МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ФАКУЛЬТЕТ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

УТВЕРЖДАЮ
Декан ФВТ
_____ Л.Р. Фионова
«03» июня 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

М1.В.02 ОЦЕНКА И ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление подготовки - *09.04.03 «Прикладная информатика»*

Направленность (магистерская программа) - *«Прикладная информатика в экономике»*

Квалификация выпускника – *магистр*

Форма обучения – *очная*

Пенза, 2019

1. Цели освоения дисциплины

Целями освоения дисциплины «Оценка и обеспечение информационной безопасности» является формирование и развитие у обучающихся профессиональных компетенций, формирование системы знаний, умений и навыков использования предусмотренных нормативными документами и стандартами методов и средств оценки качества, надежности и обеспечения информационной безопасности в процессе разработки и эксплуатации прикладных информационных систем.

2. Место дисциплины в структуре ООП ВО

Дисциплина «Оценка и обеспечение информационной безопасности» относится к части ОПОП (М1.В), формируемой участниками образовательных отношений.

Изучение дисциплины базируется на знаниях, умениях и готовностях, полученных в процессе изучения дисциплин образовательной программы бакалавриата по направлению подготовки 09.03.03 «Прикладная информатика».

Для успешного освоения дисциплины «Оценка и обеспечение информационной безопасности» к «входным» знаниям, умениям и готовностям 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; навыками решения задач защиты информации в компьютерных системах и сетях с применением современных программных средств разработки приложений.

Компетенции, приобретенные в ходе изучения дисциплины, могут быть использованы при выполнении магистерской диссертации и в профессиональной деятельности.

3. Результаты освоения дисциплины «Оценка и обеспечение информационной безопасности»

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

Коды компетенции	Наименование компетенции	Индикатор достижения компетенции	В результате освоения дисциплины обучающийся должен:
ПК-1	Способность использовать передовые методы оценки качества, надежности и информационной безопасности экономических информационных систем в процессе их эксплуатации	ПК-1.1. Понимает методы и приемы, организационно-технологической поддержки процессов обеспечения информационной безопасности, надежности, качества выполнения работ при создании и эксплуатации прикладных экономических информационных систем	**Знать:** теоретические основы и методы обеспечения информационной безопасности, надежности, качества прикладных экономических информационных систем **Уметь:** профессионально грамотно определять требуемый уровень обеспечения информационной безопасности прикладных экономических информационных систем
		ПК-1.2. Производит анализ и выбор средств для решения задач обеспечения и контроля качества, обеспечения информационной	**Знать:** современные технологии прикладной информатики для решения задач обеспечения, обеспечения информационной безопасности экономических информационных систем

		безопасности, управления рисками при создании и эксплуатации прикладных экономических информационных систем	**Уметь:** профессионально грамотно проводить анализ и выбор современных методов и технологий прикладной информатики для решения задач обеспечения информационной безопасности при создании и эксплуатации прикладных экономических информационных систем
		ПК-1.3. Применяет в практике проектирования и эксплуатации прикладных экономических информационных систем современные приемы и меры для обеспечения информационной безопасности, надежности, качества выполнения работ	**Знать:** современные приемы и меры обеспечения информационной безопасности при создании и эксплуатации прикладных экономических информационных систем, виды рисков информационной безопасности **Уметь:** профессионально грамотно выявлять потенциальные риски информационной безопасности и определять соответствующие меры по их предупреждению, устанавливать права доступа к файлам и папкам, разрабатывать документацию на прикладные экономические информационных системы с учетом требований к обеспечению информационной безопасности **Владеть:** навыками обеспечения информационной безопасности прикладных экономических информационных систем и управления потенциальными рисками

4. Структура и содержание дисциплины

4.1. Структура дисциплины

Общая трудоемкость дисциплины составляет 6 зачетных единиц, 216 часов

№ п/п	Наименование разделов и тем дисциплины (модуля)	Семестр	Недели семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)									Формы текущего контроля успеваемости *(по неделям семестра)*							
				Аудиторная работа				Самостоятельная работа												
				Всего	Лекции	Практические занятия	Лабораторные занятия	Всего	Подготовка к аудиторным занятиям	Реферат, эссе и др.	Курсовая работа (проект)	Подготовка к экзамену	Собеседование	Коллоквиум	Проверка тестов	Проверка 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	6		8	3–6							
3	Раздел 3. Электронная подпись	3	7,9	16	4		12	26	10	6		10	7–10							
4	Раздел 4. Защита информации в прикладных информационных системах и компьютерных сетях	3	11,13	16	4		12	22	8	6		8	11 – 14							
5	Раздел 5. Защита информации в глобальных компьютерных сетях	3	15,17	4	4			14	2	6		6	15 – 18		18		18			
	Подготовка к экзамену	3										36								
	Общая трудоемкость, в часах			89, 95	34		51	90,0 5	30	24		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 компьютерных сетях

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 распределенных информационных системах и компьютерных сетях

Тема 4.2. Аутентификация пользователей распределенных информационных систем и компьютерных сетей на основе биометрических параметров

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

Тема 4.4. Протоколы аутентификации в распределенных информационных системах и компьютерных сетях

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

Тема 4.6. Методы контроля доступа в распределенных информационных системах и компьютерных сетях

Тема 4.7. Типы комбинаций защищенных связей в распределенных 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 компьютерных сетях

4.2.2. Перечень и содержание лабораторных занятий

№ п/п	№ разделов	Наименование лабораторных работ	Кол. ч
1	2	Формирование хэш-кода сообщения на основе алгоритмов SHA-1	8
2	3	Математические операции на эллиптических кривых	6
3	2,3	Алгоритм формирования хэш-кода по стандарту ГОСТ Р.34.11-2012	6
4	3	Формирование электронной подписи на основе стандарта ГОСТ Р.34.10-2012	8
5	4	Комплексная защита информации по Эль-Гамалю и RSA	8
6	2	Генерация ключей для шифрования на основе стандарта ГОСТ Р 28147-89	5
7	2,4	Криптографическая система шифрования информации на основе стандарта ГОСТ Р 28147-89	8

5. Образовательные технологии

В ходе освоения дисциплины «Оценка и обеспечение информационной безопасности» при проведении аудиторных занятий используется образовательная технология, предусматривающая такие методы и формы изучения материала как лекция и лабораторное занятие, включающие активные и интерактивные формы занятий:

1. чтение лекций по дисциплине проводится с использованием доски и мультимедийного компьютерного проектора и с применением пакета Microsoft Office Power Point;
2. при изучении материалов лабораторного практикума используются образовательные материалы, программное обеспечение и информационные ресурсы с сайта кафедры ИВС (http://dep_ivs.pnzgu.ru) и файл-сервера кафедры ИВС (диск Т);
3. при выполнении лабораторного практикума используются средства разработки приложений, выбираемые обучаемыми самостоятельно, например, среда разработки приложений Delphi, C++, Matlab;
4. чтение лекций с проблемной постановкой темы;
5. лабораторные занятия носят исследовательский и проектный характер;
6. выполнение индивидуальных заданий теоретического плана (исследование алгоритмов преобразований, применяемых при шифровании, дешифровании, электронной подписи и её проверки на криптостойкость и быстродействие) с последующим интерактивным обсуждением;

7. при самостоятельной работе используются образовательные материалы, программное обеспечение и информационные ресурсы с сайта кафедры ИВС (http://dep_ivs.pnzgu.ru) и файл-сервера кафедры ИВС (диск Т);

8. образовательные технологии сочетаются с внеаудиторной работой с целью формирования и развития профессиональных навыков студентов. В частности, рекомендуются встречи студентов с представителями Пензенских IT-компаний, посвященных обсуждению вопросов состояния и перспектив развития и использования методов, средств и систем защиты информации в прикладных ИС и компьютерных сетях.

Занятия, проводимые в интерактивной форме составляют 25 % от общего количества аудиторных занятий.

Самостоятельная работа студентов подразумевает работу под руководством преподавателя (консультации, помощь в написании и отладке программ и др.) и индивидуальную работу студента, выполняемую как дома, так и в компьютерном классе с выходом в сеть Интернет.

При реализации образовательных технологий используются следующие виды самостоятельной работы:

- работа с конспектом лекции и литературой;
- подготовка к лабораторной работе: изучение теоретического материала, разработка и отладка программ заданий по лабораторным работам;
- обработка результатов лабораторных работ и подготовка письменных отчетов;
- выполнение и оформление курсового проекта: изучение теоретического материала, разработка структуры базы данных и алгоритма решения задачи, реализация базы данных, разработка и отладка программ, оформление пояснительной записки курсового проекта;
- поиск информации в сети Интернет и литературе;
- подготовка к сдаче лабораторных работ и индивидуальных заданий;
- подготовка к сдаче зачёта и экзамена.

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	Подготовка к аудиторным занятиям по темам лекционных занятий (см. п. 4.2.1), экзамену и зачету	Изучить правовые и нормативные основы обеспечения информационной безопасности и действующие законы РФ организации защиты информации в прикладных ИС и 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	6

2	Раздел 2	Подготовка к аудиторным занятиям по темам лекционных занятий (см. п. 4.2.1), экзамену и зачету	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	Подготовка к аудиторным занятиям по темам лекционных занятий (см. п. 4.2.1), экзамену и зачету	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	Подготовка к аудиторным занятиям по темам лекционных занятий (см. п. 4.2.1), экзамену и зачету	Изучить принципы и виды аутентификации пользователей, криптографические методы и средства обеспечения защиты информации в распределенных информационных системах и 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	22
5	Раздел 5	Подготовка к аудиторным занятиям по темам лекционных занятий (см. п. 4.2.1), экзамену и зачету	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

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. Контроль осуществляется в начале каждый лекции в виде экспресс-опроса. Для понимания материала лекции необходимо изучить вопросы предшествующей лекции по лекциям и основной литературе и познакомиться с дополнительной литературой, выполнить задания, даваемые преподавателем на лекции (30 часов).

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

Результатом лабораторных работ являются 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 тестирования и собеседования при защите лабораторных работ и реферата;

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, тестирование	Разделы 1 – 5	ПК-1
2	Промежуточный контроль: зачет, экзамен	Разделы 1 – 5	ПК-1

6.4 Варианты электронных тестовых заданий (примеры)

По разделу "Правовые и нормативные документы по информационной безопасности"

1. Вопрос:

С чем связано появление закона о защите информации?

Варианты ответов:

- частыми кражами информации;
- опасностью модификации и искажения информации;
- необходимости защиты прав собственности на информацию.

2. Вопрос:

Какие Вы знаете правовые средства защиты информации в компьютерных сетях?

Варианты ответов**:**

- законы РФ;
- защита информации с помощью преобразований;
- засекречивание информации и их носителей;
- защита прав субъектов информационных ресурсов.

По разделу "Хэширование сообщений"

1. Вопрос: Для чего генерируется хэш-код сообщения?

Варианты ответов:

- уменьшения длины сообщения,
- уменьшения вероятности появления коллизий,
- увеличения достоверности подписи,
- экономии вычислительных ресурсов при формировании и проверки электронной подписи.

2. Вопрос: Какие особенности формирования хэш-кода на основе алгоритма SH1?

Варианты ответов:

- использование элементарных функций;
- циклическая обработка сообщения;
- использование констант;
- получение хэш-кода размером 256 бит.

По разделу "Электронная подпись"

1. Вопрос: Для чего необходима электронная подпись?

Варианты ответов:

- защиты передаваемой по компьютерной сети информации от модификации;
- защиты передаваемой по компьютерной сети информации от раскрытия содержания сообщения;
- обеспечения подлинности, целостности и невозможности отрицания авторства.

2. Вопрос: В чём основное отличие электронной подписи от подписи на бумажном носителе?

Варианты ответов:

- применением операций шифрования и дешифрования;
- операцией «подписывания»;
- видом подписи.

По разделу "Защита информации в прикладных информационных системах и компьютерных сетях"

1. Вопрос: Какой способ надёжно защищает личные данные пользователя в распределенных информационных системах и компьютерных сетях от кражи?

Варианты ответов:

- физическая защита;
- шифрование личных данных;
- хэширование личных данных.

2. Вопрос: Что представляет собой стратегия генерации одноразовых паролей?

Варианты ответов:

- случайно произнесенная фраза;
- пароль, подвергнутый хэшированию;
- генерация паролей на основе объединения базового пароля (секрета) с показаниями часов или счётчиков.

3. Вопрос: На чём основана криптостойкость асимметричной системы шифрования?

Варианты ответов:

- на сложности разложения составного ключа на простые сомножители;
- сложности алгоритма преобразования при шифровании;
- на размере шифруемого сообщения.

По разделу "Защита информации в глобальных компьютерных сетях "

1. Вопрос: Какие режимы защиты информации используются в глобальных компьютерных сетях?

Варианты ответов:

- защита на основе асимметричной системы шифрования,
- транспортный режим защиты,
- туннельный режим защиты.

2. Вопрос: Какие основные средства защиты информации в глобальных компьютерных сетях?

Варианты ответов:

- физическая защита каналов связи,
- защита информации с помощью преобразований,
- криптографическая защита на основе ключа.

3. Вопрос: Что защищает компьютерную сеть от вторжений из сети Internet?

Варианты ответов:

- физические средства защиты информации,
- брандмауэры и мосты,
- электронная цифровая подпись.

4. Вопрос: Что обеспечивает брандмауэр?

Варианты ответов:

- блокирование не запрошенных входящих соединений;
- защиту компьютера от атак хакеров, проникновения вредоносных программ;
- аутентификацию пользователей.

6.5 Вопросы для собеседования при защите лабораторных работ (примеры)

1. Дайте определение эллиптической кривой.
2. Какие преимущества шифрования на эллиптических кривых?
3. Как получить дискретные точки на эллиптической кривой?
4. Каким образом удвоить точку эллиптической кривой?
5. Как по двум точкам эллиптической кривой определить третью точку?
6. Как определить порядок эллиптической кривой?
7. Назовите и охарактеризуйте основные этапы формирования раундовых ключей.
8. Опишите работу рекуррентного генератора последовательности чисел
9. Какие требования предъявляются к секретным ключам?
10. Что такое пространство ключей и как оно определяется?
11. Что такое изоморфные поля случайных элементов?
12. Какую роль выполняет синхропосылка в режиме «шифрование по методу гаммирование»?
13. Назовите и охарактеризуйте виды преобразований основного шага криптопреобразований.
14. Назовите основные этапы цикла шифрования в режиме гаммирования.
15. Какие математические операции используются при шифровании?
16. Назовите способы доставки синхропосылки на приемную сторону, их достоинства и недостатки.
17. Чем отличается режим шифрования от режима дешифрования?
18. Охарактеризуйте основные отличия использования цикловых ключей для дешифрования от процессов использования ключей при шифровании.
19. Сравните симметричную и асимметричную системы шифрования.
20. Назовите и охарактеризуйте основные этапы дешифрования текста в режиме гаммирования.

21. Является ли процесс дешифрования симметричным по отношению к шифрованию?

22. Какие операции преобразований используются при дешифровании?

23. Какие способы упрощения и уменьшения числа вычислений применяют в системах криптографической защиты информации?

24. Какие существуют требования при шифровании по ГОСТ Р 28147-89?

25. Что такое хэш-функция и хэш-код и где они применяются?

26. В чем заключается «парадокс дня рождения»?

27. Назовите основные свойства хэш-кода.

28. Где используется алгоритм хэширования по ГОСТ Р 34.11-2012?

29. Какими особенностями обладает алгоритм хэширования по ГОСТ Р 34.11-2012?

30. Что представляет из себя итеративная процедура формирования хэш-кода по ГОСТ Р 34.11-2012?

31. Какие основные преобразования осуществляются в алгоритме хэширования по ГОСТ Р 34.11-2012?

32. Как вычислить ключи для формирования и проверки электронной подписи по ГОСТ Р 34.10-2012?

33. Как формируется электронная подпись по ГОСТ Р 34.10-2012?

34. Что такое генерирующая точка?

35. Какие задачи решает электронная подпись?

36. В чем преимущество электронной подписи на эллиптических кривых по сравнению с другими электронными подписями, например, с электронной подписью по алгоритму Эль-Гамаля?

37. На чем основана криптостойкость электронной подписи по ГОСТ Р 34.10-2012?

38. Назовите основные операции преобразования, которые используются при формировании электронной подписи по ГОСТ Р 34.10-2012.

39. Пояснить алгоритм формирования электронной подписи по ГОСТ Р 34.10-2012.

40. Объяснить один шаг преобразования, используемого при формировании хэш-кода для электронной подписи.

41. Как найти ключ проверки электронной подписи?

42. Кто является владельцем ключей при формировании и проверке электронной подписи?

43. Назовите основные операции преобразований, используемые при проверке электронной подписи.

44. Поясните алгоритм проверки электронной подписи.

45. Как влияет изменение одного символа сообщения на электронную подпись?

46. Как влияет изменение одного символа ключа проверки подписи на дешифрование сообщения?

47. Что такое электронная подпись?

48. Какие функции выполняет электронная цифровая подпись?

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

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

6.6 Примерный перечень вопросов и заданий к зачету и экзамену

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. Сертификация информационных систем и технологий.

7. Защита информации и прав субъектов информационных ресурсов.

8. Информатизация, информационные системы, технологии и средства их обеспечения и права собственности на них.

9. Закон РФ "О правовой охране программ для ЭВМ и баз данных".

10. Объект правовой защиты, авторское право на базу данных.

11. Авторские права, авторство и личные права.

12. Имущественные права, право на регистрацию.

13. Защита прав на программные продукты и базы данных.

14. Понятие хэширования сообщений и учётных данных пользователей.

15. Алгоритм хэширования сообщений по ГОСТ Р.34.11–2012.

16. Алгоритм хэширования сообщений по алгоритму SHA1.

17. Понятия идентификации и аутентификации пользователей. В чем разница между этими понятиями?

18. Способы аутентификации. Какой из этих способов является, по-вашему, наиболее эффективным?

19. Аутентификация на основе симметричных и асимметричных систем шифрования.

20. Аутентификация и идентификация на основе биометрических параметров.

21. Службы аутентификации учетных данных пользователей в базах данных и распределения ключей.

22. Системы аутентификации, построенные по принципу "пользователь имеет". Преимущества и недостатки методов аутентификации пользователей пластиковых кредитных карточек, широко используемых в банковской сфере.

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

24. Основные методы контроля доступа, используемые в современных вычислительных системах и сетях. Охарактеризуйте данные методы и рассмотрите их возможности для реализации распределенных информационных систем.

25. Алгоритмы и ключи. Симметричные алгоритмы шифрования и алгоритмы шифрования с открытым ключом.

26. Понятия шифрования и дешифрования данных. Симметричная система шифрования. Схемы симметричного шифрования и дешифрования.

27. Понятия шифрования и дешифрования данных. Асимметричная система шифрования. Схемы асимметричного шифрования и дешифрования.

28. Безопасность систем шифрования. Категории вскрытия систем шифрования информации.

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

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

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

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

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

34. Формирование и проверка электронной подписи по алгоритму Эль-Гамаля.

35. Схема криптографического закрытия данных. Обмен ключами.
36. Обобщённая схема шифрования, формирования и проверки электронной подписи.
37. Электронная подпись на платёжных документах.
38. Математические основы электронной подписи с помощью эллиптических кривых.
39. Электронная подпись на основе ассиметричных систем шифрования.
40. Электронная подпись на основе ГОСТ Р 34.10-2012.
41. Электронная подпись по методу Эль-Гамаля.
42. Организация защиты информации на сетевом уровне модели OSI.
43. Организация защиты информации на уровне IP.
44. Услуги по защите информации на уровне IP.
45. Аутентификация и шифрование информации на уровне IP.
46. Транспортный и туннельный режимы защиты.
47. Формат заголовков при аутентификации и шифровании и описание его основных полей. Форматы кадров IPv4 и IPv6.
48. Типы комбинаций защищенных связей и их характеристики.
49. Комплексные криптографические системы защиты информации.
50. Безопасность электронных платёжных систем.
51. Частные сети и защищенный протокол IPSec в сети Internet.
52. Проблемы защиты в сети WWW (WEB).
53. Классификация угроз нарушения защиты в глобальной сети.
54. Протоколы защиты SSL и TLS.
55. Протоколы изменения параметров шифрования, извещения, квитирования.
56. Понятие брандмауэра и принципы его работы.
57. Конфигурация брандмауэров.
58. Управление доступом к данным в компьютерной сети.
59. Организация защиты от вредоносных программ в компьютерных сетях.
60. Состояние и тенденции развития криптографических средств защиты информации в компьютерных сетях.

6.7 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 - 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 материально-техническое обеспечение дисциплины «Оценка и обеспечение информационной безопасности»

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) **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

г) **программное обеспечение**:

1. среды программирования: *Delphi*, *C++*, *Matlab*;

2. графический редактор *Microsoft Office Visio*;

3. программный продукт *Microsoft Office PowerPoint*.

д) **другое материально-техническое обеспечение**

Все лабораторные работы выполняются на персональных компьютерах.

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;

3. рабочие места в компьютерном классе имеют выход в сеть Internet;

4. на персональных компьютерах установлены среды программирования *Delphi*, *C++*, *Matlab*, графический редактор *Microsoft Office Visio*, программный продукт *Microsoft Office PowerPoint*.

Рабочая программа дисциплины «Оценка и обеспечение информационной безопасности» составлена в соответствии с требованиями ФГОС ВО - магистратура по направлению подготовки 09.04.03 «Прикладная информатика», утвержденного приказом Министерства образования и науки Российской Федерации от «19» сентября 2017 г. № 916.

Программу составил:
к.т.н., доцент Бобрышева Г.В.

Программа одобрена на заседании кафедры «Информационно-вычислительные системы»

Протокол № 12 от «02» мая 2019 года

Зав. кафедрой ИВС Бобрышева Г.В.

Программа одобрена методической комиссией факультета вычислительной техники

Протокол № 10 от «03» мая 2019 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)	Внесенные изменения	Подпись зав. кафедрой