

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ФАКУЛЬТЕТ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

УТВЕРЖДАЮ  
Декан ФВТ  
Л.Р. Фионова  
« 16 » июль 2015 г.



## РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

### Б1.2.13 Информационная безопасность

Направление подготовки – *09.03.03 Прикладная информатика*

Профиль подготовки – *Прикладная информатика в экономике*

Квалификация (степень) выпускника – *бакалавр*

Форма обучения – *очная*

г. Пенза, 2015 г.

## 1. Цели освоения дисциплины

Целями освоения дисциплины «Информационная безопасность» 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 стандартные задачи профессиональной деятельности по обеспечению информационной безопасности в вычислительных системах и сетях с учетом основных требований информационной безопасности, применением методов и средств защиты информации и современных информационно-коммуникационных технологий.

## 2. Место дисциплины в структуре ОПОП бакалавриата

Дисциплина «Информационная безопасность» относится к обязательным дисциплинам вариативной части ОПОП (Б1.2).

Изучение дисциплины базируется на знаниях, умениях и готовностях полученных студентами при изучении следующих дисциплин: «Математика», «Основы алгоритмизации и программирования», «Программирование на языках высокого уровня», «Вычислительные системы, сети и телекоммуникации».

Для успешного освоения дисциплины «Информационная безопасность» к «входным» знаниям, умениям и готовностям студентов предъявляются следующие требования: студенты должны владеть знаниями и умениями решения задач математического анализа и построения вычислительных систем и сетей, готовностью применения навыков, приобретенных в результате освоения предшествующих дисциплин, в решении задач защиты информации в вычислительных системах и сетях с применением современных программных средств разработки приложений.

Дисциплина является одной из заключительных в образовательной программе подготовки бакалавров по направлению «Прикладная информатика». Компетенции, приобретенные в ходе изучения дисциплины, готовят студента к выполнению выпускной квалификационной работы и могут быть использованы в профессиональной деятельности.

## 3. Компетенции обучающегося, формируемые в результате освоения дисциплины «Информационная безопасность»

Процесс изучения дисциплины 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-4	Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	<b>Знать:</b> теоретические и нормативно-правовые основы в области информационной безопасности, методы и средства защиты информации от несанкционированного доступа и вредоносных программ в вычислительных системах и сетях и информационно-коммуникационные технологии реализации их алгоритмов

		<p><b>Уметь:</b> профессионально грамотно использовать на практике нормативно-правовую документацию при организации защиты информации в вычислительных системах и сетях, обосновывать выбор методов и средств защиты информации от несанкционированного доступа и вредоносных программ и реализовывать их алгоритмы при решении стандартных задач профессиональной деятельности</p> <p><b>Владеть:</b> навыками организации защиты информации от несанкционированного доступа и вредоносных программ и навыками реализации основных методов и средств защиты информации при решении стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности</p>
ПК-6	Способность собирать детальную информацию для формализации требований пользователей заказчика	<p><b>Знать:</b> виды угроз и способы их предотвращения, основные требования информационной безопасности в вычислительных системах и сетях</p> <p><b>Уметь:</b> профессионально грамотно собирать детальную информацию по возможным угрозам, анализировать риск возникновения возможных угроз при передаче информации в вычислительных системах и сетях</p> <p><b>Владеть:</b> навыками формализации требований пользователей заказчика к защите информации в вычислительных системах и сетях</p>

## 4. Структура и содержание дисциплины

### 4.1. Структура дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единицы, 180 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					Собеседование	Коллоквиум	Проверка тестов	Проверка контролн. работ	Проверка реферата	Проверка эссе и иных творческих работ	курсовая работа (проект)	др.
				Всего	Лекции	Практические занятия	Лабораторные занятия	Всего	Подготовка к аудиторным занятиям	Реферат, эссе и др.	Курсовая работа (проект)	Подготовка к экзамену								
1	Раздел 1. Основы информационной безопасности	7	1-3	6	6	-	-	24	16	-	-	8	1-3	-	-	-	-	-	-	-
1.1	Тема 1.1. Основные понятия в области информационной безопасности	7	1	1	1	-	-	8	6	-	-	2	1	-	-	-	-	-	-	-
1.2	Тема 1.2. Правовые основы информационной безопасности	7	1	1	1	-	-	4	2	-	-	2	1	-	-	-	-	-	-	-
1.3	Тема 1.3. Угрозы при передаче и обработке информации	7	2	2	2	-	-	4	2	-	-	2	2	-	-	-	-	-	-	-
1.4	Тема 1.4. Методы и средства обеспечения информационной безопасности	7	3	2	2	-	-	8	6	-	-	2	3	-	-	-	-	-	-	-

2	Раздел 2. Криптографические методы защиты информации	7	4-9	36	12	-	24	36	26	-	-	10	4-9	-	-	-	-	-	-
2.1	Тема 2.1. Основные понятия в области криптографии	7	4	10	2	-	8	10	8	-	-	2	4	-	-	-	-	-	-
2.2	Тема 2.2. Симметричные системы шифрования	7	5,6	12	4	-	8	12	8	-	-	4	5,6	-	-	-	-	-	-
2.3	Тема 2.3. Асимметричные системы шифрования	7	7-9	14	6	-	8	14	10	-	-	4	7-9	-	-	-	-	-	-
3	Раздел 3. Формирование и проверка электронной подписи	7	10-14	22	10	-	12	22	14	-	-	8	10-14	-	-	-	-	-	-
3.1	Тема 3.1. Хэш-код сообщения	7	10, 11	8	4	-	4	10	6	-	-	4	10, 11	-	-	-	-	-	-
3.2	Тема 3.2. Электронная подпись	7	12-14	14	6	-	8	12	8	-	-	4	12-14	-	-	-	-	-	-
4	Раздел 4. Идентификация и аутентификация пользователей	7	15, 16	4	4	-	-	10	6	-	-	4	15, 16	-	-	-	-	-	-
4.1	Тема 4.1. Идентификация пользователей	7	15	1	1	-	-	3	2	-	-	1	15	-	-	-	-	-	-
4.2	Тема 4.2. Аутентификация пользователей	7	15, 16	3	3	-	-	7	4	-	-	3	15, 16	-	-	-	-	-	-
5	Раздел 5. Защита информации от вредоносных программ	7	17, 18	4	4	-	-	16	10	-	-	6	17, 18	-	-	-	-	-	-
5.1	Тема 5.1. Вредоносные программы	7	17	2	2	-	-	7	4	-	-	3	17	-	-	-	-	-	-
5.2	Тема 5.2. Способы и методы защиты информации от вредоносных программ	7	18	2	2	-	-	9	6	-	-	3	18	-	-	-	-	-	-
	<i>Подготовка к экзамену</i>	7										36							
	Общая трудоемкость, в часах			72	36	-	36	108	72	-	-	36	Промежуточная аттестация						
													Форма	Семестр					
														Зачет	-				
														Экзамен	7				

## 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, воздействие нарушителя в условиях взаимодействующих сетей, классификация угроз информации, понятие об активном и пассивном перехвате, методы криптоанализа, противодействия нападением 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 вычислительных системах и сетях, комплексные средства 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 асимметричного шифрования, алгоритмы асимметричного шифрования RSA и Эль-Гамала;

#### **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-Гамалу.

#### **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.

### 4.2.2. Перечень и содержание лабораторных занятий

№ п/п	№ разделов	Наименование лабораторных работ	Кол. ч
1	2	Математические операции в криптографических системах	4
2	2,3	Генерация ключевой последовательности	4
3	2	Криптографическая система защиты информации на основе стандарта AES (Rijndael)	8
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-Гамалу	4
7,8	2,3	Криптографическая система PGP 10.0	8
<b>Всего</b>			<b>36</b>

## 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](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](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 – 3	Основы информационной безопасности	Подготовка к аудиторным занятиям по темам лекционных занятий (см. п. 4.2.1), подготовка к экзамену	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	Учебно-методические материалы и электронные учебные материалы с сайта кафедры ИВС ( <a href="http://dep_ivs.pnzgu.ru">http://dep_ivs.pnzgu.ru</a> ) и файл-сервера кафедры ИВС (диск Т), основная и дополнительная литература	24
4 – 9	Криптографические методы защиты информации	Подготовка к аудиторным занятиям по темам лекционных занятий (см. п. 4.2.1) и лабораторных занятий (см. п. 4.2.2), подготовка к экзамену	Изучить: - основные понятия в области криптографии; - симметричные системы шифрования; - асимметричные системы шифрования	Учебно-методические материалы и электронные учебные материалы с сайта кафедры ИВС ( <a href="http://dep_ivs.pnzgu.ru">http://dep_ivs.pnzgu.ru</a> ) и файл-сервера кафедры ИВС (диск Т), основная и дополнительная литература	36
10 – 14	Формирование и проверка электронной подписи	Подготовка к аудиторным занятиям по темам лекционных занятий (см. п. 4.2.1) и лабораторных занятий (см. п. 4.2.2), подготовка к	Изучить: - понятие хэш-кода сообщения и основные алгоритмы его формирования; - понятие электронной подписи и основные алгоритмы ее	Учебно-методические материалы и электронные учебные материалы с сайта кафедры ИВС ( <a href="http://dep_ivs.pnzgu.ru">http://dep_ivs.pnzgu.ru</a> ) и файл-сервера кафедры ИВС (диск Т), основная и	22



		экзамену	формирования	дополнительная литература	
15,16	Идентификация и аутентификация пользователей	Подготовка к аудиторным занятиям по темам лекционных занятий (см. п. 4.2.1), подготовка к экзамену	Изучить: - понятие и методы идентификации пользователей; - понятие и методы аутентификации пользователей	Учебно-методические материалы и электронные учебные материалы с сайта кафедры ИВС ( <a href="http://dep_ivs.pnzgu.ru">http://dep_ivs.pnzgu.ru</a> ) и файл-сервера кафедры ИВС (диск Т), основная и дополнительная литература	10
17,18	Защита информации от вредоносных программ	Подготовка к аудиторным занятиям по темам лекционных занятий (см. п. 4.2.1), подготовка к экзамену	Изучить: - понятие вредоносная программа; - классификацию вредоносных программ, их функциональные возможности и наносимый ими ущерб; - способы и методы защиты информации от вредоносных программ	Учебно-методические материалы и электронные учебные материалы с сайта кафедры ИВС ( <a href="http://dep_ivs.pnzgu.ru">http://dep_ivs.pnzgu.ru</a> ) и файл-сервера кафедры ИВС (диск Т), основная и дополнительная литература	16

## 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](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 и реферата, контроль в форме теста	Разделы 1 – 5	ОПК-4, ПК-6
2	Промежуточный контроль: экзамен	Разделы 1 – 5	ОПК-4, ПК-6

### 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-Гамала?
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-Гамалу?
14. Определите число корней полинома в заданном поле.
15. Найдите двойственный многочлен.
16. Вычислить асимметричный ключ по алгоритму RSA.
17. Вычислить асимметричный ключ по алгоритму Эль-Гамала.
18. Зашифровать и дешифровать сообщение длиной  $M$  по алгоритму RSA.
19. Зашифровать и дешифровать сообщение длиной  $M$  по алгоритму Эль-Гамала.
20. Сформировать и проверить электронную подпись для сообщения длиной  $M$  по алгоритму Эль-Гамала.

### **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-Гамалу?
11. Поясните алгоритм работы криптосистемы по Эль-Гамалу.
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, поддерживаемые криптографической системой PGP.
20. Охарактеризуйте основные функции системы PGP.

## 6.5 Примерный перечень вопросов 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-Гамала.
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-Гамала.
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 Гауа.
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 SHA1.
  11. Схема формирования и проверки электронной подписи.
  12. Обобщенная схема шифрования информации.
  13. Детальная схема шифрования.
  14. Обмен ключами в системе PGP..
  15. Обобщенная 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-Гамала. 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-Гамала. 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](http://citforum.ru/). Библиотека on-line» – <http://citforum.ru/>
2. Сайт «[Образовательный математический сайт Exponenta.ru](http://old.exponenta.ru/)» – <http://old.exponenta.ru/>
3. Сайт «[Тренинги и обучение по продуктам MATLAB и Simulink](https://matlab.ru/training/)» – <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 установленными на них программным продуктом Matlab.

Рабочая программа дисциплины «Информационная безопасность» составлена в соответствии с требованиями ФГОС ВО по направлению 09.03.03 «Прикладная информатика».

Программу составил:  
1. к.т.н., доцент каф.ИВС



(подпись)

Г.В. Бобрышева

**Настоящая программа не может быть воспроизведена ни в какой форме без предварительного письменного разрешения кафедры-разработчика программы.**

Программа одобрена на заседании кафедры «Информационно-вычислительные системы»

Протокол № 10 от 15.06.2015 года

Зав. кафедрой ИВС



(подпись)

Ю.Н. Косников

Программа одобрена методической комиссией ФВТ

Протокол № 6 от «15» 06 2015 года

Председатель методической комиссии ФВТ



(подпись)

Н.Н. Коннов



**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)		
			замененных	новых	аннулированных
2016/ 2017	проб. № 11 от 22.06.2016 <i>[подпись]</i>	Внесены изменения исключения в 15 эбс	16, 17		
2017/ 2018	проб. № 14 от 26.06.17 <i>[подпись]</i>	переутверждено содержание			