МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ФАКУЛЬТЕТ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

УТВЕРЖДАЮ
Декан ФВТ
_____ Л.Р. Фионова
«___» _____ 2016 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 – *Академический бакалавр*

Форма обучения – *заочная*

Пенза, 2016

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», «Конечная математика и математическая логика», «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.

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	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-4).	**Знать:** теоретические и нормативно-правовые основы в области информационной безопасности, виды угроз и способы их предотвращения, основные требования информационной безопасности, методы и средства защиты информации от несанкционированного доступа и вредоносных программам в вычислительных системах и сетях и информационно-коммуникационные технологии реализации их алгоритмов

		Уметь: профессионально грамотно использовать на практике нормативно-правовую документацию при организации защиты информации в вычислительных системах и сетях, анализировать риск возникновения возможных угроз при передаче 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
		Владеть: 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

4. Структура и содержание дисциплины

4.1. Структура дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единицы, 180 часов

№ п/п	Наименование разделов дисциплины	Семестр	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)				Формы текущего контроля успеваемости *(по неделям семестра)*	
			Аудиторная работа			Самостоятель-ная работа	Проверка контрольных работ	
			Всего	Лекции	Лабораторн. занятия			
1	Раздел 1. Основы информационной безопасности	5	1	1		26	3	
2	Раздел 2. Криптографические методы защиты информации	5	7	1	6	26	6	
3	Раздел 3. Формирование и проверка электронной подписи	5	5	1	4	26	10	
4	Раздел 4. Идентификация и аутентификация пользователей	5	0,5	0,5		26	14	
5	Раздел 5. Защита информации от вредоносных программ	5	0,5	0,5		26	18	
	Подготовка к экзамену	5				*36*		
	Общая трудоемкость, в часах		14	4	10	166	Промежуточная аттестация	
							Форма	Семестр
							Экзамен	1

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 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 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 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.

4.2.2. Перечень и содержание лабораторных занятий

№ п/п	№ разделов	Наименование лабораторных работ	Кол. ч
1	2	Математические операции в криптографических системах	2
2	2,3	Генерация ключевой последовательности	2
3	2	Криптографическая система асимметричного шифрования RSA	2
4	3	Формирование хэш-кода сообщения на основе алгоритма SHA-1	2
5	2,3	Криптографическая система PGP 10.0	2

5. Образовательные технологии

5.1. Чтении лекций по дисциплине с использованием доски и мультимедийного компьютерного проектора и с применением программного продукта Microsoft Office Power Point.

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 с использованием средств разработки приложений, выбираемых обучаемыми самостоятельно, например, среда разработки приложений Delphi, C++, Matlab.

5.4. Выполнение лабораторного практикума исследовательского и проектного характера.

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

5.6. 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).

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), написание реферата, подготовка к 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. 2. Написать реферат на заданную тему	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 /2,3,4,5/ 3. Дополнительная литература /1/ 4. Программное обеспечение и интернет-ресурсы: /1/	26
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	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 /1,2,8,9,10/ 3. Дополнительная литература: /2,3/ 4. Программное обеспечение и интернет-ресурсы: /1,2,3/	26

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 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 /1,2,8,9,10/ 3. Дополнительная литература: /2,3/ 4. Программное обеспечение и интернет-ресурсы: /1,2,3/	26
15,16	Идентификация и аутентификация пользователей	Подготовка к аудиторным занятиям по темам лекционных занятий (см. п. 4.2.1), написание реферата, подготовка к экзамену	1. Изучить: - понятие и методы идентификации пользователей; - понятие и методы аутентификации пользователей. 2. Написать реферат на заданную тему	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 /2,3,6,7,9/ 3. Дополнительная литература: /2,3,4/ 4. Программное обеспечение и интернет-ресурсы: /1/	26
17,18	Защита информации от вредоносных программ	Подготовка к аудиторным занятиям по темам лекционных занятий (см. п. 4.2.1) и лабораторных занятий (см. п. 4.2.2), написание реферата,	1. Изучить: - понятие вредоносная программа; - классификацию вредоносных программ, их функциональные возможности и наносимый ими ущерб; - способы и	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	26

		подготовка к экзамену	методы защиты информации от вредоносных программ. 2. Написать реферат на заданную тему	литература /6,7,9/ 3. Дополнительная литература: /1,3,4/ 4. Программное обеспечение и интернет-ресурсы: /1/	

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 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 должны использоваться средства разработки приложений Delphi, C++, Matlab.

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

2. **Выполнение контрольной работы.** Контроль осуществляется во время сдачи контрольной работы. Подготовка контрольной работы должна включать изучение основной и дополнительной литературы, материала с интернет-ресурсов.

Контрольная работа должна содержать теоретические сведения по изученной теме, практические результаты и выводы.

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 и контрольной работы;

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 контрольной работы	Разделы 1 – 5	ОПК-4
2	Промежуточный контроль: экзамен	Разделы 1 – 5	ОПК-4

6.4 Вопросы для собеседования при защите лабораторных работ (примеры)

1. Дайте определение группы, кольца и поля.
2. Как найти НОД и НОК целых чисел?
3. Как найти НОД многочленов?
4. В чем различие и сходство операций над целыми числами и многочленами?
5. Что такое неприводимый многочлен?
6. Что такое простой многочлен?
7. В чём состоит сходство и отличие операций вычета и сравнения?
8. Какие основные характеристики имеют поля Галуа?
9. Что такое изоморфные поля случайных элементов?
10. Как найти двойственный многочлен?
11. Что такое неприводимый и приведенный многочлен?
12. Как связан порядок примитивного элемента с числом элементов конечного поля и генерируемой последовательностью случайных элементов?
13. Как определить число корней полинома?
14. Почему сгенерированные последовательности элементов поля называются псевдослучайными последовательностями?
15. Назовите и охарактеризуйте основные этапы формирования раундовых ключей.
16. Назовите и охарактеризуйте основные этапы шифрования текста по алгоритму AES.
17. Назовите и охарактеризуйте основные этапы дешифрования текста по алгоритму AES.
18. Сравните симметричную и асимметричную системы шифрования.
19. Чем определяется криптостойкость асимметричной системы шифрования RSA?
20. Охарактеризуйте алгоритм работы криптосистемы RSA.
21. Какие способы упрощения и уменьшения числа вычислений применяют в системах криптографической защиты информации?
22. Какие существуют требования при шифровании в системе RSA?
23. Что такое хэш-функция и хэш-код и где они применяются?
24. В чем заключается «парадокс дня рождения»?
25. Где используется алгоритм хэширования SHA-1?
26. Какими особенностями обладает алгоритм хэширования SHA-1?
27. Назовите основные свойства хэш-кода.
28. Какие задачи решает криптографическая система защиты информации PGP?
29. Какие программные компоненты входят в состав криптографической системы PGP?
30. Какие типы ключей поддерживаются криптографической системой PGP и в чем их различие?
31. Поясните алгоритм Диффи-Хеллмана формирования сеансового ключа.
32. Как формируется цифровая подпись открытого ключа?
33. Каким образом распространяются ключи в вычислительных сетях?
34. Для чего предназначены группы открытых ключей?
35. Какие алгоритмы шифрования файлов и сообщений электронной почты используются в системе PGP и чем они отличаются?
36. На чем основана криптостойкость системы шифрования и электронной цифровой подписи по методу Эль-Гамаля?
37. Что такое электронная цифровая подпись?
38. Какие функции выполняет электронная цифровая подпись?

39. В чем состоит основное отличие алгоритмов шифрования и цифровой подписи?

40. В чем заключается проверка цифровой подписи и как она осуществляется?

6.5 Примерный перечень тем контрольных работ

1. Развитие средств защиты информации. Роль защиты информации в организации производства и решении экономических задач
2. Криптология, криптография, криптоанализ
3. Понятие информационной безопасности, требования к защите данных и классификация методов и средств ее обеспечения
4. Обзор современных устройств защиты информации
5. Криптоанализ и классы криптоаналитического воздействия
6. Несанкционированные воздействия при передаче и обработке информации: воздействие нарушителя в условиях взаимодействующих сетей
7. Анализ угроз информации, хранящейся в базах данных автоматизированных систем. Средства и методы ее защиты
8. Анализ угроз информации, передаваемой по вычислительным сетям. Средства и методы ее защиты
9. Анализ угроз информации, передаваемой по сети Интернет. Средства и методы ее защиты
10. Случайные и преднамеренные угрозы и способы защиты от них
11. Активный и пассивный перехват и способы защиты
12. Криптоанализ шифрованных текстов. Методы криптоанализа и противодействие нападениям на защищенные сообщения
13. Современные методы защиты информации и их классификация
14. Средства защиты информации в вычислительных сетях: предотвращение раскрытия содержания информации и анализа потока
15. Идентификация пользователя. Методы идентификации пользователя
16. Аутентификация пользователей. Методы аутентификации пользователей
17. Аутентификация пользователей. Службы аутентификации: распределение ключей и аутентификация пользователей, распределение ключей и цифровые сертификаты
18. Протокол Kerberos
19. Криптосистемы. Стойкость криптосистем. Воздействия нарушителей на криптосистемы
20. Симметричные системы шифрования, схемы их реализации и их сравнительный анализ
21. Асимметричные системы шифрования и их сравнительный анализ
22. Поточные и блочные шифры: шифр с автоключом, шифры с шифрованным текстом в качестве автоключа (ШТАК)
23. Стандарт шифрования данных AES: принципы шифрования, алгоритм шифрования по стандарту AES и работа его в режимах шифрования и дешифрования
24. Криптосистема с ключом общего пользования RSA
25. Криптографическая система Эль-Гамаля
26. Электронная подпись: понятие, структура и области ее применения
27. Электронная подпись и алгоритмы ее реализации
28. Схема формирования электронной подписи по алгоритму Эль-Гамаля
29. Электронная подпись на основе стандарта ГОСТ Р 34.10-2012
30. Хэш-код сообщения и схемы формирования хэш-кода сообщения
31. Хэш-код сообщения и электронная подпись
32. Алгоритм формирования хэш-кода SHA1

33. Алгоритм формирования хэш-кода MD5
34. Обобщенная схема криптографического закрытия информации
35. Криптографическая система PGP
36. Методы защиты информации при реализации электронной торговли
37. Классификация вредоносных программ и вирусов. Способы и методы защиты информации от вредоносных программ и вирусов
38. Системы защиты информации в корпоративных автоматизированных сетях и перспективы их развития
39. Персональные данные, методы и средства их защиты
40. Политика безопасности компании в области информационной безопасности, методы и средства ее реализации

6.6 Примерный перечень вопросов и заданий к экзамену

1. Необходимость защиты информации. Понятие информационной безопасности.
2. Понятие информации. Ценность информации. Важность информации и распределение её по уровням. Права собственности на информацию.
3. Основные принципы защиты информации от несанкционированного доступа.
4. Классификация угроз безопасности информации и их сравнительная характеристика с точки зрения наибольшего соответствия практическим потребностям создания систем защиты информации.
5. Основные предпосылки появления угроз безопасности информации.
6. Случайные и преднамеренные угрозы. Причины случайных воздействий.
7. Случайные и преднамеренные угрозы. Средства доступа к информации при преднамеренных угрозах.
8. Возможные способы действия нарушителя в сети передачи данных.
9. Понятия криптологии, криптографии, криптоанализа.
10. Проверка подлинности, целостности и неотрицание авторства.
11. Классификация методов защиты информации.
12. Понятия идентификации и аутентификации пользователей. В чем разница между этими понятиями?
13. Способы аутентификации. Какой из этих способов является, по-вашему, наиболее эффективным?
14. Системы аутентификации, построенные по принципу "пользователь имеет". Преимущества и недостатки методов аутентификации пользователей пластиковых кредитных карточек, широко используемых в банковской сфере.
15. Основные характеристики устройств аутентификации. Сравните известные вам устройства по каждой из этих характеристик.

16. Основные методы контроля доступа, используемые в современных вычислительных системах и сетях. Охарактеризуйте данные методы и рассмотрите их возможности для реализации автоматизированной системы ведения текущих счетов клиентов банка.
17. Алгоритмы и ключи. Симметричные алгоритмы шифрования и алгоритмы шифрования с открытым ключом.
18. Понятия шифрования и дешифрования данных. Симметричная система шифрования. Схемы симметричного шифрования и дешифрования.
19. Понятия шифрования и дешифрования данных. Асимметричная система шифрования. Схемы асимметричного шифрования и дешифрования.
20. Безопасность систем шифрования. Категории вскрытия систем шифрования информации.

21. Блочные шифры на основе стандарта AES. Принципы шифрования и дешифрования. Основные параметры.

22. Симметричная система шифрования AES. Алгоритм формирования ключевого материала и раундовых ключей.

23. Шифрование сообщений по методу RSA. Основные параметры. Открытые и закрытые ключи. Алгоритмы шифрования и дешифрования.

24. Шифрование и дешифрование сообщений по методу Эль-Гамаля.

25. Понятие и свойства хэш-кода сообщения. Формирование хэш-кода сообщения. Требования к хэш-функции.

26. Понятие и свойства хэш-кода сообщения. Итеративная процедура формирования хэш-кода на основе алгоритма SH1.

27. Понятие и свойства хэш-кода сообщения. Схема формирования хэш-кода на основе итеративных процедур Майера – Матиаса и Дэвиса – Майера.

28. Понятие электронной цифровой подписи. Связь электронной цифровой подписи и хэш-кода. Схема формирования и проверки электронной цифровой подписи.

29. Формирование и проверка электронной цифровой подписи по алгоритму Эль-Гамаля. Основные параметры.

30. Схема криптографического закрытия данных. Обобщенная схема шифрования информации.

31. Детальная схема шифрования. Обмен ключами.

32. Обобщённая схема шифрования, формирования и проверки цифровой подписи.

33. Детальная схема шифрования, формирования и проверки цифровой подписи. Подлинность и целостность сообщения.

34. Понятие конечного поля и его основные свойства. Основные математические операции. Связь числа и многочлена. Примеры применения конечных полей.

35. Понятие поля Галуа и его основные свойства. Построение поля Галуа. Изоморфные поля.

36. Криптографическая система PGP.

37. Понятие ключа. Виды и характеристики ключей. Способы и особенности их генерации.

38. Понятие ключа. Виды и характеристики ключей. Способы обмена ключевой информацией.

39. Понятие ключа. Виды ассиметричных ключей. Особенности и способы генерации ассиметричных ключей.

40. Система открытого распределения ключей Диффи-Хеллмана.

6.7 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. Фороузан Б.А. Криптография и безопасность сетей: учеб. Пособие / Б.А. Фороузан. – М.: Интернет – Университет Информационных технологий: Бином. Лаборатория знаний, 2010. – 784 с.

2. Глухих, В.И. Информационная безопасность и защита данных: учебное пособие. – Иркутск: Изд-во Иркутского гос. техн. ун-та, 2012 - 244 с.

3. Заводцев И.В. Программно-аппаратные средства обеспечения информационной безопасности / И.В. Заводцев, В.А. Кучер, В.Н. Хализев. – Краснодар : Кубанский гос. технологический ун-т , 2013 - 235 с.

4. Кабанов А.С. Основы информационной безопасности: учебное пособие / А. С. Кабанов, А.Б. Лось, В.И. Трунцев – М.: Московский гос. ин-т электроники и математики , 2012 - 162 с.

5. Правовые основы информационной безопасности: учебное пособие по дисциплине «Информационное право» / Н.М. Кожуханов, Е.С. Недосекова – М.: Изд-во Российской таможенной акад., 2013 - 87 с.

6. Мазаник С. Безопасность компьютера: защита от сбоев, вирусов и неисправностей / С. Мазаник. – М.: Эксмо-Пресс, 2014. – 240 с.

7. Мельников Д.А. Информационная безопасность открытых систем. – М.: Флинта, 2014. – 350 с.

8. Платонов В.В. Программно-аппаратные средства защиты информации: учебник для студентов высших учебных заведений, обучающихся по направлению подготовки "Информационная безопасность"/В.В. Платонов. – М.: Академия, 2013 – 330 с.

9. Петровский, В.В. Комплексная защита информации на предприятии: методы и способы противодействия средствам технических разведок: учебное пособие / В.В. Петровский, В.И. Петровский, В.И. Глова – Казань : Изд-во Казанского гос. технического ун-та , 2012 - 626 с.

10. Бобрышева Г.В. Информационная безопасность: Методические указания к лабораторным работам / Б.А. Савельев, Г.В. Бобрышева. – Пенза: Информационно издательский центр ПГУ, 2012.-102 с.

б) дополнительная литература:

1. Колеров, И.С. Основы информационной безопасности : учебное пособие – Иркутск: Изд-во ИГУ , 2013 - 113 с.

2. Барабанова М.И., Кияев В.И. Информационные технологии: открытые системы, сети, безопасность в системах и сетях: : Учебное пособие. – СПб.: Изд-во СПбГУЭФ, 2010. – 270 с.

3. Партыка Т.П., Попов И.И. Информационная безопасность. – М:, ФОРУМ, 2010. – 432 с.

4. Васильев, Ю.С. Перспективные направления научных исследований в области информационной безопасности :по материалам диссертационных работ / Ю. С. Васильев ; М-во образования и науки Российской Федерации, Санкт-Петербургский гос. политехнический ун-т. – Санкт-Петербург: Изд-во Политехнического ун-та , 2012 - 130 с.

в) программное обеспечение и Интернет-ресурсы

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

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

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

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, с процессором Pentium-4, оперативной памятью не менее 1024 Мб, памятью винчестера не менее 40 Гб, экраном дисплея с разрешением не менее 1024x758 и установленными на них средами программирования: Delphi, C++, Matlab.

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

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

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 № 1 от «6» 09 2016 года

Зав. кафедрой ИВС _____ Косников Ю. Н.

Программа одобрена методической комиссией факультета вычислительной техники

Протокол № 1 от «22» 09 2016 года

Председатель методической комиссии ФВТ _____ Глотова Т. В.

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