования ЭЦП – алгоритм DSA (метод SignData)
16	Для шифрования использовать алгоритм RC2, для формирования ЭЦП – алгоритм DSA (метод SignData)

Не используя пространство имен System.Security.Cryptography и CryptoAPI, выполнить следующие задания

Номер варианта	Задание
1	Хэш-функция Ральфа Меркла
2	N-хэш
3	MD4
4	MD5
5	MD2
6	Алгоритм безопасного хэширования SHA1
7	Хэш-функция HAVAL
8	Хэш-функция ГОСТ Р 34.11-94
9	ЭЦП RSA
10	ЭЦП DSA
11	ЭЦП Эль-Гамаля
12	ЭЦП ГОСТ Р 34.10-94
13	ЭЦП ГОСТ Р 34.10-2001
14	ЭЦП ESIGN
15	Алгоритм безопасного хэширования SHA256
16	Алгоритм безопасного хэширования SHA384
17	Алгоритм безопасного хэширования SHA512

Контрольные вопросы к лабораторной работе № 3

1. Что называется электронной цифровой подписью?
2. Для чего используется электронная цифровая подпись?
3. Что такое хэш-функция?
4. Что такое дайджест сообщения?
5. Используя схему RSA, при P=809, Q=751 и секретный ключ D=23, вычислите открытый ключ E, Затем: подпишите и проверьте сообщение M_1=100. Получите подпись S_1.
6. Используя схему RSA, при P=809, Q=751 и секретный ключ D=23, вычислите открытый ключ E, Затем: подпишите и проверьте сообщение M_2=50. Получите подпись S_2.
7. Используя схему RSA, при P=809, Q=751 и секретный ключ D=23, вычислите открытый ключ E, Затем: покажите, что если $M=M_1 x M_2$=5000, то $S=S_1 x S_2$.

Тест по теме 4

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. 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 $A^x \bmod N = Y$

3. 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
4. Какой из перечисленных алгоритмов является алгоритмом хэширования:
    a. SHA
    b. RSA
    c. Эль-Гамаля
    d. DSA
5. Какой из режимов работы алгоритма DES можно использовать для формирования электронной цифровой подписи
    a. ECB
    b. CBC
    c. CFB
    d. OFB
6. Какой из режимов работы алгоритма DES используется в телекоммуникационных системах
    a. ECB
    b. CBC
    c. CFB
    d. OFB
7. 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
8. 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
9. 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
10. Определите возможные значения открытого ключа алгоритма RSA, если P=3, Q=11
    a. 7
    b. 11
    c. 13

d. 6
e. 9
f. 4

11. 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
12. 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
13. 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
14. 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
15. Размер блока в DES:
16. Размер ключа в DES:
17. Размер ключа раунда в DES:
18. Покажите результат прохождения 110111 через S-блок 3:
19. Покажите результат прохождения 001100 через S-блок 4:
20. Покажите результат прохождения 000000 через S-блок 7:
21. Покажите результат прохождения 111111 через S-блок 2:
22. Найдите результат следующей операции $(01001101) \oplus (01001101)$:
23. Найдите результат следующей операции $(01001101) \oplus (10110010)$:
24. Назовите размер блока, размер ключа и число раундов для AES-128:
25. Назовите размер блока, размер ключа и число раундов для AES-192:
26. Назовите размер блока, размер ключа и число раундов для AES-256:

Самостоятельная работа студентов по теме 5
Задания к лабораторной работе № 4 (тема 5)
Цель лабораторной работы:

1. Исследование методов контроля доступа к ресурсам операционной системы:
2. Удаленный доступ к ресурсам с использованием технологии WMI.
3. Рассмотреть методы работы с системными журналами

4. Отслеживать события изменения аппаратуры и файловой системы
5. Отслеживать события записи в системные журналы

Вариант 1

1. С помощью технологии WMI получить информацию о дисках удаленного компьютера
2. С помощью технологии WMI подсчитать количество групп на удаленном компьютере
3. Изменить права доступа для какого-либо файла на локальном компьютере (файл, создан Вами)
4. Отслеживать изменения аппаратуры и заносить информацию об изменениях в специально созданный журнал событий. Выполнять обработку созданного журнала (очистка, фильтрация по любому признаку и т.д.)

Вариант 2

1. С помощью технологии WMI получить информацию о процессоре удаленного компьютера
2. С помощью технологии WMI подсчитать количество пользователей на удаленном компьютере
3. Изменить права доступа для какого-либо файла на локальном компьютере (файл, создан Вами)
4. Отслеживать события создания папок в любом выбранном каталоге и заносить информацию об изменениях в специально созданный журнал событий. Выполнять обработку созданного журнала (очистка, фильтрация по любому признаку и т.д.)

Вариант 3

1. С помощью технологии WMI получить информацию о видеоконтроллере удаленного компьютера
2. С помощью технологии WMI вывести на экран SID всех пользователей удаленного компьютера
3. Изменить права доступа для какого-либо файла на локальном компьютере (файл, создан Вами)
4. Отслеживать события создания файлов и папок в любом выбранном каталоге и заносить информацию об изменениях в специально созданный журнал событий. Выполнять обработку созданного журнала (очистка, фильтрация по любому признаку и т.д.).

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

Самостоятельная работа студентов по теме 6
Лабораторная работа № 5 (по теме 6)
Цель работы;

1. Аудит сетевого трафика
2. Изучить возможности библиотеки WinPcap
3. Изучить возможности библиотеки SharpPcap

Разработать оконное приложение для:

1. StealthFIN сканирования и его обнаружения(критерий: с одного адреса на разные порты пришло более 10 пакетов с флагом FIN);
2. Сниффер (перехват пакетов, сохранение их в лог-файле);
3. Подсчета интенсивности трафика в сети по протоколу TCP
4. Подсчета интенсивности трафика в сети по протоколу UDP;
5. Подсчета интенсивности трафика в сети по протоколу ICMP;

6. Подсчета количества HTTP-пакетов в сети;
7. Подсчета количества SMTP-пакетов в сети;
8. Подсчета количества POP или IMAP-пакетов в сети;
9. Подсчета интенсивности трафика по протоколу TCP для данного компьютера;
10. Подсчета интенсивности трафика по протоколу UDP для данного компьютера;
11. Подсчета интенсивности трафика по протоколу ICMP для данного компьютера;
12. Подсчета количества переданных и принятых HTTP-пакетов для данного компьютера;
13. Подсчета количества переданных и принятых SMTP-пакетов для данного компьютера;
14. Подсчета количества POP или IMAP-пакетов для данного компьютера;
15. Направленного шторма запросов на определенные порты
16. Широковещательного шторма запросов
17. Получения списка портов, с которыми было установлено соединение
18. Получения списка адресов, с которыми было установлено соединение
19. Запись в файл всех пакетов, адресованных данному компьютеру
20. Запись в файл всех пакетов, переданных по сети

Контрольные вопросы к лабораторной работе № 5

1. Перечислите основные функции библиотеки WinPcap
2. Перечислите основные функции библиотеки SharpPcap
3. Почему для аудита сетевого трафика требуется создание отдельного потока
4. Расскажите механизм обработки событий в C#
5. Как определить получаемые и отправляемые пакеты
6. Как определить, что передается или принимается пакет HTTP, SNMP или FTP

Контрольная работа 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 COA 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

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:

- общекультурные ОК-11, ОК-12, ОК-13;
- профессиональные ПК-1, ПК-2, ПК-5, ПК-9, ПК-10, ПК-11.

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

Образовательные технологии, обеспечивающие результаты освоения дисциплины в форме компетенций

Код и название компетенции	Компонентный состав компетенции (дескрипторы)	Технологии формирования	Средства оценки
ОК-11	Знать: основные положения законодательства в области современного авторского права и защиты	лекции,	Тест

	информации		
	Уметь: разрабатывать модели компонентов систем защиты информации	Домашнее задание	Тест
	Владеть: терминологией в области защиты информации	Домашнее задание	Тест
ОК-12	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	Домашнее задание	Опрос, Контрольная работа
ОК-13	Знать: основные понятия, используемые в сфере защиты информации, основные виды угроз сохранности информации и методы борьбы с ними	лекции, лабораторные занятия	Опрос, контрольные работы
	Уметь: организовывать систему защиты информации в глобальных компьютерных сетях	лабораторные занятия	Опрос
	Владеть: методами защиты вычислительных комплексов и автоматизированных систем в глобальных сетях	лабораторные занятия	Опрос
ПК-1	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	Домашнее задание	Тест
	Владеть: технологиями администрирования и защиты сетевых приложений	Домашнее задание	Тест
ПК-2	Знать: современные программные средства разработки систем защиты, защищенных приложений, методов аудита безопасности и отслеживания вторжений	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
ПК5:	Знать: основные инструментальные средства и программные технологии, используемые для защиты информации в сети и на отдельном компьютере	лекции, лабораторные занятия	Опрос, контрольные работы, тест
	Уметь: выбирать оптимальные методы защиты конфиденциальной информации в сети и на отдельном компьютере соответствии с особенностями конкретной ОС	лабораторные занятия	Опрос, контрольные работы, тест
	Владеть: Программными технологиями,		

	используемыми для создания защищенных приложений. Владеть практикой создания защищенных приложений		
ПК-9:	Знать: современные средства защиты программных комплексов	лекции, лабораторные занятия	Опрос, контрольные работы,
	Уметь: разрабатывать компоненты защиты программных комплексов и баз данных, использовать современные средства и технологии защиты информации	лабораторные занятия	Опрос, контрольные работы
	Владеть: технологиями разработки и внедрения средств защиты	лабораторные занятия	Опрос, контрольные работы
ПК-10	Знать: методы сопряжения аппаратных и программных средств в составе информационных и автоматизированных систем защиты	лекции, лабораторные занятия	Опрос, контрольные работы,
	Уметь: сопрягать аппаратные и программные средства в составе информационных и автоматизированных систем защиты	лабораторные занятия	Опрос, контрольные работы
	Владеть: методами сопряжения аппаратных и программных средств в составе информационных и автоматизированных систем защиты	лабораторные занятия	Опрос, контрольные работы
ПК-11	Знать: основные модели обеспечения компьютерной безопасности	лекции, лабораторные занятия	Опрос, контрольные работы,
	Уметь: разрабатывать модели систем защиты информации вычислительных комплексов и автоматизированных систем	лабораторные занятия	Опрос, контрольные работы
	Владеть: методами инсталляции программного и аппаратного обеспечения для информационных и автоматизированных систем защиты	лабораторные занятия	Опрос, контрольные работы

Оценка уровней сформированности компетенций в результате освоения учебной дисциплины

Коды компетен-ций	Уровни сформированности компетенции	Основные признаки уровня
Общекультурные компетенции - ОК		
ОК-11	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
ОК-12	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
ОК-13	Пороговый уровень освоения компетенции	Знает: основные понятия, используемые в сфере защиты информации, основные виды угроз сохранности информации и методы борьбы с ними
	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
ПК-1	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
	Высокий уровень освоения компетенции	Дополнительно владеет: технологиями администрирования и защиты сетевых приложений
ПК-2	Пороговый уровень освоения компетенции	Знает: современные программные средства разработки систем защиты, защищенных приложений, методов аудита безопасности и отслеживания вторжений
	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
ПК-5	Пороговый уровень освоения компетенции	Знает: основные инструментальные средства и программные технологии, используемые для защиты информации в сети и на отдельном компьютере
	Продвинутый уровень освоения компетенции	Дополнительно умеет: выбирать оптимальные методы защиты конфиденциальной информации в сети и на отдельном компьютере соответствии с особенностями конкретной ОС
	Высокий уровень освоения компетенции	Дополнительно владеет: Программными технологиями, используемыми для создания защищенных приложений. Владеть практикой создания защищенных приложений
ПК-9	Пороговый уровень освоения компетенции	Знает: современные средства защиты программных комплексов и баз данных
	Продвинутый уровень освоения	Дополнительно умеет: разрабатывать компоненты

	компетенции	защиты программных комплексов и баз данных, использовать современные средства и технологии защиты информации
	Высокий уровень освоения компетенции	Дополнительно владеет: технологиями разработки и внедрения средств защиты
ПК-10	Пороговый уровень освоения компетенции	Знает: методы сопряжения аппаратных и программных средств в составе информационных и автоматизированных систем защиты
	Продвинутый уровень освоения компетенции	Дополнительно умеет: сопрягать аппаратные и программные средства в составе информационных и автоматизированных систем защиты
	Высокий уровень освоения компетенции	Дополнительно владеет: методами сопряжения аппаратных и программных средств в составе информационных и автоматизированных систем защиты
ПК-11	Пороговый уровень освоения компетенции	Знает: основные модели обеспечения компьютерной безопасности
	Продвинутый уровень освоения компетенции	Дополнительно умеет: разрабатывать модели систем защиты информации вычислительных комплексов и автоматизированных систем
	Высокий уровень освоения компетенции	Дополнительно владеет: методами инсталляции программного и аппаратного обеспечения для информационных и автоматизированных систем защиты

Формы текущего контроля по разделам, темам дисциплины

№№пп	Наименование раздела, 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

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

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 З.РПД Б3.Б.8 (лк));
2. Методические указания к выполнению лабораторных работ (см. приложение З.РПД Б3.Б.8 (лб));
3. Методические указания к самостоятельной работе студентов (см. приложение З.РПД Б.3.Б.8 (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=5242
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.

Практические (семинарские) занятия составляют важную часть профессиональной подготовки студентов. Основная цель проведения практических (семинарских) занятий - формирование у студентов аналитического, творческого мышления путем приобретения практических навыков.

Методические указания к практическим (семинарским) занятиям по дисциплине наряду с рабочей программой и графиком учебного процесса относятся к методическим документам, определяющим уровень организации и качества образовательного процесса.

Содержание *практических (семинарских) занятий* фиксируется в РПД в разделе 4 настоящей программы.

Важнейшей составляющей любой формы практических занятий являются упражнения (задания). Основа в упражнении - пример, который разбирается с позиций теории, развитой в лекции. Как правило, основное внимание уделяется формированию конкретных умений, навыков, что и определяет содержание деятельности студентов - решение задач, графические работы, уточнение категорий и понятий науки, являющихся предпосылкой правильного мышления и речи.

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 полученных 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)

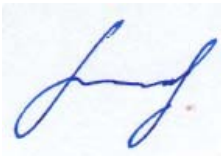
При проведении **лабораторных работ** предусматривается использование персональных компьютеров, оснащенных необходимым комплектом лицензионного программного обеспечения. – Viusual Studio 2010 по подписке Dream Spark.

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 28 августа 2015 года, протокол № 01.