МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ФАКУЛЬТЕТ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

УТВЕРЖДАЮ

Декан ФВТ

_____ Л.Р. Фионова

«22» сентября 2016 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

С1.1.21 Защита информации

Специальность: 09.05.01 *«Применение и эксплуатация автоматизированных систем специального назначения»*

Специализация №12: *«Автоматизированные системы обработки информации и управления специального назначения»*

Квалификация (степень) выпускника: *инженер*

Форма обучения: *очная*

Пенза, 2016

1. Цели освоения дисциплины

Целями освоения дисциплины «Защита информации» являются: овладение студентами понятиями, нормативно-правовой базой в области информационной безопасности и основными методами и средствами защиты информации от несанкционированного доступа и вредоносных программ; подготовка студентов к способности решать задачи профессиональной деятельности по обеспечению защиты информации в автоматизированных системах специального назначения с учетом основных требований информационной безопасности, применением методов и средств защиты информации и современных информационно-коммуникационных технологий.

2. Место дисциплины в структуре ОПОП специалитета

Дисциплина «Защита информации» относится к дисциплинам базовой части ОПОП (С1.1).

Изучение дисциплины базируется на знаниях, умениях и готовностях полученных студентами при изучении следующих дисциплин: «Математика», «Информатика», «Программирование».

Дисциплина является одной из заключительных в образовательной программе подготовки специалистов по направлению «Применение и эксплуатация автоматизированных систем специального назначения». Компетенции, приобретенные в ходе изучения данной дисциплины, могут быть использованы в процессе дипломного проектирования и в профессиональной деятельности.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины «Защита информации»

Процесс изучения дисциплины «Защита информации» направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО по данному направлению:

Коды компетенции	Наименование компетенции	Структурные элементы компетенции (в результате освоения дисциплины обучающийся должен знать, уметь, владеть)
ОПК-3	Способность использовать основные законы естественнонаучных дисциплин в профессиональной деятельности, применять методы математического анализа и моделирования, теоретического и экспериментального исследования	**Знать:** методы математического анализа, теоретические и нормативно-правовые основы в области защиты информации, основы моделирования систем защиты информации
		Уметь: профессионально грамотно использовать на практике нормативно-правовую документацию по организации защиты информации, реализовывать методы математического анализа при решении задач в области защиты информации и проводить теоретические и экспериментальные исследования при решении задач по обеспечению информационной безопасности в сфере профессиональной деятельности
		Владеть: навыками организации и моделирования систем защиты информации, реализации основных методов математического анализа при решении задач в сфере профессиональной деятельности

ПК-20	Способность разрабатывать и выбирать методы и средства обеспечения информационной безопасности в сфере профессиональной деятельности	**Знать:** виды угроз информационной безопасности и способы их предотвращения, основные требования к информационной безопасности, методы и средства защиты информации от несанкционированного доступа и вредоносных программам в автоматизированных системах специального назначения и технологии реализации их алгоритмов
		Уметь: профессионально грамотно анализировать риск возникновения возможных угроз при передаче информации в автоматизированных системах специального назначения, обосновывать выбор методов и средств защиты информации от несанкционированного доступа и вредоносных программ и реализовывать их алгоритмы при решении задач по обеспечению информационной безопасности в сфере профессиональной деятельности
		Владеть: навыками организации защиты информации от несанкционированного доступа и вредоносных программ и навыками реализации основных методов и средств защиты информации при решении задач по обеспечению защиты информации в сфере профессиональной деятельности с учетом основных требований к обеспечению информационной безопасности
ПК-26	Способность оценивать эффективность защиты информации в автоматизированных системах специального назначения (ПК-26).	**Знать:** методы оценки эффективности защиты информации в автоматизированных системах специального назначения
		Уметь: профессионально грамотно использовать на практике методы оценки эффективности защиты информации при решении задач по обеспечению информационной безопасности в автоматизированных системах специального назначения
		Владеть: навыками оценки эффективности защиты информации в автоматизированных системах специального назначения при решении задач в сфере профессиональной деятельности

4. Структура и содержание дисциплины

4.1. Структура дисциплины

Общая трудоемкость дисциплины составляет 6 зачетных единицы, 216 часов

№ п/п	Наименование разделов и тем дисциплины (модуля)	Семестр	Недели семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)									Формы текущего контроля успеваемости *(по неделям семестра)*							
				Аудиторная работа				Самостоятельная работа												
				Всего	Лекции	Практические занятия	Лабораторные занятия	Всего	Подготовка к аудиторным занятиям	Реферат, эссе и др.	Курсовая работа (проект)	Подготовка к экзамену	Собеседование	Коллоквиум	Проверка тестов	Проверка клабор. работ	Проверка реферата	Проверка эссе и иных творческих работ	курсовая работа (проект)	Защита лабораторных работ
1	Раздел 1. Основы информационной безопасности	8	1-9	14	8	-	6	28	20	-	-	8	1-18	-	-	-	-	-	-	1-9
2	Раздел 2. Криптографические методы защиты информации	8	10-18	34	18	-	16	50	40	-	-	10	1-18	-	-	-	-	-	-	10-18
3	Раздел 3. Формирование и проверка электронной подписи	9	1-8	23	11	-	12	30	22	-	-	8	1-18	-	-	-	-	-	-	1-18
4	Раздел 4. Идентификация и аутентификация пользователей	9	9-11	6	6	-	-	9	5	-	-	4	-	-	-	-	-	-	-	-
5	Раздел 5. Защита информации от вредоносных программ	9	12-14	4	4	-	-	6	4	-	-	2	-	-	-	-	-	-	-	-

6	Раздел 6. Оценка эффективности защиты информации	9	15-18	4	4	-	-	8	4	-	-	4		-	-	-	-	-	-	-
	Подготовка к экзамену	9										36								
	Общая трудоемкость, в часах			85	51	-	34	131	95	-	-	36	Промежуточная аттестация							
													Форма					Семестр		
													Зачет					8		
													Экзамен					9		

4.2. Содержание дисциплины

4.2.1. Содержание лекционного курса

Раздел 1. Основы информационной безопасности

Тема 1.1. Основные понятия в области информационной безопасности: понятия информации, информационного ресурса, документированной информации, уровня секретности информации, конфиденциальности информации; ценность информации; категории важности информации, группы потребителей информации, качество информации и базовая система его показателей, понятие, цели и задачи информационной безопасности;

Тема 1.2. Правовые основы информационной безопасности: информация как объект права собственности, собственник и хранитель информации; право собственности на информацию, реализация права собственности на информацию, ответственность и полномочия субъектов права собственности на информацию, правовые документы о защите информации, закон Российской Федерации «Об информатизации, информационных технологиях и о защите информации».

Тема 1.3. Угрозы при передаче и обработке информации: понятие угрозы информации, факторы возникновения угроз информации, воздействия нарушителей в автоматизированных системах специального назначения, классификация угроз информации, понятие об активном и пассивном перехвате, методы криптоанализа, противодействия нападениям на защищенные сообщения;

Тема 1.4. Методы и средства обеспечения информационной безопасности: требования и принципы информационной безопасности, методы защиты информации и их классификация, средства защиты информации в автоматизированных системах специального назначения, комплексные средства защиты информации;

Тема 1.5. Методы математического анализа в области защиты информации

Тема 1.6. Моделирование систем защиты информации

Раздел 2. Криптографические методы защиты информации

Тема 2.1. Основные понятия в области криптографии: понятия криптологии, криптографии, криптоанализа; понятия открытого текста и шифротекста, воздействия нарушителей на криптосистемы, понятие о стойкости криптосистем, виды криптографических методов защиты информации, математические операции в криптографических системах;

Тема 2.2. Симметричные системы шифрования: принципы и схема симметричного шифрования; поточные и блочные шифры; генерация ключевой последовательности, стандарт шифрования данных AES;

Тема 2.3. Асимметричные системы шифрования: принципы и обобщенная схема асимметричного шифрования; обмен ключевой информацией, детальная схема ассиметричного шифрования, алгоритмы асимметричного шифрования RSA и Эль-Гамаля.

Раздел 3. Формирование и проверка электронной подписи

Тема 3.1. Хэш-код сообщения: понятия хэш-функции и хэш-кода сообщения, свойства хэш-кода сообщения; типовая схема вычисления хэш-кода сообщения, парадокс «Дня рождения», усложненные схемы вычисления хэш-кода сообщения, алгоритм безопасного формирования хэш-кода сообщения SHA1;

Тема 3.2. Электронная подпись: понятие электронной подписи, обобщенная и детальная схемы формирования электронной подписи, алгоритм формирования и проверки электронной подписи по Эль-Гамалю.

Раздел 4. Идентификация и аутентификация пользователей

Тема 2.1. Идентификация пользователя: понятие идентификации, методы идентификации пользователя;

Тема 2.2. Аутентификация пользователей: понятие аутентификации, методы аутентификации, многофакторная аутентификация.

Раздел 5. Защита информации от вредоносных программ

Тема 5.1. Вредоносные программы: понятие вредоносной программы, классификация вредоносных программ, их функциональные возможности и наносимый ими ущерб;

Тема 5.2. Способы и методы защиты информации от вредоносных программ.

Раздел 6. Оценка эффективности защиты информации

Тема 6.1 Понятие эффективности защиты информации

Тема 6.2 Методы оценки эффективности систем защиты информации

Тема 6.3 Риски информационной безопасности

Тема 6.4 Меры защиты и поддержания эффективности системы защиты информации

4.2.2. Перечень и содержание лабораторных занятий

№ п/п	№ разделов	Наименование лабораторных работ	Кол. ч
1	1	Математические операции в криптографических системах	6
2	1	Генерация ключевой последовательности	5
3	2	Криптографическая система защиты информации на основе стандарта AES (Rijndael)	6
4	2	Криптографическая система асимметричного шифрования RSA	4
5	3	Формирование хэш-кода сообщения на основе алгоритма SHA-1	4
6	2,3	Комплексная система защиты информации по Эль-Гамалю	4
7,8	2,3	Криптографическая система PGP	5
Всего			34

5. Образовательные технологии

5.1. Чтение лекций с использованием доски и мультимедийного компьютерного проектора и с применением программного продукта Open Office.

5.2. Изучение материалов лабораторного практикума с использованием образовательного материала, программного обеспечения и информационных ресурсов с сайта кафедры ИВС (http://dep_ivs.pnzgu.ru) и файл-сервера кафедры ИВС (диск Т).

5.3. Выполнение лабораторного практикума исследовательского и проектного характера с использованием средств разработки приложений, выбираемых обучаемыми самостоятельно, например, среды разработки Matlab.

5.4. Мастер-классы по работе с криптографическими средствами защиты информации.

5.5. Самостоятельная работа студентов с использованием образовательного материала, программного обеспечения и информационных ресурсов с сайта кафедры ИВС (http://dep_ivs.pnzgu.ru) и файл-сервера кафедры ИВС (диск Т).

5.6. В целях реализации индивидуального подхода к обучению студентов, осуществляющих учебный процесс по собственной траектории в рамках индивидуального рабочего плана, изучение данной дисциплины базируется на следующих возможностях: обеспечение внеаудиторной работы со студентами в том числе в электронной образовательной среде с использованием соответствующего программного оборудования, дистанционных форм обучения, возможностей интернет-ресурсов, индивидуальных консультаций и т.д.

6. Учебно-методическое обеспечение самостоятельной работы студентов. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

6.1. План самостоятельной работы студентов

№ нед.	Тема	Вид самостоятельной работы	Задание	Рекомендуемая литература	Количество часов
1-9	Основы информационной безопасности	Подготовка к аудиторным занятиям по темам лекционных и лабораторных занятий (см. п. 4.2.1 и 4.2.2), подготовка к зачету и экзамену	1. Изучить: - основные понятия в области информационной безопасности; - правовые основы информационной безопасности; - существующие угрозы при передаче и обработке информации; - современные методы и средства обеспечения информационной безопасности; - методы математического анализа в области защиты информации; - основы моделирования систем защиты информации	1. Учебно-методические материалы и электронные учебные материалы с сайта кафедры ИВС (http://dep_ivs.pnzgu.ru) и файл-сервера кафедры ИВС (диск Т) 2. Основная литература /1,2,3/ 3. Дополнительная литература /2/ 4. Программное обеспечение и интернет-ресурсы: /1/	28
10-18	Криптографические методы защиты информации	Подготовка к аудиторным занятиям по темам лекционных и лабораторных занятий (см. п. 4.2.1 и 4.2.2), подготовка к зачету и экзамену	Изучить: - основные понятия в области криптографии; - симметричные системы шифрования; - асимметричные системы шифрования	1. Учебно-методические материалы и электронные учебные материалы с сайта кафедры ИВС (http://dep_ivs.pnzgu.ru) и файл-сервера кафедры ИВС (диск Т) 2. Основная литература /1,2,3/	50

				3. Дополнительная литература: /1,2,3/ 4. Программное обеспечение и интернет-ресурсы: /1,2,3/	
1-8	Формирование и проверка электронной подписи	Подготовка к аудиторным занятиям по темам лекционных и лабораторных занятий (см. п. 4.2.1 и 4.2.2), подготовка к зачету и экзамену	Изучить: - понятие хэш-кода сообщения и основные алгоритмы его формирования; - понятие электронной подписи и основные алгоритмы ее формирования	1. Учебно-методические материалы и электронные учебные материалы с сайта кафедры ИВС (http://dep_ivs.pnzgu.ru) и файл-сервера кафедры ИВС (диск Т) 2. Основная литература /1,2,3/ 3. Дополнительная литература: /1,2,3/ 4. Программное обеспечение и интернет-ресурсы: /1,2,3/	30
9-11	Идентификация и аутентификация пользователей	Подготовка к аудиторным занятиям по темам лекционных и лабораторных занятий (см. п. 4.2.1 и 4.2.2), подготовка к зачету и экзамену	Изучить: - понятие и методы идентификации пользователей; - понятие и методы аутентификации пользователей	1. Учебно-методические материалы и электронные учебные материалы с сайта кафедры ИВС (http://dep_ivs.pnzgu.ru) и файл-сервера кафедры ИВС (диск Т) 2. Основная литература /1,2/ 3. Дополнительная литература: /2,3/ 4. Программное обеспечение и интернет-ресурсы:/1/	9
12-14	Защита информации от вредоносных программ	Подготовка к аудиторным занятиям по темам лекционных и лабораторных занятий (см. п. 4.2.1 и 4.2.2),	Изучить: - понятие вредоносная программа; - классификацию вредоносных программ, их функциональные возможности и	1. Учебно-методические материалы и электронные учебные материалы с сайта кафедры ИВС (http://dep_ivs.pnzgu.ru) и файл-сервера	6

		подготовка к зачету и экзамену	наносимый ими ущерб; - способы и методы защиты информации от вредоносных программ	кафедры ИВС (диск Т) 2. Основная литература /1,2,3/ 3. Дополнительная литература: /2,3/ 4. Программное обеспечение и интернет-ресурсы:/1/	
15-18	Оценка эффективности защиты информации	Подготовка к аудиторным занятиям по темам лекционных и лабораторных занятий (см. п. 4.2.1 и 4.2.2), подготовка к зачету и экзамену	Изучить: - понятие эффективности защиты информации; - методы оценки эффективности систем защиты информации; - существующие риски информационной безопасности; - основные меры защиты и поддержания эффективности системы защиты информации	1. Учебно-методические материалы и электронные учебные материалы с сайта кафедры ИВС (http://dep_ivs.pnzgu.ru) и файл-сервера кафедры ИВС (диск Т) 2. Основная литература /1,2/ 3. Дополнительная литература: /2,3/ 4. Программное обеспечение и интернет-ресурсы: /1/	8
Всего					131

6.2. Методические указания по организации самостоятельной работы студентов

Каждый студент должен вести самостоятельную работу по основным разделам дисциплины в объемах, не меньших, чем указано в программе.

1. **Самостоятельная подготовка к лекциям**. Для понимания материала лекции необходимо изучить вопросы предшествующей лекции по лекциям и основной литературе и познакомиться с дополнительной литературой.

Для самостоятельной подготовки студентов к темам лекций, к текущему и промежуточному контролю необходимо использовать основную и дополнительную литературу и электронные учебные материалы с сайта кафедры ИВС (http://dep_ivs.pnzgu.ru) и файл-сервера кафедры ИВС (диск Т).

2. **Самостоятельная подготовка к лабораторным работам**. Контроль осуществляется во время выполнения и сдачи лабораторных работ. Подготовка к лабораторным работам должна включать изучение математических операций в криптографических системах и алгоритмов криптографического закрытия данных.

При выполнении лабораторных работ средства разработки выбираются обучаемыми самостоятельно, например, среда разработки Matlab.

Результатом лабораторных работ должны быть отчеты по выполненным работам, содержащие теоретические сведения по изученной теме, практические результаты и вывод.

6.3. Материалы для проведения текущего и промежуточного контроля знаний студентов

1. Для проведения промежуточного и текущего контроля знаний используются экзаменационные вопросы и задачи в соответствии с тематикой лекционных разделов;

2. Текущий контроль знаний проводится в форме собеседования при защите лабораторных работ;

3. Промежуточный и текущий контроль знаний заключается в контроле освоения компетенций по тематике лекционных разделов.

Контроль освоения компетенций

№ п\п	Вид контроля	Контролируемые темы (разделы)	Компетенции, компоненты которых контролируются
1	Текущий контроль: собеседование при защите лабораторных работ	Разделы 1 – 3	ОПК-3, ПК-20
2	Промежуточный контроль: экзамен	Разделы 1 – 6	ОПК-3, ПК-20, ПК-26

6.4 Вопросы для собеседования при защите лабораторных работ (примеры)

Структурный элемент компетенций «знать»

1. Дайте определение группы, кольца и поля.
2. В чем различие и сходство операций над целыми числами и многочленами?
3. Что такое неприводимый многочлен?
4. Что такое простой многочлен?
5. Что такое НОД?
6. В чём состоит сходство и отличие операций вычета и сравнения?
7. Какие основные характеристики имеют поля Галуа?
8. Что такое изоморфные поля случайных элементов?
9. Что такое неприводимый и приведенный многочлен?
10. Почему сгенерированные последовательности элементов поля называются псевдослучайными последовательностями?
11. Какие существуют требования при шифровании в системе RSA?
12. Что такое хэш-функция и хэш-код и где они применяются?
13. В чем заключается «парадокс дня рождения»?
14. Где используется алгоритм хэширования SHA-1?
15. Что понимают под хэш-кодом?
16. Назовите основные свойства хэш-кода.
17. Какие программные компоненты входят в состав криптографической системы PGP?
18. На чем основана криптостойкость системы шифрования и электронной цифровой подписи по методу Эль-Гамаля?
19. Что такое электронная подпись?
20. Что понимают под комплексной системой защиты информации?

Структурный элемент компетенций «уметь»

1. Как найти НОД и НОК целых чисел?
2. Приведите пример вычета и сравнения чисел.
3. Приведите пример вычета и сравнения многочленов.
4. Как связан порядок примитивного элемента с числом элементов конечного поля и генерируемой последовательностью случайных элементов?
5. Сравните симметричную и асимметричную системы шифрования.
6. Какие способы упрощения и уменьшения числа вычислений применяют в системах криптографической защиты информации?
7. Какие задачи решает криптографическая система защиты информации PGP?
8. Как формируется цифровая подпись открытого ключа?
9. Для чего предназначены группы открытых ключей?
10. Какие алгоритмы шифрования используются в системе PGP?
11. В чем состоит основное отличие алгоритмов шифрования и цифровой подписи?
12. В чем заключается проверка электронной подписи и как она осуществляется?
13. В чем заключается проверка электронной подписи по Эль-Гамалю?
14. Определите число корней полинома в заданном поле.
15. Найдите двойственный многочлен.
16. Вычислить ассиметричный ключ по алгоритму RSA.
17. Вычислить ассиметричный ключ по алгоритму Эль-Гамаля.
18. Зашифровать и дешифровать сообщение длиной М по алгоритму RSA.
19. Зашифровать и дешифровать сообщение длиной М по алгоритму Эль-Гамаля.
20. Сформировать и проверить электронную подпись для сообщения длиной М по алгоритму Эль-Гамаля.

Структурный элемент компетенций «владеть»

1. Построить поле Галуа заданного размера.
2. Построить изоморфные поля.
3. Определить число элементов конечного поля и построить ключевую последовательность.
4. Определить число корней полинома?
5. Назовите и охарактеризуйте основные этапы формирования раундовых ключей.
6. Назовите и охарактеризуйте основные этапы шифрования текста по алгоритму AES.
7. Назовите и охарактеризуйте основные этапы дешифрования текста по алгоритму AES.
8. Чем определяется криптостойкость асимметричной системы шифрования RSA?
9. Поясните алгоритм работы криптосистемы RSA.
10. Чем определяется криптостойкость асимметричной системы шифрования по Эль-Гамалю?
11. Поясните алгоритм работы криптосистемы по Эль-Гамалю.
12. Какими особенностями обладает алгоритм хэширования SHA-1?
13. Поясните алгоритм хэширования SHA-1?
14. Поясните схему комплексной системы защиты информации.
15. Поясните алгоритм Диффи-Хеллмана формирования сеансового ключа.
16. Каким образом распространяются ключи в вычислительных сетях?
17. Какие функции выполняет электронная подпись?
18. Охарактеризуйте структуру цифрового сертификата
19. Охарактеризуйте виды ключей, поддерживающиеся криптографической системой PGP.
20. Охарактеризуйте основные функции системы PGP.

6.5 Примерный перечень вопросов и заданий к экзамену

Структурный элемент компетенций «знать»

1. Необходимость защиты информации.
2. Понятие информационной безопасности.
3. Понятие информации.
4. Ценность информации.
5. Важность информации и распределение её по уровням.
6. Права собственности на информацию.
7. Основные принципы защиты информации от несанкционированного доступа.
8. Основные предпосылки появления угроз безопасности информации.
9. Случайные и преднамеренные угрозы. Причины случайных воздействий.
10. Случайные и преднамеренные угрозы. Средства доступа к информации при преднамеренных угрозах.
11. Возможные способы действия нарушителя в сети передачи данных.
12. Понятия криптологии, криптографии, криптоанализа.
13. Основные методы контроля доступа, используемые в современных вычислительных системах и сетях.
14. Понятия шифрования и дешифрования данных.
15. Безопасность систем шифрования.
16. Категории вскрытия систем шифрования информации.
17. Понятие и свойства хэш-кода сообщения.
18. Требования к хэш-функции.
19. Понятие электронной подписи.
20. Понятие конечного поля и его основные свойства.
21. Понятие поля Галуа и его основные свойства.
22. Понятие ключа. Виды и характеристики ключей.

Структурный элемент компетенций «уметь»

1. Классификация угроз безопасности информации и их сравнительная характеристика с точки зрения наибольшего соответствия практическим потребностям создания систем защиты информации.
2. Классификация методов защиты информации.
3. Системы аутентификации, построенные по принципу "пользователь имеет". Преимущества и недостатки методов аутентификации пользователей пластиковых кредитных карточек, широко используемых в банковской сфере.
4. Основные характеристики устройств аутентификации. Сравните известные вам устройства по каждой из этих характеристик.
5. Симметричная система шифрования
6. Асимметричная система шифрования.
7. Симметричная система шифрования AES.
8. Шифрование сообщений по методу RSA.
9. Шифрование и дешифрование сообщений по методу Эль-Гамаля.
10. Формирование хэш-кода сообщения.
11. Схема формирования хэш-кода на основе итеративных процедур Майера – Матиаса и Дэвиса – Майера.
12. Связь электронной подписи и хэш-кода.
13. Формирование и проверка электронной цифровой подписи по алгоритму Эль-Гамаля.
14. Схемы криптографического закрытия данных.
15. Основные математические операции в конечном поле.
16. Связь числа и многочлена.

17. Примеры применения конечных полей.
18. Построение поля Галуа.
19. Построение изоморфных полей.
20. Способы и особенности генерации ключей.
21. Особенности и способы генерации симметричных ключей.
22. Особенности и способы генерации ассиметричных ключей.

Структурный элемент компетенций «владеть»

1. Проверка подлинности, целостности и неотрицание авторства.
2. Понятия идентификации и аутентификации пользователей. В чем разница между этими понятиями?
3. Охарактеризуйте основные методы контроля доступа, используемые в автоматизированных системах специального назначения.
4. Способы аутентификации. Какой из способов является, по-вашему, наиболее эффективным?
5. Схемы симметричного шифрования и дешифрования.
6. Алгоритмы шифрования с открытым ключом.
7. Схемы асимметричного шифрования и дешифрования.
8. Блочные шифры на основе стандарта AES.
9. Алгоритм формирования ключевого материала и раундовых ключей в системе шифрования AES.
10. Итеративная процедура формирования хэш-кода на основе алгоритма SH1.
11. Схема формирования и проверки электронной подписи.
12. Обобщенная схема шифрования информации.
13. Детальная схема шифрования.
14. Обмен ключами в системе PGP..
15. Обобщённая схема шифрования, формирования и проверки электронной подписи.
16. Детальная схема шифрования, формирования и проверки цифровой подписи. Подлинность и целостность сообщения.
17. Криптографическая система PGP.
18. Способы обмена ключевой информацией.
19. Система открытого распределения ключей Диффи-Хеллмана.
20. Основные математические операции в конечных полях.
21. Алгоритм Евклида и его роль в криптографии.
22. Правила построения ключевых последовательностей.

6.6 Примеры задач

Примеры задач по математическим основам криптографии.

1. Произвести генерацию псевдослучайного пространства ключей заданного для каждого студента объёма.
2. Решить задачу по нахождению наибольшего общего делителя (НОД) и наименьшего общего кратного (НОК) *n* чисел или многочленов. Для каждого студента конкретные числа или многочлены задаются индивидуально преподавателем. Величину НОК требуется найти двумя способами.
3. Решить задачу по нахождению вычета и сравнения многочленов по модулю числа или многочлена. Исходные данные задаёт преподаватель студентам индивидуально.
4. Найти обратное число в поле по модулю простого числа. Исходные данные задаются преподавателем индивидуально для каждого студента.

Примеры задач к разделу "Криптографические методы защиты информации"

1. Произвести шифрование и дешифрование текста по алгоритму Эль-Гамаля. Размер текста задается преподавателем индивидуально.

2. Произвести шифрование и дешифрование текста по алгоритму RSA на основе индивидуально разработанной программы. Вычислить ключи. Размер текста задается преподавателем индивидуально.

Примеры задач к разделу "Формирование и проверка электронной подписи"

1. Произвести хэширование сообщений по заданному преподавателем методу из 12 стойких алгоритмов. Длина сообщения до 64 бит, длина хэш-кода до 32 бит. Составить индивидуальные программы.

2. Произвести хэширование сообщений по протоколу SHA-1. Длина сообщения, функция преобразования, количество этапов и длина хэш-кода задаются преподавателем индивидуально. По усмотрению студентов хэширование может быть выполнено программными средствами.

3. Сформировать и проверить электронную подпись для сообщения по алгоритму Эль-Гамаля. Размер сообщения задается преподавателем индивидуально.

7. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях: учеб. пособие [Электронный ресурс] – Электронно-библиотечная система «Лань» – Москва: ДМК Пресс, 2012. – 592 с. – Режим доступа: https://e.lanbook.com/book/3032

2. Шаньгин, В.Ф. Информационная безопасность. [Электронный ресурс] : учеб. пособие – Электронно-библиотечная система «Лань» – М.: ДМК Пресс, 2014. – 702 с. – Режим доступа: http://e.lanbook.com/book/50578

3. Бобрышева Г.В. Защита информации в вычислительных сетях: Методические указания к лабораторным работам / Б.А. Савельев, Г.В. Бобрышева. – Пенза: Информационно издательский центр ПГУ, 2007.-102 с.

б) дополнительная литература:

1. Адаменко, М.В. Основы классической криптологии: секреты шифров и кодов. [Электронный ресурс] – Электронно-библиотечная система «Лань» – М.: ДМК Пресс, 2016. – 296 с. – Режим доступа: http://e.lanbook.com/book/82817

2. Бирюков, А.А. Информационная безопасность: защита и нападение. [Электронный ресурс] – Электронно-библиотечная система «Лань» – М.: ДМК Пресс, 2017. – 434 с. – Режим доступа: http://e.lanbook.com/book/93278

3. Петров, А.А. Компьютерная безопасность. Криптографические методы защиты. [Электронный ресурс] – Электронно-библиотечная система «Лань». – М.: ДМК Пресс, 2008. – 448 с. – Режим доступа: http://e.lanbook.com/book/3027

в) программное обеспечение и интернет ресурсы

1. Сайт «Море(!) аналитической информации. Библиотека on-line» – http://citforum.ru/

2. Сайт «Образовательный математический сайт Exponenta.ru» – http://old.exponenta.ru/

3. Сайт «Тренинги и обучение по продуктам MATLAB и Simulink» – https://matlab.ru/training/

8. Материально-техническое обеспечение дисциплины

Перечень специализированных аудиторий с указанием используемого в учебном процессе основного учебно-лабораторного оборудования, технических средств обучения и контроля:

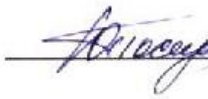
1. лекционные занятия проводятся в аудитории, оснащенной ноутбуком, компьютерным проектором с пультом дистанционного управления, проекционным экраном, шторами, сетью электропитания 220 В;
2. лабораторные занятия проводятся в компьютерном классе, оснащенном 12 персональными компьютерами, соединенных в локальную сеть, экраном дисплея с разрешением не менее 1024x758 и установленным на них программным продуктом Matlab.

Рабочая программа дисциплины «Защита информации» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 09.05.01 «Применение и эксплуатация автоматизированных систем специального назначения».

Программу составил:
к.т.н., доцент кафедры ИВС Бобрышева Галина Владимировна 

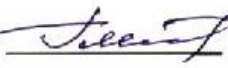
Программа одобрена на заседании кафедры «Информационно-вычислительные системы»
Программа одобрена на заседании кафедры «Информационно-вычислительные системы»

Протокол № 1 от «06» 09 2016 г.

Зав. кафедрой ИВС  Ю.Н. Косников

Программа одобрена методической комиссией факультета вычислительной техники

Протокол № 1 от «22» 09 2016 г.

Председатель методической комиссии ФВТ  Т.В.Глотова

Сведения о переутверждении программы на очередной учебный год и регистрации изменений

Учебный год	Решение кафедры (№ протокола, дата, подпись зав. кафедрой)	Внесенные изменения	Номера листов (страниц)		
			заменен-ных	новых	аннулиро-ванных
2017/2018	Прот. № 14 от 27.06.17	переутверждено без изменений			