МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ФАКУЛЬТЕТ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

М1.1.8 Оценка и обеспечение информационной безопасности

Направление подготовки – *09.04.03 Прикладная информатика*

Магистерская программа – *Прикладная информатика в экономике*

Квалификация (степень) выпускника – *магистр*

Форма обучения – *очная*

г. Пенза, 2015 г.

1. Цели освоения дисциплины

Целями освоения дисциплины (модуля) «Оценка и обеспечение информационной безопасности» является подготовка магистрантов к использованию предусмотренных нормативными документами и стандартами методов и средств оценки качества, надежности и обеспечения информационной безопасности с использованием современного электронного оборудования в процессе разработки и эксплуатации прикладных информационных систем (ИС).

2. Место дисциплины в структуре ООП ВО

Дисциплина «Оценка и обеспечение информационной безопасности» относится к дисциплинам базовой части ОПОП (М 1.1).

Изучение дисциплины базируется на знаниях, умениях и готовностях, полученных студентами в процессе изучения дисциплины бакалавриата «Информационная безопасность».

Для успешного освоения дисциплины «Оценка и обеспечение информационной безопасности» к «входным» знаниям, умениям и готовностям студентов предъявляются следующие требования: студенты должны владеть знаниями основных понятий в области информационной безопасности и теоретических основ реализации основных методов обеспечения информационной безопасности в компьютерных системах и сетях и умениями применять их на практике; готовностью применения навыков, приобретенных в результате освоения дисциплины «Информационная безопасность», в решении задач защиты информации в компьютерных системах и сетях с применением современных программных средств разработки приложений и современного электронного оборудования.

Дисциплина является одной из заключительных в образовательной программе подготовки магистрантов. Компетенции, приобретенные в ходе изучения данной дисциплины, готовят магистранта к освоению профессиональных компетенций и могут быть использованы при выполнении выпускной магистерской работы.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

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)
1	2	3
ОПК-6	способность к профессиональной эксплуатации современного электронного оборудования в соответствии с целями основной образовательной программы магистратуры	**Знать:** современное электронное оборудование, применяемое для обеспечения требуемого уровня информационной безопасности в прикладных ИС
		Уметь: учитывать и применять современное электронное оборудование при организации работ по обеспечению информационной безопасности в прикладных ИС в процессе их разработки и эксплуатации
		Владеть: навыками обеспечения информационной безопасности прикладных ИС в процессе профессиональной эксплуатации современного электронного оборудования

ПК-21	способность использовать передовые методы оценки качества, надежности и информационной безопасности ИС в процессе эксплуатации прикладных ИС	**Знать:** теоретические основы организации работы по обеспечению информационной безопасности ИС и КС в процессе их эксплуатации; действующие нормативные документы и стандарты на методы и средства организации защиты информации в прикладных ИС, передовые методы оценки качества, надежности и информационной безопасности ИС, особенности их реализации посредством современных компьютерных технологий
		Уметь: учитывать нормативные документы и стандарты на методы и средства защиты информации, передовые методы оценки качества, надежности и информационной безопасности при организации работ по обеспечению информационной безопасности прикладных ИС в процессе их разработки и эксплуатации
		Владеть: навыками реализации алгоритмов передовых методов и средств организации защиты информации в прикладных ИС, методов оценки качества, надежности и информационной безопасности ИС с использованием языков программирования высокого уровня

4. Структура и содержание дисциплины
4.1. Структура дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы, 144 часа

№ 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 контрольн. работ	Проверка реферата	Проверка эссе и иных творческих работ	курсовая работа (проект)	др.
1	Раздел 1. Правовые и нормативные документы по информационной безопасности	3	1	2	2	-	-	6	2	-	-	4	1,2	-	-	-	-	-	-	-
2	Раздел 2. Хэширование сообщений	3	3,5	16	4	-	12	22	8	-	-	8	3–6	-	-	-	-	-	-	-
3	Раздел 3. Электронная подпись	3	7,9	16	4	-	12	26	10	-	-	10	7–10	-	-	-	-	-	-	-
4	Раздел 4. Защита информации в прикладных информационных системах	3	11,13	16	4	-	12	22	8	-	-	8	11 – 14	-	-	-	-	-	-	-
5	Раздел 5. Защита информации в глобальных компьютерных сетях	3	15,17	4	4	-	-	14	2	-	-	6	15 – 18	-	-	-	-	-	-	-
	Подготовка к экзамену	3										36								
	Общая трудоемкость, в часах			54	18	-	36	90	30			36	Промежуточная аттестация							
													Форма			Семестр				
													Зачет			3				
													Экзамен			3				

4.2. Содержание дисциплины

4.2.1. Содержание лекционного курса

Раздел 1. Правовые и нормативные документы по информационной безопасности

Тема 1.1. Роль стандартизации и нормативных документов при организации защиты информации в информационных системах

Тема 1.2. Закон о государственной тайне. Сведения, относимые к государственной тайне. Засекречивание и рассекречивание сведений и носителей информации. Распоряжения о сведениях, составляющих государственную тайну

Тема 1.3. Закон РФ "Об информации, информационных технологиях и защите информации". Информационные ресурсы и документирование информации. Информатизация, информационные системы, технологии и средства их обеспечения и права собственности на них. Сертификация информационных систем и технологий. Защита информации и прав субъектов информационных ресурсов

Тема 1.4. Закон РФ "О правовой охране программ для ЭВМ и баз данных". Объект правовой защиты, авторское право на базу данных. Авторские права, авторство и личные права. Имущественные права, право на регистрацию. Защита прав на программные продукты и базы данных

Раздел 2. Хэширование сообщений

Тема 2.1. Понятие и свойства хэш-кода сообщения

Тема 2.2. Хэширование сообщений и учётных данных пользователей

Тема 2.3. Схема формирования хэш-кода на основе итеративных процедур Майера – Матиаса и Дэвиса – Майера

Тема 2.4. Итеративная процедура формирования хэш-кода на основе алгоритмов SHA-1

Тема 2.5. Хэширования сообщений по ГОСТ Р.34.11-2012

Раздел 3. Электронная подпись

Тема 3.1. Электронные подписи на основе ассиметричных систем шифрования

Тема 3.2. Электронная подпись по алгоритму Эль-Гамаля

Тема 3.3. Математические основы электронной подписи на основе эллиптических кривых

Тема 3.4. Электронная подпись на основе ГОСТ Р 34.10-2012

Тема 3.5. Электронная подпись на платёжных документах

Раздел 4. Защита информации в прикладных информационных системах и компьютерных сетях

Тема 4.1. Принципы и способы аутентификации в информационных системах

Тема 4.2. Аутентификация пользователей информационных систем на основе биометрических параметров

Тема 4.3. Аутентификация пользователей информационных систем на основе симметричных и асимметричных систем шифрования

Тема 4.4. Протоколы аутентификации в информационных системах

Тема 4.5. Службы аутентификации учетных данных пользователей в информационных системах и распределения ключей

Тема 4.6. Методы и средства контроля доступа в информационных системах

Тема 4.7. Типы комбинаций защищенных связей в информационных системах и компьютерных сетях и их характеристики

Тема 4.8. Комплексные криптографические системы защиты информации

Раздел 5. Защита информации в глобальных компьютерных сетях

Тема 5.1. Частные сети и защищенный протокол IPSec в сети Internet

Тема 5.2. Проблемы защиты в сети WWW (WEB)

Тема 5.3. Угроза нарушения защиты в глобальной сети

Тема 5.4. Протоколы защиты SSL и TLS. Протоколы изменения параметров шифрования, извещения, квитирования

Тема 5.5. Защита информации с помощью брандмауэров

Тема 5.6. Безопасность электронных платёжных систем

Тема 5.7. Состояние и тенденции развития криптографических средств защиты информации в информационных системах

4.2.2. Перечень и содержание лабораторных занятий

№ п/п	№ разделов	Наименование лабораторных работ	Кол. ч
1	2	Формирование хэш-кода сообщения на основе алгоритма SHA	6
2	3	Математические операции на эллиптических кривых	4
3	2,3	Алгоритм формирования хэш-кода по стандарту ГОСТ Р.34.11-2012	4
4	3	Формирование электронной подписи на основе стандарта ГОСТ Р.34.10-2012	6
5	4	Комплексная защита информации по Эль-Гамалю и RSA	6
6	2	Генерация ключей для шифрования на основе стандарта ГОСТ Р 28147-89	4
7	2,4	Криптографическая система шифрования информации на основе стандарта ГОСТ Р 28147-89	6
Всего			**36**

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	Раздел 1. Правовые и нормативные документы по информационной безопасности	Подготовка к аудиторным занятиям по темам лекционных занятий (см. п. 4.2.1), к зачету и экзамену	Изучить правовые и нормативные основы обеспечения информационной безопасности и действующие законы РФ организации защиты информации в прикладных ИС	Учебно-методические материалы и электронные учебные материалы с сайта кафедры ИВС (http://dep_ivs.pnzgu.ru) и файл-сервера кафедры ИВС (диск Т), основная и дополнительная литература	6
2	Раздел 2. Хэширование сообщений	Подготовка к аудиторным занятиям по темам лекционных занятий (см. п. 4.2.1), к зачету и экзамену	Изучить принципы хэширования сообщений и учетных данных пользователей и алгоритмы его реализации	Учебно-методические материалы и электронные учебные материалы с сайта кафедры ИВС (http://dep_ivs.pnzgu.ru) и файл-сервера кафедры ИВС (диск Т), основная и дополнительная литература	22
3	Раздел 3. Электронная подпись	Подготовка к аудиторным занятиям по темам лекционных занятий (см. п. 4.2.1), к зачету и экзамену	Изучить структуру и математические основы электронной подписи и алгоритмы ее формирования и проверки	Учебно-методические материалы и электронные учебные материалы с сайта кафедры ИВС (http://dep_ivs.pnzgu.ru) и файл-сервера кафедры ИВС (диск Т), основная и дополнительная литература	26

4	Раздел 4. Защита информации в прикладных информационных системах	Подготовка к аудиторным занятиям по темам лекционных занятий (см. п. 4.2.1) и к зачету	Изучить принципы и виды аутентификации пользователей, криптографические методы и средства обеспечения защиты информации в информационных системах	Учебно-методические материалы и электронные учебные материалы с сайта кафедры ИВС (http://dep_ivs.pnzgu.ru) и файл-сервера кафедры ИВС (диск Т), Основная и дополнительная литература	22
5	Раздел 5. Защита информации в глобальных компьютерных сетях	Подготовка к аудиторным занятиям по темам лекционных занятий (см. п. 4.2.1), к зачету и экзамену	Изучить организацию защиты информации в глобальных компьютерных сетях	Учебно-методические материалы и электронные учебные материалы с сайта кафедры ИВС (http://dep_ivs.pnzgu.ru) и файл-сервера кафедры ИВС (диск Т), Основная и дополнительная литература	14
Всего					**90**

6.2. Методические указания по организации самостоятельной работы студентов

Каждый магистрант 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 производится во время выполнения и сдачи лабораторных работ.

Подготовка к лабораторным работам должна включать изучение математических операций, применяемых 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 остаточных знаний магистрантов 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-6, ПК-21
2	Промежуточный контроль: зачет, экзамен	Разделы 1 – 5	ОПК-6, ПК-21

6.4. Вопросы для собеседования при защите лабораторных работ (примеры)

Структурный элемент компетенций «знать»

1. Дайте определение эллиптической кривой.
2. Какие требования предъявляются к секретным ключам?
3. Что такое пространство ключей и как оно определяется?
4. Что такое изоморфные поля случайных элементов?
5. Какую роль выполняет синхропосылка в режиме «шифрование по методу гаммирование»?
6. Какие математические операции используются при шифровании?
7. Назовите способы доставки синхропосылки на приемную сторону, их достоинства и недостатки.
8. Является ли процесс дешифрования симметричным по отношению к шифрованию?
9. Какие существуют требования при шифровании по ГОСТ Р 28147-89?
10. Что такое хэш-функция и хэш-код и где они применяются?
11. В чем заключается «парадокс дня рождения»?
12. Назовите основные свойства хэш-кода.
13. Что такое генерирующая точка?
14. На чем основана криптостойкость электронной подписи по ГОСТ Р 34.10-2012?
15. Кто является владельцем ключей при формировании и проверке электронной подписи?
16. Как влияет изменение одного символа сообщения на электронную подпись?
17. Как влияет изменение одного символа ключа проверки подписи на дешифрование сообщения?
18. Что такое электронная подпись?

Структурный элемент компетенций «уметь»

1. Какие преимущества шифрования на эллиптических кривых?
2. Как определить порядок эллиптической кривой?
3. Назовите и охарактеризуйте основные этапы формирования раундовых ключей.
4. Опишите работу рекуррентного генератора последовательности чисел.
5. Назовите и охарактеризуйте виды преобразований основного шага криптопреобразований.
6. Назовите основные этапы цикла шифрования в режиме гаммирования.
7. Охарактеризуйте основные отличия использования цикловых ключей для дешифрования от процессов использования ключей при шифровании.
8. Какие операции преобразований используются при дешифровании?
9. Какие способы упрощения и уменьшения числа вычислений применяют в системах криптографической защиты информации?
10. Какими особенностями обладает алгоритм хэширования по ГОСТ Р 34.11-2012?
11. Что представляет из себя итеративная процедура формирования хэш-кода по ГОСТ Р 34.11-2012?
12. В чем преимущество электронной подписи на эллиптических кривых по сравнению с другими электронными подписями, например, с электронной подписью по алгоритму Эль-Гамаля?
13. Пояснить алгоритм формирования электронной подписи по ГОСТ Р 34.10-2012.
14. Объяснить один шаг преобразования, используемого при формировании хэш-кода для электронной подписи.
15. Как найти ключ проверки электронной подписи?
16. В чем заключается разница алгоритмов шифрования и дешифрования, формирования и проверки электронной подписи?
17. Чем определяется криптостойкость симметричных и асимметричных систем шифрования?
18. Какие функции обеспечения информационной безопасности выполняет современное электронное оборудование?

Структурный элемент компетенций «владеть»

1. Как получить дискретные точки на эллиптической кривой?
2. Каким образом удвоить точку эллиптической кривой?
3. Как по двум точкам эллиптической кривой определить третью точку?
4. Чем отличается режим шифрования от режима дешифрования?
5. Сравните симметричную и асимметричную системы шифрования.
6. Назовите и охарактеризуйте основные этапы дешифрования текста в режиме гаммирования.
7. Где используется алгоритм хэширования по ГОСТ Р 34.11-2012?
8. Какие основные преобразования осуществляются в алгоритме хэширования по ГОСТ Р 34.11-2012?
9. Как вычислить ключи для формирования и проверки электронной подписи по ГОСТ Р 34.10-2012?
10. Как формируется электронная подпись по ГОСТ Р 34.10-2012?
11. Какие задачи решает электронная подпись?
12. Назовите основные операции преобразования, которые используются при формировании электронной подписи по ГОСТ Р 34.10-2012.
13. Назовите основные операции преобразований, используемые при проверке электронной подписи.
14. Поясните алгоритм проверки электронной подписи.

15. Какие функции выполняет электронная подпись?

16. В чем состоит основное отличие алгоритмов шифрования и электронной подписи?

17. В чем заключается проверка электронной подписи и как она осуществляется?

18. Какие задачи решают криптографические системы защиты информации?

6.5. Примерный перечень вопросов и заданий к экзамену

Структурный элемент компетенций «знать»

1. Роль стандартизации и нормативных документов при организации защиты информации в прикладных ИС и компьютерных сетях.
2. Необходимость защиты информации. Закон о государственной тайне.
3. Сведения и носители информации, относимые к государственной тайне.
4. Информационные ресурсы и документирование информации. Права собственности на информацию.
5. Закон РФ "Об информации, информационных технологиях и защите информации".
6. Защита информации и прав субъектов информационных ресурсов.
7. Информатизация, информационные системы, технологии и средства их обеспечения и права собственности на них.
8. Закон РФ "О правовой охране программ для ЭВМ и баз данных”.
9. Объект правовой защиты, авторское право на базу данных.
10. Авторские права, авторство и личные права.
11. Имущественные права, право на регистрацию.
12. Понятие хэширования сообщений и учётных данных пользователей.
13. Понятия идентификации и аутентификации пользователей. В чем разница между этими понятиями?
14. Электронная подпись на платёжных документах.
15. Математические основы электронной подписи с помощью эллиптических кривых.
16. Услуги по защите информации на уровне IP.
17. Формат заголовков при аутентификации и шифровании и описание его основных полей. Форматы кадров IPv4 и IPv6.
18. Типы комбинаций защищенных связей и их характеристики.
19. Понятие брандмауэра и принципы его работы. Конфигурация брандмауэров.
20. Управление доступом к данным в компьютерной сети.

Структурный элемент компетенций «уметь»

1. Сертификация информационных систем и технологий.
2. Защита прав на программные продукты и базы данных.
3. Способы аутентификации. Какой из этих способов является, по-вашему, наиболее эффективным?
4. Системы аутентификации, построенные по принципу "пользователь имеет". Преимущества и недостатки методов аутентификации пользователей пластиковых кредитных карточек, широко используемых в банковской сфере.
5. Основные характеристики устройств аутентификации. Сравните известные вам устройства по каждой из этих характеристик.
6. Безопасность систем шифрования. Категории вскрытия систем шифрования информации.
7. Понятие и свойства хэш-кода сообщения. Формирование хэш-кода сообщения. Требования к хэш-функции.
8. Понятие и свойства хэш-кода сообщения. Итеративная процедура

формирования хэш-кода на основе алгоритма SH1.

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

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

11. Схема криптографического закрытия данных. Обмен ключами.

12. Обобщённая схема шифрования, формирования и проверки электронной подписи.

13. Организация защиты информации на сетевом уровне модели OSI.

14. Организация защиты информации на уровне IP.

15. Аутентификация и шифрование информации на уровне IP.

16. Транспортный и туннельный режимы защиты.

17. Комплексные криптографические системы защиты информации.

18. Безопасность электронных платёжных систем.

19. Состояние и тенденции развития криптографических средств защиты информации в компьютерных сетях.

20. Основные характеристики устройств аутентификации. Сравните известные вам устройства по каждой из этих характеристик.

Структурный элемент компетенций «владеть»

1. Алгоритм хэширования сообщений по ГОСТ Р.34.11–2012.
2. Алгоритм хэширования сообщений по алгоритму SHA1.
3. Аутентификация на основе симметричных и асимметричных систем шифрования.
4. Аутентификация и идентификация на основе биометрических параметров.
5. Службы аутентификации учетных данных пользователей в базах данных и распределения ключей.
6. Основные методы контроля доступа, используемые в современных вычислительных системах и сетях. Охарактеризуйте данные методы и рассмотрите их возможности для реализации распределенных информационных систем.
7. Алгоритмы и ключи. Симметричные алгоритмы шифрования и алгоритмы шифрования с открытым ключом.
8. Понятия шифрования и дешифрования данных. Симметричная система шифрования. Схемы симметричного шифрования и дешифрования.
9. Понятия шифрования и дешифрования данных. Асимметричная система шифрования. Схемы асимметричного шифрования и дешифрования.
10. Шифрование и дешифрование сообщений по методу Эль-Гамаля.
11. Формирование и проверка электронной подписи по алгоритму Эль-Гамаля. Основные параметры.
12. Электронная подпись на основе ассиметричных систем шифрования.
13. Электронная подпись на основе ГОСТ Р 34.10-2012.
14. Электронная подпись по методу Эль-Гамаля.
15. Частные сети и защищенный протокол IPSec в сети Internet.
16. Проблемы защиты в сети WWW (WEB).
17. Классификация угроз нарушения защиты в глобальной сети.
18. Протоколы защиты SSL и TLS.
19. Протоколы изменения параметров шифрования, извещения, квитирования.
20. Организация защиты от вредоносных программ в компьютерных сетях.

6.6. Примеры задач

Примеры задач по математическим основам криптографии.

1. Произвести генерацию псевдослучайного пространства ключей заданного объёма. Исходные данные задаются преподавателем индивидуально для каждого студента.

2. Решить задачу по нахождению наибольшего общего делителя (НОД) и наименьшего общего кратного (НОК) *n* чисел или многочленов. Исходные данные задаются преподавателем индивидуально для каждого студента.

3. Решить задачу по нахождению вычета и сравнения чисел или многочленов по модулю числа или многочлена. Исходные данные задаются преподавателем индивидуально для каждого студента.

4. Найти обратное число в поле по модулю простого числа. Исходные данные задаются преподавателем индивидуально для каждого студента.

Примеры задач к разделу "Хэширование сообщений"

1. Произвести хэширование сообщения по ГОСТ Р 34.11-2012. Длина сообщения до 64 бит. Разработать и протестировать программу.

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

Примеры задач к разделу "Электронная подпись"

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

2. Сформировать электронную подпись по алгоритму ГОСТ Р 34.10-2012. Длина подписи 32 и 64 бита.

3. Сравнить характеристики электронных подписей, полученных по ГОСТ Р 34.10-2012 и SHA-1.

Примеры задач по шифрованию и дешифрованию сообщений

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

2. Произвести шифрование и дешифрование текста по алгоритму RSA. Размер текста задается преподавателем индивидуально для каждого студента.

3. Вычислить ключи для криптографического закрытия сообщений по алгоритму Эль-Гамаля и RSA и сравнить их параметры. Размер сообщения задается преподавателем индивидуально для каждого студента.

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. Информационная безопасность: Методические указания к лабораторным работам / Б.А. Савельев, Г.В. Бобрышева. – Пенза: Издательство ПГУ, 2012.- 64 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 «Оценка и обеспечение информационной безопасности» составлена в соответствии с требованиями ФГОС ВО по направлению 09.04.03 «Прикладная информатика».

Программу составил:

1. к.т.н., доцент каф. ИВС _____ Г.В. Бобрышева

(подпись)

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 № 7 от 09.02.2015 года

Зав. кафедрой ИВС _____ Ю.Н. Косников

(подпись)

Программа одобрена методической комиссией ФВТ

Протокол № 4 от «13» 02 2015 года

Председатель методической комиссии ФВТ _____ Н.Н. Коннов

(подпись)

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
2016/2017	Прот. № 11 от 22.06.16	Внесены информ. изменения из ЭБС	4, 16		
2017/2018	Протокол № 14 от 22.06.2017	Переутверждено без изменений			