МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

«СОГЛАСОВАНО»
Руководитель ОП

_____ Добржинский Ю.В
(подпись) (Ф.И.О.)

«УТВЕРЖДАЮ»
И.о. заведующего кафедрой
информационной безопасности

_____ Добржинский Ю.В
(подпись) (Ф.И.О.)

«_15_» _____июня_____2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Дополнительные главы криптографических протоколов
Специальность 10.05.01 Компьютерная безопасность
(Математические методы защиты информации)
Форма подготовки очная

курс ___5____ семестр ____10____
лекции _36__ час.
практические занятия____36___час.
лабораторные работы_______час.
в том числе с использованием МАО лек.__9___/пр.___00__/лаб.__00___ час.
в том числе в электронной форме лек.__00___/пр.__00___/лаб.__00___ час.
всего часов аудиторной нагрузки____72____ час.
в том числе с использованием МАО ___9__ час.
в том числе в электронной форме __00__час.
самостоятельная работа ____36_____ час.
в том числе на подготовку к экзамену ___00___ час.
курсовая работа / курсовой проект не предусмотрены
зачет _____10_____ семестр
экзамен не предусмотрен

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования, утвержденного приказом Министерства образования и науки РФ от 01.12.2016 № 1512

Рабочая программа обсуждена на заседании кафедры информационной безопасности
протокол № __10__ от «__15__» _____июня_____2019 г.

И.о. заведующего кафедрой: Добржинский Ю.В., к.т.н., с.н.с.
Составитель (ли): Боршевников А.Е. Ассистент

Владивосток
2019

Оборотная сторона титульного листа РПД

I. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

II. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

III. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

IV. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

ABSTRACT

Specialist's degree in 10.05.01 Computer Security

Specialization "Mathematical Methods for Information Security"

Course title: *Additional chapters of cryptographic protocols*

Variable part of Block 1, 4 credits

Instructor: *Borshevnikov A.E.*

At the beginning of the course a student should be able to:

• *the ability to apply research methodology in professional activities, including in the work on interdisciplinary and innovative projects (OPK-4);*

• *the ability to use regulatory legal documents in their professional activities (OPK-5).*

Learning outcomes:

(PC-5) the ability to participate in the development and configuration of software and hardware information security tools, including protected operating systems, database management systems, computer networks, anti-virus protection systems, cryptographic information protection tools

(PC-10) the ability to assess the effectiveness of the implementation of information protection systems and existing security policies in computer systems, including protected operating systems, database management systems, computer networks, anti-virus protection systems, cryptographic information protection tools.

Course description:

Discipline is a continuation of the course "Theory of Probability and Mathematical Statistics". As part of this course, it is proposed to consider such sections of it as queuing theory and game theory. At the time of studying the discipline, a student should have the ability to differentiate and integrate, have an understanding of the basic concepts of mathematical analysis and the theory of functions of a complex variable, possess matrix algebra, and be able to work with spreadsheets.

Main course literature:

1. Шаньгин, В.Ф. Защита компьютерной информации: учебное пособие / В.Ф. Шаньгин — Москва : ДМК Пресс, 2010. — 544 с. — Режим доступа: https://e.lanbook.com/book/1122

2. Кукина, Е.Г. Введение в криптографию: сборник задач и упражнений / Е.Г. Кукина, В.А. Романьков — Омск : ОмГУ, 2013. — 91 с. — Режим доступа: https://e.lanbook.com/book/75394

3. Рябко, Б.Я. Основы современной криптографии и стеганографии: монография / Б.Я. Рябко, А.Н. Фионов — Москва : Горячая линия-Телеком, 2011. — 232 с. — Режим доступа: https://e.lanbook.com/book/5192

Form of final knowledge control: *pass-fail exam.*

Аннотация к рабочей программе дисциплины «Дополнительные главы криптографических протоколов»

Рабочая программа учебной дисциплины «Дополнительные главы криптографических протоколов» разработана для студентов 5 курса специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав обязательных дисциплин вариативной части учебного плана с кодом Б1.В.ОД.3.

Трудоёмкость дисциплины в зачетных единицах составляет 3 з.е., в академических часах – 108 часов. Учебным планом предусмотрены лекционные занятия – 36 часов, практические занятия – 36 часов, самостоятельная работа студента – 36 часов. Дисциплина реализуется на 5 курсе в А семестре. Форма контроля по дисциплине – зачет.

Изучение дисциплины базируется на курсах: «Криптографические методы защиты информации», «Криптографические протоколы». Дисциплина «Дополнительные главы криптографических протоколов» обеспечивает приобретение знаний и умений в области использования криптографических протоколов для защиты информации. Изучение этой дисциплины способствует освоению принципов применения совершенных информационных технологий, содействует формированию мировоззрения и развитию системного мышления.

Дисциплина является продолжением курса «Теория вероятностей и математическая статистика». В рамках этого курса предлагается рассмотреть такие его разделы, как теория массового обслуживания и теория игр. На

момент изучения дисциплины студент должен обладать умением дифференцировать и интегрировать, иметь понимание основных концепций математического анализа и теории функций комплексного переменного, владеть матричной алгеброй, уметь работать с электронными таблицами.

Цель дисциплины - углубленное изложение принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике.

Задачи:

- дать общие представления об эллиптических кривых над конечными полями,
- изучить криптографических особенностях применения интеллектуальных картах и специфических криптографических протоколах.

Для успешного изучения дисциплины «Дополнительные главы криптографических протоколов» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-4);
- способность использовать нормативные правовые документы в своей профессиональной деятельности (ОПК-5).

В результате изучения данной дисциплины у обучающихся формируются следующие профессиональные компетенции (элементы компетенций):

Код и формулировка компетенции	**Этапы формирования компетенции**	
(ПК-5) способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных,	Знает	защитные механизмы и средства обеспечения безопасности операционных систем, средства и методы хранения и передачи аутентификационной информации, требования к подсистеме аудита и политике аудита, основные средства и методы анализа программных реализаций.
	Умеет	формулировать и настраивать политику

компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации		безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе, корректно применять симметричные и асимметричные криптографические алгоритмы.
	Владеет	навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств, навыками анализа программных реализаций.
(ПК-10) способность оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	Знает	основные виды симметричных и асимметричных криптографических алгоритмов, защитные механизмы и средства обеспечения безопасности операционных систем, средства и методы хранения и передачи аутентификационной информации, требования к подсистеме аудита и политике аудита. Основные средства и методы анализа программных реализаций.
	Умеет	использовать средства защиты, предоставляемые системами управления базами данных, осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты. Применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях.
	Владеет	методиками анализа сетевого трафика, методиками анализа результатов работы средств обнаружения вторжений, навыками конфигурирования локальных компьютерных сетей, реализации сетевых протоколов с помощью программных средств, навыками настройки межсетевых экранов.

Для формирования вышеуказанных компетенций в рамках дисциплины «Дополнительные главы криптографических протоколов» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: конспект (ПР-7), собеседование (ОУ-1), коллоквиум (ОУ-2).

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Раздел I. Стандарты на цифровую подпись и функцию хеширования (10 час.)

Тема 1. Введение в теорию эллиптических кривых (3 час.)

Понятие эллиптической кривой. Сингулярные и несингулярные кривые. Сложение точек эллиптической кривой. Понятие дискриминанта и j-инварианта ЭК. Построение кривой с заданным j-инвариантом.

Тема 2. Стандарты на цифровую подпись (3 час.)

Понятие цифровой подписи. Схемы ЦП семейства Эль-Гамаля. Российский стандарт ЭЦП - ГОСТ 34.10-2001: параметры, алгоритм вычисления ЦП, алгоритм верификации ЦП. Американский стандарт ЭЦП – DSS. DSA. EC DSA, параметры алгоритма, используемые поля и кривые.

Тема 3. Стандарты на функции хэширования (4 час.)

Ключевые и бесключевые функции хеширования. Одношаговая сжимающая функция. Российский стандарт хеш-функции - ГОСТ Р 34.11-94, алгоритм одношаговой сжимающей функции, процедура вычисления результирующего хэша. Американский стандарт хеш-функции – SHS. SHA – подготовка текста, главный цикл алгоритма. SHA-256, SHA-384, SHA-512: отличия от алгоритма SHA.

Раздел II. Специфические криптографические протоколы (8 час.)

Тема 1. Специфические подписи (3 час.)

Мультиподпись. Групповая подпись, свойства, простейший вариант. Групповая подпись с затемненными открытыми ключами. Полностью слепые подписи, реализация на базе RSA. Слепая подпись, свойства, 2 варианта протоколов, виды мошенничества. Неотрицаемая цифровая подпись.

Тема 2. Специфические протоколы (3 час.)

Совместная подпись контракта. Протокол рассеянной передачи. Протокол подбрасывания честной монеты: вариант с однонаправленной функцией; вариант квадратных корней; вариант возведения в степень. Квантовая криптография.

Тема 3. Безопасные выборы (2 час.)

Безопасные выборы. Свойства идеального протокола. Возможные схемы. Голосование со слепыми подписями. Голосование с Центральными Комиссиями. Голосование с анонимным распределением регистрационных номеров.

Раздел III. Практические криптографические протоколы (12 час.)

Тема 1. Общие понятия (4 час.)

Уровни защиты данных в каналах связи. Практические криптопротоколы. Виртуальные частные сети. Протоколы PPTP, SSL/TLS, IPSec, SSH, SET, PGP.

Тема 2. Протокол SSL (4 час.)

2 уровня подпротоколов. Протокол записи. Протокол извещения. Протокол изменения параметров шифрования. Протокол квитирования. Схема работы протокола квитирования. Используемые криптопримитивы.

Тема 3. Протокол IPSec (4 час.)

Области применения IPSec. Документы IPSec.Транспортный и туннельный режимы. Протокол AH. Протокол ESP. Управление ключами. Протоколы ISAKMP и Oakley.

Раздел IV. Особенности применения криптографических алгоритмов на ИК (6 час).

Тема 1. Особенности применения криптографических алгоритмов на ИК. (3 час.)

Причины специфики криптоалгоритмов на ИК. Особенности алгоритмов шифрования. Специфика схем: аутентификации, цифровой подписи, управления ключами. Криптографические примитивы и криптографические протоколы по защите информации. Специальные алгоритмы и протоколы, включающие криптографические механизмы.

Тема 2. Аутентификация на интеллектуальных картах. (3 час.)

Задачи аутентификации. Логическая аутентификация. Протокол внутренней логической аутентификации. Протокол внешней логической аутентификации. Биометрическая аутентификация.

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Практические занятия (36 час.)

Занятие 1. Изучение стандартов на цифровую подпись и функцию хеширования (12 час.)

1. Стандарты на цифровую подпись.
2. Стандарты на функции хэширования.

Занятие 2. Изучение специфических криптографических протоколов (12 час.)

1. Специфические подписи.

2. Специфические протоколы.

Занятие 3 Изучение практических криптографических протоколов (12 час.)

1. Протокол SSL
2. Протокол IPSec

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Дополнительные главы криптографических протоколов» представлено в Приложении 1 и включает в себя:

план-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию;

характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;

требования к представлению и оформлению результатов самостоятельной работы;

критерии оценки выполнения самостоятельной работы

IV. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства - наименование	
				текущий контроль	промежуточная аттестация
1	Раздел I. Стандарты на цифровую подпись и функцию хеширования	ПК-5, ПК-10	знает	Конспект (ПР-7)	1-9
			умеет	Собеседование (ОУ-1)	1-9
			владеет	Собеседование (ОУ-1)	1-9
2	Раздел II. Специфические криптографические протоколы	ПК-5, ПК-10	знает	Конспект (ПР-7)	10-19
			умеет	Собеседование (ОУ-1)	10-19
			владеет	Собеседование (ОУ-1)	10-19
3	Раздел III. Практические криптографические	ПК-5, ПК-10	знает	Конспект (ПР-7)	20-28
			умеет	Собеседование (ОУ-1)	20-28

	протоколы		владеет	Собеседование (ОУ-1)	20-28
4	Раздел IV. Особенности применения криптографических алгоритмов на ИК	ПК-5, ПК-10	знает	Конспект (ПР-7)	29-38
			умеет	Собеседование (ОУ-1)	29-38
			владеет	Собеседование (ОУ-1)	29-38

Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков и (или) опыта деятельности, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 2.

V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

(электронные и печатные издания)

1. Шаньгин, В.Ф. Защита компьютерной информации: учебное пособие / В.Ф. Шаньгин — Москва : ДМК Пресс, 2010. — 544 с. — Режим доступа: https://e.lanbook.com/book/1122
2. Кукина, Е.Г. Введение в криптографию: сборник задач и упражнений / Е.Г. Кукина, В.А. Романьков — Омск : ОмГУ, 2013. — 91 с. — Режим доступа: https://e.lanbook.com/book/75394
3. Рябко, Б.Я. Основы современной криптографии и стеганографии: монография / Б.Я. Рябко, А.Н. Фионов — Москва : Горячая линия-Телеком, 2011. — 232 с. — Режим доступа: https://e.lanbook.com/book/5192

Дополнительная литература

(печатные и электронные издания)

1. Де, К. Просто криптография / К. Де ; пер. с англ. Жуковой М — Санкт-Петербург : , 2014. — 208 с. — Режим доступа: https://e.lanbook.com/book/102340
2. Глухов, М.М. Введение в теоретико-числовые методы криптографии: учебное пособие / М.М. Глухов, И.А. Круглов, А.Б. Пичкур, А.В. Черемушкин — Санкт-Петербург : Лань, 2011. — 400 с. — Режим доступа: https://e.lanbook.com/book/68466

3. Серёдкин, А.Н. Основы защиты информации и информационные технологии. В 3 частях. Кн. 2: Криптография, криптоанализ и методы защиты информации в ИС и ИТ: учебное пособие / А.Н. Серёдкин, В.Р. Роганов, В.О. Филиппенко. — Пенза : ПензГТУ, 2013

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Основные виды криптографических протоколов [Электронный ресурс]. – Электрон. дан. – Режим доступа : http://infoprotect.net/varia/kriptograficheskie_protokolyi
2. ГОСТ Р 34.11-2012 [Электронный ресурс]. – Электрон. дан. – Режим доступа : https://fintender.ru/star/gost/r-34-11-2012
3. ГОСТ Р 34.11-94 [Электронный ресурс]. – Электрон. дан. – Режим доступа : https://fintender.ru/star/gost/r-34-11-94

Перечень информационных технологий и программного обеспечения

Для работы с литературой из списка необходимо наличие у студента аккаунтов в указанных электронно-библиотечных системах: Электронно-библиотечная система Издательства "Лань" (https://e.lanbook.com/).

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Количество аудиторных часов, отведенных на изучение дисциплины «Дополнительные главы криптографических протоколов», составляет 72 часа. На самостоятельную работу – 36 часов.

Аудиторная нагрузка состоит из 36 лекционных часов и 36 часов практических работ. На лекционных занятиях обучающийся получает теоретические знания, усвоение которых необходимо для дальнейшего выполнения практических заданий. Студенту рекомендуется предварительно готовиться к лекции, используя ресурсы из списка, приведённого в разделе V, для более качественного освоения теоретического материала, а также возможности задать вопросы преподавателю.

Подготовка к практическим занятиям предполагает повторение лекционного материала. В результате выполнения работы студент

предоставляет преподавателю отчёт о проделанной работе, содержащий следующие пункты: цель работы, краткий теоретический материал, задание, ход работы, результаты и выводы о проделанной работе.

В рамках указанной дисциплины итоговой формой аттестации является зачет. Вопросы к зачету соответствуют темам, изучаемым на лекционных занятиях. Самостоятельная работа при подготовке к зачету включает изучение теоретического материала с использованием лекционных материалов, рекомендуемых источников из списка литературы и материалов по практическим работам.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус L, ауд. L 633, Учебная аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 50) Оборудование: Доска аудиторная, переносной компьютер (ноутбук Lenovo) с сумкой – 1 шт. Шкаф вытяжной для муф. Печей, печь муфельная ПМ 10М, стол для весов ЛАБ-PRO СВ 60.40.75 Г, шкаф вытяжной, рабочая поверхность - керамогранит (в комплекте) ЛАБ-PRO ШВ 150.80.225 KG, шкаф для хранения реактивов ЛАБ-PRO ШМР 60.50.195 (Длина 600мм Глубина 500мм Высота 1950мм),
Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус L, ауд. L 607, Учебная аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 30) Оборудование: Доска аудиторная, переносной компьютер (ноутбук Lenovo) с сумкой – 1 шт.

Приложение 1

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

по дисциплине «Дополнительные главы криптографических протоколов»

Направление подготовки 10.05.01 Компьютерная безопасность

специализация «Математические методы защиты информации»

Форма подготовки очная

Владивосток
2019

План-график выполнения самостоятельной работы по дисциплине

№ п/п	Дата/сроки выполнения	Вид самостоятельной работы	Примерные нормы времени на выполнение	Форма контроля
1	1-17 неделя обучения	Подготовка практического задания (выполнение отчета к занятию)	18	Отчет о выполнении практического задания
2	18 неделя обучения	Подготовка и сдача зачета	18	Зачет

Рекомендации по самостоятельной работе студентов

При подготовке отчета о выполнении практического задания должны использоваться источники из списка учебной литературы, а также примеры, рассмотренные на лекционных и практических занятиях. Отчет должен содержать:

- титульный лист;
- содержание;
- описание задания;
- решение;
- выводы.

Методические указания к выполнению отчета по занятию

Для получения **«зачтено»** отчет должен содержать основные пункты: титульный лист, содержание, описание задания, решение, выводы. При представлении отчета к сдаче обучающийся последовательно излагает принцип выполненной работы.

Оценка **«незачтено»** выставляется в случае, если отчет не содержит решения или выводов; обучающийся не может объяснить решение, излагает материал непоследовательно, сбивчиво.

Приложение 2

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Дополнительные главы криптографических протоколов»

Направление подготовки 10.05.01 Компьютерная безопасность

специализация «Математические методы защиты информации»

Форма подготовки очная

Владивосток
2019

Паспорт ФОС

Код и формулировка компетенции	**Этапы формирования компетенции**	
(ПК-5) способность участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	Знает	Защитные механизмы и средства обеспечения безопасности операционных систем, средства и методы хранения и передачи аутентификационной информации, требования к подсистеме аудита и политике аудита, основные средства и методы анализа программных реализаций.
	Умеет	Формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе, корректно применять симметричные и асимметричные криптографические алгоритмы.
	Владеет	Навыками разработки программных модулей, реализующих задачи, связанные с обеспечением безопасности операционных систем распространенных семейств, навыками анализа программных реализаций.
(ПК-10) способность оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации	Знает	Основные виды симметричных и асимметричных криптографических алгоритмов, защитные механизмы и средства обеспечения безопасности операционных систем, средства и методы хранения и передачи аутентификационной информации, требования к подсистеме аудита и политике аудита. Основные средства и методы анализа программных реализаций.
	Умеет	Использовать средства защиты, предоставляемые системами управления базами данных, осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты. Применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях.
	Владеет	Методиками анализа сетевого трафика, методиками анализа результатов работы средств обнаружения вторжений, навыками конфигурирования локальных компьютерных сетей, реализации сетевых

		протоколов с помощью программных средств, навыками настройки межсетевых экранов.

Контроль достижения целей курса

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства - наименование	
				текущий контроль	промежуточная аттестация
1	Раздел I. Стандарты на цифровую подпись и функцию хеширования	ПК-5, ПК-10	знает	Конспект (ПР-7)	1-9
			умеет	Собеседование (ОУ-1)	1-9
			владеет	Собеседование (ОУ-1)	1-9
2	Раздел II. Специфические криптографические протоколы	ПК-5, ПК-10	знает	Конспект (ПР-7)	10-19
			умеет	Собеседование (ОУ-1)	10-19
			владеет	Собеседование (ОУ-1)	10-19
3	Раздел III. Практические криптографические протоколы	ПК-5, ПК-10	знает	Конспект (ПР-7)	20-28
			умеет	Собеседование (ОУ-1)	20-28
			владеет	Собеседование (ОУ-1)	20-28
4	Раздел IV. Особенности применения криптографических алгоритмов на ИК	ПК-5, ПК-10	знает	Конспект (ПР-7)	29-38
			умеет	Собеседование (ОУ-1)	29-38
			владеет	Собеседование (ОУ-1)	29-38

Оценочные средства для промежуточной аттестации

Список вопросов на зачет

1. Задачи, которые позволяет решать ЦП.
2. Сложностью каких задач определяется надежность ЦП.
3. Перечислить 3 класса ЦП.
4. В чем заключается проблема инфраструктуры открытых ключей.
5. Основные математические проблемы, на основе которых строятся ЦП.

6. ЦП RSA.
7. ЦП Эль-Гамаля.
8. Сравнение, лежащее в основе ЦП класса Эль-Гамаля.
9. В чем заключается возможность уменьшения длины ключа, для ЦП класса Эль-Гамаля.
10. 3 алгоритма в DSS.
11. Параметры DSA.
12. Какие поля используются в EC DSA.
13. Какие кривые используются в EC DSA.
14. Что является секретным ключом в EC DSA.
15. Как строятся поля $GF(p^m)$. Построить поле $GF(2^2)$, $GF(2^3)$.
16. Вид кривой в ГОСТ 34.10.
17. Формула инварианта J(E).
18. Как выбираются параметры кривой.
19. Описать параметры схемы ЦП ГОСТ 34.10.
20. Алгоритм выработки ЦП в ГОСТ 34.10.
21. Алгоритм проверки ЦП в ГОСТ 34.10.
22. Понятие хеш-функции.
23. Понятие одношаговых сжимающих функций (ОСФ).
24. Построение хеш-функции на основе ОСФ.
25. Ключевые хеш-функции, требования, предъявляемые к ним.
26. Бесключевые хеш-функции, требования, предъявляемые к ним.
27. Диапазоны длин ключевых и бесключевых хешей.
28. Пример ключевой хеш-функции на основе ОСФ с использованием блочного шифрования.
29. Примеры бесключевой хеш-функции на основе ОСФ.
30. Длина хеша в SHA, MD5, ГОСТ 34.11.
31. Разбиение на блоки сообщения в алгоритме SHA (последний блок).
32. Описание набора нелинейных функций в SHA.
33. Переход к следующему циклу в SHA. Выходное значение хеша в SHA.
34. 3 шага одношаговой сжимающей функции в ГОСТ 34.11.
35. Процедура вычисления хеша в ГОСТ 34.11.
36. SHA-256, SHA-384, SHA-512.
37. Определение группы и поля.
38. Мощность конечного поля, количество элементов мультипликативной группы поля

Критерии выставления оценки на зачет

Оценка	Требования к сформированным компетенциям
«зачтено»	Оценка «зачтено» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения.
«не зачтено»	Оценка «не зачтено» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. Как правило, оценка «не зачтено» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

Оценочные средства для текущей аттестации

№ п/п	Код ОС	Наименование оценочного средства	Кроткая характеристика оценочного средства	Представление оценочного средства в фонде
1	ОУ-1	Собеседование	Средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определённому разделу, теме, проблеме и т.п.	Вопросы по темам/разделам дисциплины
2	ОУ-2	Коллоквиум	Средство контроля усвоения учебного материала темы, раздела или разделов дисциплины, организованное как учебное занятие в виде собеседования преподавателя с обучающимися.	Вопросы по темам/разделам дисциплины
3	ПР-7	Конспект	Продукт самостоятельной работы обучающегося, отражающий основные идеи заслушанной лекции, сообщения и т.д.	Темы/разделы дисциплины