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____00___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____54____ час.
в том числе с использованием МАО __9___ час.
самостоятельная работа ___36_____ час.
в том числе на подготовку к экзамену ___00___ час.
контрольные работы (количество) не предусмотрены
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: Боршевников А.Е., ассистент штатный

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, 3 credits
Instructor: Borshevnikov A.E.

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

• ability to correctly apply the apparatus of mathematical analysis, geometry, algebra, discrete mathematics, mathematical logic, theory of algorithms, probability theory, mathematical statistics, information theory, number-theoretic methods (OPK-2) when solving professional problems;

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

• ability to build an algorithm independently, to conduct its analysis and implementation in modern software systems (OPK-10);

• ability to develop formal models of security policies, access control and information flow control policies in computer systems, taking into account information security threats (OPK-9).

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

Main course literature:

1. 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

2. 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» предназначен для обучения студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в обязательные дисциплины вариативной части дисциплин (модулей) 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 – в А семестре 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.

Содержание дисциплины охватывает следующий круг вопросов: стандарты на цифровую подпись и функцию хеширования, специфические криптографические протоколы, практические криптографические протоколы, особенности применения криптографических алгоритмов на ИК.

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:

- способностью корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов (ОПК-2);
- способность применять методологию научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами (ОПК-4);
- способностью к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах (ОПК-10);
- способностью разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации (ОПК-9).

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные, 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	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

системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации		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

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: собеседование (ОУ-1), коллоквиум (ОУ-2), конспект (ПР-7).

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. (4 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. (2 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	собеседование (ОУ-1)	1-9
			умеет	коллоквиум (ОУ-2)	1-9
			владеет	конспект (ПР-7)	1-9

2	Раздел II. Специфические криптографические протоколы	ПК-5, ПК-10	знает	собеседование (ОУ-1)	10-19
			умеет	коллоквиум (ОУ-2)	10-19
			владеет	конспект (ПР-7)	10-19
3	Раздел III. Практические криптографические протоколы	ПК-5, ПК-10	знает	собеседование (ОУ-1)	20-28
			умеет	коллоквиум (ОУ-2)	20-28
			владеет	конспект (ПР-7)	20-28
4	Раздел IV. Особенности применения криптографических алгоритмов на ИК	ПК-5, ПК-10	знает	собеседование (ОУ-1)	29-38
			умеет	коллоквиум (ОУ-2)	29-38
			владеет	конспект (ПР-7)	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. 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

2. 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. — 180 с. — Режим доступа: https://e.lanbook.com/book/62755

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

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 546, Компьютерный класс, аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	1) IBM SPSS Statistics Premium Campus Edition. Поставщик ЗАО Прогностические решения. Договор ЭА-442-15 от 18.01.16 лот 5. Срок действия договора 30.06.2016. Лицензия бессрочно. 2) SolidWorks Campus 500. Поставщик Солид Воркс Р. Договор 15-04-101 от 23.12.2015. Срок действия договора 15.03.2016. Лицензия бессрочно. 3) АСКОН Компас 3D v17. Поставщик Навиком. Договор 15-03-53 от 20.12.2015. Срок действия договора 31.12.2015. Лицензия бессрочно. 4) MathCad Education Universety Edition. Поставщик Софт Лайн Трейд. Договор 15-03-49 от 02.12.2015. Срок действия договора 30.11.2015. Лицензия бессрочно.

	5) Corel Academic Site. Поставщик Софт Лайн Трейд. Договор ЭА-442-15 от 18.01.16 лот 4. Срок действия договора 30.06.2016. Лицензия закончилась 28.01.2019. 6) Microsoft Office, Microsoft Visual Studio. Поставщик Софт Лайн Трейд. Договор ЭА-261-18 от 02.08.18 лот 4. Срок действия договора 20.09.2018. Лицензия до 30.06.2020.

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Количество аудиторных часов, отведенных на изучение дисциплины «Дополнительные главы криптографических протоколов», составляет 54 часа. На самостоятельную работу – 54 часов.

Аудиторная нагрузка состоит из 36 лекционных часов и 18 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 D, ауд. D 546,	Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 15) Оборудование:

Компьютерный класс, аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	Компьютер (твердотельный диск - объемом 128 ГБ; жесткий диск - объем 1000 ГБ; форм-фактор - Tower; комплектуется клавиатурой, мышью, монитором AOC i2757Fm; комплектом шнуров эл. питания) модель - M93p 1 Мультимедийное оборудование: Экран проекционный ScreenLine Trim White Ice 50 см черная кайма сверху, размер рабочей области 236x147 см Документ-камера Avervision CP355AF ЖК-панель 47"", Full HD, LG M4716 CCBA Мультимедийный проектор, Mitsubishi EW33OU, 3000 ANSI Lumen, 1280x800 Сетевая видеокамера Multipix MP-HD718"

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»

Специальность 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	1-10 недели обучения	Подготовка практических заданий (выполнение отчетов к практическим работам № 1-2)	16	Отчеты о выполнении
2	10-17 недели обучения	Подготовка практического задания (выполнение отчета к практической работе № 3)	16	Отчет о выполнении
3	18 неделя обучения	Подготовка к зачету	4	Зачет

Подготовка отчета по практическим работам предполагает повторение лекционного материала и выполнение задания для практических работ по темам из Раздела II РПУД.

В ходе самостоятельной работы обучающийся должен подготовить для сдачи отчёт по проделанной работе. Необходимо указать в отчёте следующую информацию: название и цель работы, краткий теоретический материал, задание на практическую работу, ход работы, полученные результаты и выводы. По результатам защиты отчёта студенту выставляется «зачтено» или «не зачтено». Студент получает «зачтено», если отчёт содержит все перечисленные ранее пункты и оформлен в соответствии с правилами оформления письменных работ.

Самостоятельная работа при подготовке к зачету включает изучение теоретического материала с использованием лекционных материалов, а также основной и дополнительной литературы из списка рекомендуемых источников. Список вопросов для подготовки к зачету, а также методические рекомендации по оцениванию представлены в Приложении 2 РПУД.

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»

Специальность 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	собеседование (ОУ-1)	1-9
			умеет	коллоквиум (ОУ-2)	1-9
			владеет	конспект (ПР-7)	1-9
2	Раздел II. Специфические криптографические протоколы	ПК-5, ПК-10	знает	собеседование (ОУ-1)	10-19
			умеет	коллоквиум (ОУ-2)	10-19
			владеет	конспект (ПР-7)	10-19
3	Раздел III. Практические криптографические протоколы	ПК-5, ПК-10	знает	собеседование (ОУ-1)	20-28
			умеет	коллоквиум (ОУ-2)	20-28
			владеет	конспект (ПР-7)	20-28
4	Раздел IV. Особенности применения криптографических алгоритмов на ИК	ПК-5, ПК-10	знает	собеседование (ОУ-1)	29-38
			умеет	коллоквиум (ОУ-2)	29-38
			владеет	конспект (ПР-7)	29-38

Шкала оценивания уровня сформированности компетенций

Код и формулировка компетенции	**Этапы формирования компетенции**		**критерии**	**показатели**
(ПК-5)	знает	защитные	полнота и	изложение

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	(пороговый уровень)	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.	системность знаний	полученных знаний полное, в соответствии с требованиями учебной программы; ошибки отсутствуют или несущественны, обучающийся способен самостоятельно исправить.
	умеет (продвинутый)	формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе, корректно применять симметричные и асимметричные криптографические алгоритмы.	степень самостоятельности выполнения действия (умения); осознанность действия (умения).	обучающийся способен свободно формулировать и настраивать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе, корректно применять симметричные и асимметричные криптографические алгоритмы самостоятельно; свободно отвечает на вопросы, касающиеся выполняемых действий.
	владеет (высокий)	навыками разработки программных модулей, реализующих	степень умения отбирать и интегрировать имеющиеся	обучающийся способен самостоятельно разрабатывать программные

		задачи, связанные с обеспечением безопасности операционных систем распространенных семейств, навыками анализа программных реализаций.	знания и навыки исходя из поставленной цели, проводить самоанализ и самооценку.	модули, реализующие задачи, связанные с обеспечением безопасности операционных систем распространенных семейств.
(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 (пороговый уровень)	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.	полнота и системность знаний	изложение полученных знаний полное, в соответствии с требованиями учебной программы; ошибки отсутствуют или несущественны, обучающийся способен самостоятельно исправить.
	умеет (продвинутый)	использовать средства защиты, предоставляемые системами управления базами данных, осуществлять	степень самостоятельности выполнения действия (умения); осознанность действия	обучающийся способен свободно использовать средства защиты, предоставляемые системами управления базами данных,

		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.	(умения).	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 самостоятельно; свободно отвечает на вопросы, касающиеся выполняемых действий.
	владеет (высокий)	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.	степень умения отбирать и интегрировать имеющиеся знания и навыки исходя из поставленной цели, проводить самоанализ и самооценку.	обучающийся способен самостоятельно анализировать сетевой трафик, результаты работы средств обнаружения вторжений, конфигурировать локальные компьютерные сети, реализовывать сетевые протоколы с помощью программных средств, настраивать межсетевые экраны.

Методические рекомендации, определяющие процедуры оценивания результатов освоения дисциплины

Промежуточная форма аттестации по данной дисциплине – зачет.

Для допуска к зачету обучающийся должен получить оценку «зачтено» по всем практическим работам курса. Критерии оценивания практических работ представлены далее в данном Приложении.

Зачет проводится в форме собеседования (УО-1), вопросы к зачету соответствуют темам, изучаемым на лекционных занятиях, и представлены далее в Приложении. Для подготовки к ответу на зачете обучающийся получает 20 минут. В ходе подготовки обучающийся может составлять любые записи, однако оценивается прежде всего устный, а не письменный ответ.

При определении оценки учитываются:

-знание основных терминов и понятий курса;

-знание и владение методами и средствами решения задач;

-последовательное изложение материала курса;

-умение формулировать некоторые обобщения по теме вопросов;

-достаточно полные ответы на вопросы;

-умение использовать фундаментальные понятия из базовых естественнонаучных и общепрофессиональных дисциплин при ответе.

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

Каждый студент должен ответить на два вопроса из списка выше. Результаты зачета оцениваются по двухбалльной системе («зачтено», «не зачтено») и заносятся в экзаменационную ведомость и зачетную книжку. В зачетную книжку заносятся только положительные оценки.

При определении оценки учитываются:

-знание основных терминов и понятий курса;

-знание и владение методами и средствами решения задач;

-последовательное изложение материала курса;

-умение формулировать некоторые обобщения по теме вопросов;

-достаточно полные ответы на вопросы;

-умение использовать фундаментальные понятия из базовых естественнонаучных и общепрофессиональных дисциплин при ответе.

Оценка **«зачтено».** Хорошее знание основных терминов и понятий курса. Хорошее знание и владение методами и средствами решения задач. Последовательное изложение материала курса. Умение формулировать некоторые обобщения по теме вопросов. Достаточно полные ответы на вопросы. Умение использовать фундаментальные понятия из базовых естественнонаучных и общепрофессиональных дисциплин при ответе.

Оценка **«не зачтено».** Неудовлетворительное знание основных терминов и понятий курса. Неумение решать задачи. Отсутствие логики и последовательности в изложении материала курса. Неумение формулировать отдельные выводы и обобщения по теме вопросов. Неумение использовать фундаментальные понятия из базовых естественнонаучных и общепрофессиональных дисциплин при ответе.

Оценочные средства для текущей аттестации

В качестве оценочных средств для текущей аттестации применяются лабораторные работы (ПР-6) и конспект (ПР-7).

Конспект является показателем сформированности компетенции на пороговом уровне. Темы конспектов соответствуют темам теоретической части курса из Раздела II РПУД. Критерии оценки по данному виду оценочных средств представлены в таблице:

Оценка	Содержание конспекта
Отлично	Конспект содержит все понятия, термины, положения, изученные на лекции и/или с использованием основных источников литературы, а также содержит сведения из дополнительных источников.
Хорошо	Конспект содержит все понятия, термины, положения, изученные на лекции и/или с использованием основных источников литературы.
Удовлетворительно	Конспект содержит базовые понятия, термины, положения, изученные на лекции.
Неудовлетворительно	Конспект не содержит основных понятий, терминов, положений по данной теме.

Для оценки продвинутого и высокого уровня сформированности компетенции проводятся лабораторные работы. Темы практических работ представлены в Разделе II РПУД. Критерии оценки представлены в таблице:

Оценка	**Критерий**
Зачтено	Отчёт по практической работе содержит все необходимые пункты (цель работы, краткий теоретический материал, задание на практическую работу, ход работы, полученные результаты, выводы). Оформление отчёта соответствует правилам оформления письменных работ. Конспект содержит все понятия, термины, положения, изученные на лекции и/или с использованием основных источников литературы.
Незачтено	Отчёт по практической работе не содержит какого-либо необходимого пункта(ов) и/или оформление отчёта не соответствует правилам оформления письменных работ. Конспект не содержит основных понятий, терминов, положений по данной теме