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
Криптографические протоколы
Специальность 10.05.01 Компьютерная безопасность
(Математические методы защиты информации)
Форма подготовки очная

курс ____3___ семестр ____6____
лекции _36__ час.
Практические занятия____90___час.
Лабораторные работы____00___час.
В том числе с использованием МАО лек.__9___/пр.__36___/лаб.___00__ час.
В том числе в электронной форме лек.___00__/пр.___00__/лаб._00__ час.
Всего часов аудиторной нагрузки____126____ час.
В том числе с использованием МАО ___45__ час.
В том числе в электронной форме __00__ час.
Самостоятельная работа ____54_____ час.
В том числе на подготовку к экзамену ___36___ час.
курсовая работа / курсовой проект не предусмотрены
зачет__не предусмотрен__
экзамен_____6_____семестр

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): Гончаров С.М. к.т.н., доцент

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: *Cryptographic protocols*

Basic part of Block , _6_credits

Instructor: *Goncharov S.M.*

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);*

• *ability to independently build an algorithm, conduct its analysis and implement it in modern software systems (OPK-10).*

Learning outcomes:

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

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

Course description:

The content of the discipline covers the following issues: classification of cryptographic protocols, the use of cryptographic protocols to ensure information security, cryptographic messaging protocols with integrity and confidentiality, password-based authentication protocols using asymmetric encryption systems, symmetric key generation and transfer protocols and asymmetric encryption systems.

Main course literature:

1. *Ожиганов А.А. Криптография: учебное пособие / А.А. Ожиганов – СПб. : Университет ИТМО, 2016. – 142 с. – Режим доступа: http://www.iprbookshop.ru/67231.html*
2. *Лапонина О.Р. Основы сетевой безопасности. Криптографические алгоритмы и протоколы взаимодействия / О.Р. Лапонина – М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. – 242 с. – Режим доступа: http://www.iprbookshop.ru/52217.html*
3. *Варлатая С.К., Шаханова М.В. Криптографические методы и средства обеспечения информационной безопасности: учебно-методический комплекс / С.К. Варлатая, М.В. Шаханова – М. : Проспект, 2015. – 151 с. – Режим доступа: https://lib.dvfu.ru:8443/lib/item?id=chamo:791159&theme=FEFU*

Form of final control: *exam.*

Аннотация к рабочей программе дисциплины «Криптографические протоколы»

Курс учебной дисциплины «Криптографические протоколы» разработана для студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав базовых дисциплин учебного плана Б1.Б.28.

Общая трудоемкость освоения дисциплины составляет 180 часов (5 з.е.). Учебным планом предусмотрены лекционные занятия (36 часов), практические занятия (90 часов), самостоятельная работа 18 часов. Дисциплина реализуется на 3 курсе в 6 семестре. Форма контроля по дисциплине – экзамен.

Дисциплина «Криптографические протоколы» логически и содержательно связана с такими курсами, как «Математическая логика и теория алгоритмов», «Дискретная математика», «Криптографические методы защиты информации».

Содержание дисциплины охватывает следующий круг вопросов: классификация криптографических протоколов, приименение криптографических протоколов для обеспечения информационной безопасности, криптографические протоколы передачи сообщений с обеспечением свойства целостности и конфиденциальности, протоколы аутентификации на основе паролей и с использованием систем ассиметричного шифрования, протоколы генерации и передачи ключей на основе симметричных и асимметричных шифрсистем.

Цель – сформировать представление об использования криптографических протоколов для защиты информации, о принципах применения совершенных информационных технологий.

Задачи:

- дать основы знаний об основных криптографических протоколах;

•познакомить с методикой выбора и оценки их качества.

Для успешного изучения дисциплины «Криптографические протоколы» 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 к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах (ОПК-10).

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные (элементы компетенций).

Код и формулировка компетенции	**Этапы формирования компетенции**	
(ОПК-2) способность 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	Знает	основные понятия и теоремы математического анализа, геометрии, алгебры, дискретной математики, математической логики
	Умеет	определять возможности применения методов математического анализа; анализировать поставленную задачу, находить методы ее решения, проводить анализ полученного решения
	Владеет	навыками использования стандартных методов и моделей математического анализа и их применения к решению прикладных задач в области криптографической защиты информации
(ОПК-9) способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации	Знает	базовые протоколы проверки подлинности и обмена ключами; основные криптологические аспекты проектирования и развертывания технологии PKI в корпоративных сетях; основные подходы к конструированию систем защиты информации с использованием криптографических протоколов различной направленности
	Умеет	проектировать и внедрять схемы аутентификации на основе типовых

		стандартизированных механизмов; использовать схемы разделения секрета для хранения критической информации
	Владеет	навыком настройки параметров протоколов используемых для аутентификации и обмена ключами в операционных системах семейства Windows; навыком генерирования ключевых пар

Для формирования вышеуказанных компетенций в рамках дисциплины «Криптографические протоколы» 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. Основные понятия (4 час.)

Тема 1. Криптографические протоколы (2 час.)

1.1. Понятие криптографического протокола.

1.2. Применение криптографических протоколов для обеспечения информационной безопасности.

1.3. Классификация криптографических протоколов.

Тема 2. Безопасность криптографических протоколов (2 час.)

1.1. Основные виды уязвимостей и атак на криптографические протоколы. Защитные меры.

1.2. Подходы к оценке безопасности криптографических протоколов.

Раздел II. Криптографические протоколы передачи сообщений (8 час.)

Тема 1. Протоколы передачи сообщений (6 час.)

1.1. Криптографический протокол передачи сообщений с обеспечением свойства целостности.

1.2. Криптографический протокол передачи сообщений с обеспечением свойства конфиденциальности.

1.3. Криптографический протокол передачи сообщений с обеспечением свойства неотказуемости.

Тема 2. Общие протоколы (2 час.)

1.1. Комбинированные криптографические протоколы.

Раздел III. Протоколы аутентификации (8 час.)

Тема 1. Общие положения (8 час.)

1.1. Односторонняя и двухсторонняя аутентификация.

1.2. Протоколы аутентификации на основе паролей.

1.3. Протоколы «рукопожатия» и типа «запрос-ответ».

1.4. Протоколы аутентификации с использованием систем ассиметричного шифрования.

Раздел IV. Протоколы аутентифицированного ключевого обмена (4 час.)

Тема 1. Протоколы обмена (2 час.)

1.1. Протоколы генерации и передачи ключей на основе симметричных и асимметричных шифрсистем.

1.2. Двух и трех сторонние протоколы передачи и распределения ключей.

1.3. Функции доверенной третьей стороны и выполняемые ею роли.

1.4. Схемы предварительного распределения ключей.

1.5. Протокол ключевого обмена Диффи-Хеллмана.

Раздел V. Криптографические протоколы электронных платёжных систем (4 час.)

Тема 1. Основные положения (4 час.)

1.1. Свойства неотслеживаемости и несвязывемости.

1.2. Протоколы битовых обязательств.

1.3. Автономные схемы электронных платежей.

Раздел VI. Прикладные протоколы (8 час.)

Тема 1. Виды протоколов (8 час.)

1.1. Базовый протокол Kerberos.

1.2. Особенности построения семейства протоколов IPsec.

1.3. Протоколы SKIP, SSL/TLS и особенности их реализации.

1.4. Протоколы OCSP и TSP.

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Практические занятия (90 час.)

Занятие 1. Анализ уязвимостей криптографических протоколов передачи сообщений (45 час.)

1. Анализ уязвимостей протокола передачи сообщений с обеспечением свойства целостности.

2. Анализ уязвимостей протокола передачи сообщений с обеспечением свойств неотказуемости.

3. Анализ уязвимостей протокола передачи сообщений с обеспечением свойства конфиденциальности.

Занятие 2. Криптографические протоколы (45 час.)

1. Протоколы аутентификации.

2. Протоколы явного ключевого обмена.

3. Криптографические протоколы электронных платежных систем.

4. Протоколы семейства Ipsec.

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Криптографические протоколы» 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. Основные понятия	ОПК-2, ОПК-9	знает	Конспект (ПР-7)	1-5
			умеет	коллоквиум (ОУ-2)	1-5
			владеет	коллоквиум (ОУ-2)	1-5
2	Раздел II.	ОПК-2,	знает	Конспект (ПР-7)	6-9

	Криптографические протоколы передачи сообщений	ОПК-9	умеет	коллоквиум (ОУ-2)	6-9
			владеет	коллоквиум (ОУ-2)	6-9
			знает	Конспект (ПР-7)	10-13
3	Раздел III. Протоколы аутентификации	ОПК-2, ОПК-9	умеет	коллоквиум (ОУ-2)	10-13
			владеет	коллоквиум (ОУ-2)	10-13
			знает	Конспект (ПР-7)	14-18
4	Раздел IV. Протоколы аутентифицированного ключевого обмена	ОПК-2, ОПК-9	умеет	коллоквиум (ОУ-2)	14-18
			владеет	коллоквиум (ОУ-2)	14-18
			знает	Конспект (ПР-7)	19-21
5	Раздел V. Криптографические протоколы электронных платёжных систем	ОПК-2, ОПК-9	умеет	коллоквиум (ОУ-2)	19-21
			владеет	коллоквиум (ОУ-2)	19-21
			знает	Конспект (ПР-7)	22-25
6	Раздел VI. Прикладные протоколы	ОПК-2, ОПК-9	умеет	коллоквиум (ОУ-2)	22-25
			владеет	коллоквиум (ОУ-2)	22-25

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. Ожиганов А.А. Криптография: учебное пособие / А.А. Ожиганов – СПб. : Университет ИТМО, 2016. – 142 с. – Режим доступа:

http://www.iprbookshop.ru/67231.html
2. Лапонина О.Р. Основы сетевой безопасности. Криптографические алгоритмы и протоколы взаимодействия / О.Р. Лапонина – М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. – 242 с. – Режим доступа: http://www.iprbookshop.ru/52217.html
3. Варлатая С.К., Шаханова М.В. Криптографические методы и средства обеспечения информационной безопасности: учебно-методический комплекс / С.К. Варлатая, М.В. Шаханова – М. : Проспект, 2015. – 151 с. – Режим доступа: https://lib.dvfu.ru:8443/lib/item?id=chamo:791159&theme=FEFU

Дополнительная литература

(печатные и электронные издания)

1. Петров, А.А. Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс] / А.А. Петров. — Электрон. дан. — Москва : ДМК Пресс, 2008. — 448 с. — Режим доступа: https://e.lanbook.com/book/3027
2. Романьков, В.А. Алгебраическая криптография [Электронный ресурс] : монография / В.А. Романьков. — Электрон. дан. — Омск : ОмГУ, 2013. — 136 с. — Режим доступа: https://e.lanbook.com/book/75405
3. Спицын В.Г. Информационная безопасность вычислительной техники [Электронный ресурс]: учебное пособие/ Спицын В.Г.— Электрон. текстовые данные.— Томск: Томский государственный университет систем управления и радиоэлектроники, Эль Контент, 2011.— 148 с.— Режим доступа: http://www.iprbookshop.ru/13936.html
4. Варлатая С.К., Шаханова М.В. Криптографические методы и средства обеспечения информационной безопасности: учебно-методический комплекс / С.К. Варлатая, М.В. Шаханова – М. : Проспект, 2015. – 152 с. – Режим доступа: https://elib.dvfu.ru/vital/access/manager/Repository/fefu:5176

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Основы криптографии [Электронный ресурс]. – Электрон. дан. – Режим доступа: http://www.intuit.ru/studies/courses/691/547/info
2. Криптографические основы безопасности [Электронный ресурс]. – Электрон. дан. – Режим доступа: http://www.intuit.ru/studies/courses/28/28/info
3. Криптография [Электронный ресурс]. – Электрон. дан. – Режим доступа: http://habrahabr.ru/hub/crypto/

Перечень информационных технологий и программного обеспечения

Для работы с литературой из списка необходимо наличие у студента аккаунтов в указанных электронно-библиотечных системах: «Лань» (https://e.lanbook.com/), «ЭБС IPR BOOKS» (http://www.iprbookshop.ru/).

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Количество аудиторных часов, отведенных на изучение дисциплины «Криптографические протоколы», составляет 126 часов. На самостоятельную работу – 90 часов, в том числе 36 часов на подготовку к экзамену. При этом аудиторная нагрузка состоит из 36 лекционных часов и 90 часов практических занятий.

Обучающийся получает теоретические знания на лекционных занятиях, необходимые для последующего выполнения практических заданий. В ходе подготовки к лекциям должны использоваться источники из списка учебной литературы.

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.

При подготовке к практическим занятиям также необходимо повторить теоретический материал.

Промежуточная форма аттестации по данной дисциплине – экзамен. Вопросы к экзамену соответствуют темам, изучаемым на лекционных занятиях. Таким образом, при самостоятельной подготовке к экзамену студенту необходимо воспользоваться конспектами лекций, а также иными источниками из списка литературы для более глубокого понимания материала.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров,	Помещение укомплектовано специализированной учебной мебелью

ул. Аякс п., д. 10, корпус D, ауд. D 318, Компьютерный класс кафедры информационной безопасности, аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	(посадочных мест – 15) Оборудование: Моноблок HPP-B0G08ES#ACB/8200E AIO i52400S 500G 4.0G 28 PC Электронная доска Poly Vision Walk-and-Talk WTL 1810 Мультимедийная аудитория: 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 Доска аудиторная

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 «Криптографические протоколы»
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	1-18 неделя обучения	Подготовка практического задания (выполнение отчета к занятию)	18	Отчет о выполнении практического задания
2	Сессия	Подготовка и сдача экзамена	36	Экзамен

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 «Криптографические протоколы»
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	
(ОПК-2) способность 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	Знает	основные понятия и теоремы математического анализа, геометрии, алгебры, дискретной математики, математической логики
	Умеет	определять возможности применения методов математического анализа; анализировать поставленную задачу, находить методы ее решения, проводить анализ полученного решения
	Владеет	навыками использования стандартных методов и моделей математического анализа и их применения к решению прикладных задач в области криптографической защиты информации
(ОПК-9) способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации	Знает	базовые протоколы проверки подлинности и обмена ключами; основные криптологические аспекты проектирования и развертывания технологии PKI в корпоративных сетях; основные подходы к конструированию систем защиты информации с использованием криптографических протоколов различной направленности
	Умеет	проектировать и внедрять схемы аутентификации на основе типовых стандартизированных механизмов; использовать схемы разделения секрета для хранения критической информации
	Владеет	навыком настройки параметров протоколов используемых для аутентификации и обмена ключами в операционных системах семейства Windows; навыком генерирования ключевых пар

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства - наименование	
				текущий контроль	промежуточная аттестация
1	Раздел I. Основные понятия	ОПК-2, ОПК-9	знает	Конспект (ПР-7)	1-5
			умеет	коллоквиум	1-5

				(ОУ-2)	
			владеет	коллоквиум (ОУ-2)	1-5
2	Раздел II. Криптографические протоколы передачи сообщений	ОПК-2, ОПК-9	знает	Конспект (ПР-7)	6-9
			умеет	коллоквиум (ОУ-2)	6-9
			владеет	коллоквиум (ОУ-2)	6-9
3	Раздел III. Протоколы аутентификации	ОПК-2, ОПК-9	знает	Конспект (ПР-7)	10-13
			умеет	коллоквиум (ОУ-2)	10-13
			владеет	коллоквиум (ОУ-2)	10-13
4	Раздел IV. Протоколы аутентифицированного ключевого обмена	ОПК-2, ОПК-9	знает	Конспект (ПР-7)	14-18
			умеет	коллоквиум (ОУ-2)	14-18
			владеет	коллоквиум (ОУ-2)	14-18
5	Раздел V. Криптографические протоколы электронных платёжных систем	ОПК-2, ОПК-9	знает	Конспект (ПР-7)	19-21
			умеет	коллоквиум (ОУ-2)	19-21
			владеет	коллоквиум (ОУ-2)	19-21
6	Раздел VI. Прикладные протоколы	ОПК-2, ОПК-9	знает	Конспект (ПР-7)	22-25
			умеет	коллоквиум (ОУ-2)	22-25
			владеет	коллоквиум (ОУ-2)	22-25

Оценочные средства для промежуточной аттестации

Список вопросов на экзамен

1. Понятие криптографического протокола.
2. Применение криптографических протоколов для обеспечения информационной безопасности.
3. Классификация криптографических протоколов.
4. Основные виды уязвимостей и атак на криптографические протоколы. Защитные меры.
5. Подходы к оценке безопасности криптографических протоколов.

6. Криптографический протокол передачи сообщений с обеспечением свойства целостности.

7. Криптографический протокол передачи сообщений с обеспечением свойства конфиденциальности.

8. Криптографический протокол передачи сообщений с обеспечением свойства неотказуемости.

9. Комбинированные криптографические протоколы.

10. Односторонняя и двухсторонняя аутентификация.

11. Протоколы аутентификации на основе паролей.

12. Протоколы «рукопожатия» и типа «запрос-ответ».

13. Протоколы аутентификации с использованием систем ассиметричного шифрования.

14. Протоколы генерации и передачи ключей на основе симметричных и асимметричных шифрсистем.

15. Двух и трех сторонние протоколы передачи и распределения ключей.

16. Функции доверенной третьей стороны и выполняемые ею роли.

17. Схемы предварительного распределения ключей.

18. Протокол ключевого обмена Диффи-Хеллмана.

19. Свойства неотслеживаемости и несвязывемости.

20. Протоколы битовых обязательств.

21. Автономные схемы электронных платежей.

22. Базовый протокол Kerberos.

23. Особенности построения семейства протоколов IPsec.

24. Протоколы SKIP, SSL/TLS и особенности их реализации.

25. Протоколы OCSP и TSP.

Критерии выставления оценки на экзамене

Оценка	Требования к сформированным компетенциям
«отлично»	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал монографической литературы, правильно обосновывает принятое решение, владеет

	разносторонними навыками и приемами выполнения практических задач по методологии научных исследований.
«хорошо»	Оценка «хорошо» 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.
«удовлетворительно»	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ
«неудовлетворительно»	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

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
4	ПР-7	Конспект	Продукт самостоятельной работы обучающегося, отражающий основные идеи заслушанной лекции, сообщения и т.д.	Темы/разделы дисциплины