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

Корнюшин П.Н
(подпись) (Ф.И.О.)

«__01__» февраля 2020 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 54 час.
лабораторные работы 36 час.
в том числе с использованием МАО лек. 9 / пр. 36 / лаб. 00 час.
всего часов аудиторной нагрузки 126 час.
в том числе с использованием МАО 00 час.
самостоятельная работа 18 час.
в том числе на подготовку к экзамену 36 час.
контрольные работы (количество) не предусмотрены
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 № 5 от « 01 » февраля 2020 г.

И. о. заведующего кафедрой : Корнюшин П.Н., д.ф.-м.н., профессор.
Составитель: Гончаров С.М., к.ф.-м.н, доцент

Владивосток
2020

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 , _5_credits

Instructor: *Goncharov S.M.*

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

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

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: *This discipline covers issues such as the use of cryptographic protocols to ensure information security, the classification of cryptographic protocols, the main types of vulnerabilities and attacks on cryptographic protocols, protective measures.*

Main course literature:

1. Ожиганов А.А. Криптография [Электронный ресурс]: учебное пособие/ Ожиганов А.А.— Электрон. текстовые данные. — 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 [Электронный ресурс]/ Лапонина О.Р.— Электрон. текстовые данные. — 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. – 152 с. – Режим доступа: https://elib.dvfu.ru/vital/access/manager/Repository/fefu:5176м

Form of final control: *exam*

Аннотация к рабочей программе дисциплины
«Криптографические протоколы»

Курс учебной дисциплины «Криптографические протоколы» разработан для студентов, обучающихся по специальности 10.05.01 «Компьютерная безопасность» специализация «Математические методы защиты информации» и входит в состав базовых дисциплин учебного плана Б1.Б.11.6.

Трудоемкость дисциплины в зачетных единицах составляет 5 з.е., в академических часах – 180 часов (лекции – 36 часов, практические занятия – 54 часов, самостоятельная работа – 18 часов, в том числе на подготовку к экзамену 36 часов). Дисциплина реализуется на 3 курсе в 6 семестре. Форма контроля по дисциплине – экзамен.

Дисциплина логически и содержательно связана с такими курсами, как «Алгебра», «Основы информационной безопасности», «Теоретико-числовые методы в криптографии».

Данная дисциплина затрагивает такие вопросы, как применение криптографических протоколов для обеспечения информационной безопасности, классификация криптографических протоколов, основные виды уязвимостей и атак на криптографические протоколы, защитные меры.

Цель дисциплины: сформировать представление об использовании криптографических протоколов для защиты информации, об основных видах уязвимостей и атак на криптографические протоколы, а также о соответствующих мерах защиты.

Задачи дисциплины:

- сформировать знания об основных видах криптографических протоколов, их применении для обеспечения информационной безопасности;

- применять защитные меры от основных видов уязвимостей и атак на криптографические протоколы.

Для успешного изучения дисциплины «Криптографические протоколы» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность использовать нормативные правовые акты в своей профессиональной деятельности (ОПК-5).

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные компетенции (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 разделы математики, необходимые для понятия механизмов работы криптографических протоколов
	Умеет	применять изученные математические методы при решении профессиональных задач и задач с практическим содержанием
	Владеет	математическим аппаратом, изученным в данном курсе и необходимым для дальнейшего совершенствования профессиональной деятельности
(ОПК-9) способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации	Знать	основные виды политик управления доступом и информационными потоками в компьютерных системах
	Уметь	разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками
	Владеть	навыками разработки моделей угроз и моделей нарушителя

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

Лабораторные работы (90 час.)

Лабораторная работа № 1. Шифрование с закрытым ключом незнакомого теста. (10 час.)

Лабораторная работа № 2. Программная реализация шифра Цезаря. (10 час.)

Лабораторная работа №3. Одноалфавитная замена. (10 час.)

Лабораторная работа №4. Многоалфавитные подстановки, методы гаммирования. (10 час.)

Лабораторная работа №5. Программная реализация шифра Вижинера. (10 час.)

Лабораторная работа №6. Методы перестановки. Понятие композиционного шифра. (10 час.)

Лабораторная работа №7. Поточные шифры. (10 час.)

Лабораторная работа №8. Протокол распределения ключей Диффи-Хеллмана. (10 час.)

Лабораторная работа №9. Изучение средств настройки протокола IPSEC. (10 час.)

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	собеседование (ОУ-1)	1-4
			умеет	коллоквиум (ОУ-2)	1-4
			владеет	конспект (ПР-7)	1-4
2	Раздел II. Криптографические протоколы передачи сообщений	ОПК-2, ОПК-9	знает	собеседование (ОУ-1)	5-12
			умеет	коллоквиум (ОУ-2)	5-12
			владеет	конспект (ПР-7)	5-12
3	Раздел III. Протоколы аутентификации	ОПК-2, ОПК-9	знает	собеседование (ОУ-1)	13-20
			умеет	коллоквиум (ОУ-2)	13-20
			владеет	конспект (ПР-7)	13-20
4	Раздел IV. Протоколы аутентифицированного ключевого обмена	ОПК-2, ОПК-9	знает	собеседование (ОУ-1)	21-24
			умеет	коллоквиум (ОУ-2)	21-24
			владеет	конспект (ПР-7)	21-24
5	Раздел V. Криптографические протоколы	ОПК-2, ОПК-9	знает	собеседование (ОУ-1)	25-28
			умеет	коллоквиум (ОУ-2)	25-28

	электронных платёжных систем		владеет	конспект (ПР-7)	25-28
6	Раздел VI. Прикладные протоколы	ОПК-2, ОПК-9	знает	собеседование (ОУ-1)	29-36
			умеет	коллоквиум (ОУ-2)	29-36
			владеет	конспект (ПР-7)	29-36

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 [Электронный ресурс]: учебное пособие/ Ожиганов А.А.— Электрон. текстовые данные. — СПб.: Университет ИТМО, 2016.— 142 c.— Режим доступа: http://www.iprbookshop.ru/67231.html

2. Лапонина О.Р. Основы сетевой безопасности. Криптографические алгоритмы и протоколы взаимодействия [Электронный ресурс]/ Лапонина О.Р.— Электрон. текстовые данные. — М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 242 c.— 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. – 152 с. – Режим доступа: https://elib.dvfu.ru/vital/access/manager/Repository/fefu:5176м

Дополнительная литература
(печатные и электронные издания)

1. Ниссенбаум, О.В. Криптографические протоколы: лабораторный практикум: учебно-методическое пособие для студентов специальностей «Компьютерная безопасность» и «Информационная безопасность автоматизированных систем"/ О.В. Ниссенбаум, Н.В. Поляков; Тюм. гос. ун-т. - Тюмень: Изд-во ТюмГУ, 2012. - 40 с. Режим доступа: https://e.lanbook.com/reader/journalArticle/403553/#1

2. Романьков В.А. Алгебраическая криптография /В.А. Романьков – Омск: ОмГУ, 2013. – 136 с. Режим доступа: https://e.lanbook.com/reader/journalArticle/403553/#1

3. Спицын, В. Г. Информационная безопасность вычислительной техники: учебное пособие / В. Г. Спицын – Томск: Эль Контент, 2011 – 148 с. Режим доступа: https://e.lanbook.com/reader/journalArticle/381028/#1

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

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

Перечень информационных технологий и программного обеспечения

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 732, Учебная 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. Срок действия договора 20.09.2018. Лицензия до 30.06.2020.

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Для подготовки к тестам и контрольным необходимо пользоваться конспектом лекций из основного и дополнительного списка литературы. Для выполнения самостоятельных работ следует использовать список

дополнительной литературы. Для получения расширенных и углублённых знаний по тематике рекомендуется пользоваться ссылками из списка Интернет-ресурсов.

В рамках указанной дисциплины итоговой формы аттестации является экзамен. Самостоятельная работа при подготовке к экзамену включает изучение теоретического материала с использованием лекционных материалов, рекомендуемых источников и материалов по лабораторным занятиям.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 732, 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 – 48) Оборудование: Экран проекционный Projecta Elpro Large Electron, 500x316 см, размер рабочей области 490x306 Документ-камера Avervision CP 355 AF Мультимедийный проектор Panasonic PT-DZ11OXE, 10 600 ANSI Lumen, 1920x1200 Сетевая видеокамера Multipix MP-HD718 ЖК-панель 47"", Full HD, LG M4716 CCBA ЖК-панель 42"", Full HD, LG M4214 CCBA ЖК-панель 42"", Full HD, LG M4214 CCBA", доска аудиторная, переносной компьютер (ноутбук Lenovo) с сумкой – 1 шт

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»
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	1-2 неделя обучения	Подготовка к аудиторным занятиям. Подготовка отчёта по лабораторным работам	6	Отчёт о выполнении
2	3-4 неделя обучения	Подготовка к аудиторным занятиям. Подготовка отчёта по лабораторным работам	6	Отчёт о выполнении
3	5-6 неделя обучения	Подготовка к аудиторным занятиям. Подготовка отчёта по лабораторным работам	6	Отчёт о выполнении
4	7-8 неделя обучения	Подготовка к аудиторным занятиям. Подготовка отчёта по лабораторным работам	6	Отчёт о выполнении
5	9-10 неделя обучения	Подготовка к аудиторным занятиям. Подготовка отчёта по лабораторным работам	6	Отчёт о выполнении
6	10-11 неделя обучения	Подготовка к аудиторным занятиям. Подготовка отчёта по лабораторным работам	6	Отчёт о выполнении
7	12-13 неделя обучения	Подготовка к аудиторным занятиям. Подготовка отчёта	6	Отчёт о выполнении

		по лабораторным работам		
8	14-16 неделя обучения	Подготовка к аудиторным занятиям. Подготовка отчёта по лабораторным работам	6	Отчёт о выполнении
9	16-18 неделя обучения	Подготовка к аудиторным занятиям. Подготовка отчёта по лабораторным работам	6	Отчёт о выполнении
10	Сессия	Подготовка к экзамену	36	Экзамен

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»

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	
(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 разделы математики, необходимые для понятия механизмов работы криптографических протоколов
	Умеет	применять изученные математические методы при решении профессиональных задач и задач с практическим содержанием
	Владеет	математическим аппаратом, изученным в данном курсе и необходимым для дальнейшего совершенствования профессиональной деятельности
(ОПК-9) способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации	Знать	основные виды политик управления доступом и информационными потоками в компьютерных системах
	Уметь	разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками
	Владеть	навыками разработки моделей угроз и моделей нарушителя

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	собеседование (ОУ-1)	1-4
			умеет	коллоквиум (ОУ-2)	1-4
			владеет	конспект (ПР-7)	1-4
2	Раздел II. Криптографические протоколы передачи сообщений	ОПК-2, ОПК-9	знает	собеседование (ОУ-1)	5-12
			умеет	коллоквиум (ОУ-2)	5-12
			владеет	конспект (ПР-7)	5-12

3	Раздел III. Протоколы аутентификации	ОПК-2, ОПК-9	знает	собеседование (ОУ-1)	13-20
			умеет	коллоквиум (ОУ-2)	13-20
			владеет	конспект (ПР-7)	13-20
4	Раздел IV. Протоколы аутентифицированного ключевого обмена	ОПК-2, ОПК-9	знает	собеседование (ОУ-1)	21-24
			умеет	коллоквиум (ОУ-2)	21-24
			владеет	конспект (ПР-7)	21-24
5	Раздел V. Криптографические протоколы электронных платёжных систем	ОПК-2, ОПК-9	знает	собеседование (ОУ-1)	25-28
			умеет	коллоквиум (ОУ-2)	25-28
			владеет	конспект (ПР-7)	25-28
6	Раздел VI. Прикладные протоколы	ОПК-2, ОПК-9	знает	собеседование (ОУ-1)	29-36
			умеет	коллоквиум (ОУ-2)	29-36
			владеет	конспект (ПР-7)	29-36

Шкала оценивания уровня форсированности компетенций

Код и формулировка компетенции	**Этапы формирования компетенции**		**критерии**	**показатели**
(ПК-1) способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты	Знает	методы криптографической информации; концепцию инфраструктуры открытых ключей основы функционирования компьютерных сетей, методы формирования и	полнота и системность знаний	изложение полученных знаний полное, в соответствии с требованиями учебной программы; ошибки отсутствуют или несущественны, обучающийся способен самостоятельно исправить.

информации		компьютерных сетей.		
	Умеет	определять требуемый метод криптографической защиты; работать с инфраструктурой открытых ключей, выбирать тип электронной подписи и носитель контейнера закрытого ключа проектировать виртуальные частные сети.	степень самостоятельности выполнения действия (умения); осознанность действия (умения).	обучающийся способен свободно строить модели простых неформализуемых задач самостоятельно; свободно отвечает на вопросы, касающиеся выполняемых действий.
	Владеет	навыками развертывания инфраструктуры открытых ключей, навыками развертывания защищенных сетей с помощью криптографических средств навыками развертывания и применения средств электронной подписи.	степень умения отбирать и интегрировать имеющиеся знания и навыки исходя из поставленной цели, проводить самоанализ и самооценку.	обучающийся способен самостоятельно создать вычислительную сеть для решения прикладных инженерных задач.
(ПК-7) способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении	Знает	особенности сертификации криптографических средств особенности лицензирования деятельности, связанной криптографическими средствами: перечень сертифицированных криптографических средств.	полнота и системность знаний	изложение полученных знаний полное, в соответствии с требованиями учебной программы; ошибки отсутствуют или несущественны, обучающийся способен самостоятельно исправить.

технико-экономического обоснования соответствующих проектных решений	Умеет	определять необходимость применения и выбирать сертифицированные криптографические средства.	степень самостоятельности выполнения действия (умения); осознанность действия (умения).	обучающийся способен свободно строить модели простых неформализуемых задач самостоятельно; свободно отвечает на вопросы, касающиеся выполняемых действий.
	Владеет	навыками определения необходимости использования криптографических средств; навыками выбора сертифицированных технико-экономических криптографических средств.	степень умения отбирать и интегрировать имеющиеся знания и навыки исходя из поставленной цели, проводить самоанализ и самооценку.	обучающийся способен самостоятельно создать вычислительную сеть для решения прикладных инженерных задач.
(ПК-17) способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационн	Знает	требования к эксплуатации криптографических средств; нормативные и распорядительные документы, регламентирующие работу с криптографическими средствами.	полнота и системность знаний	изложение полученных знаний полное, в соответствии с требованиями учебной программы; ошибки отсутствуют или несущественны, обучающийся способен самостоятельно исправить.

ой безопасности	Умеет	анализировать нормативные и распорядительные документы, регламентирующие работу с криптографическими средствами.	степень самостоятельности выполнения действия (умения); осознанность действия (умения).	обучающийся способен свободно строить модели простых неформализуемых задач самостоятельно; свободно отвечает на вопросы, касающиеся выполняемых действий.
	Владеет	навыками формирования организационно-правового обеспечения при применении криптографических средств; навыками подготовки к лицензированию при использовании криптографических средств.	степень умения отбирать и интегрировать имеющиеся знания и навыки исходя из поставленной цели, проводить самоанализ и самооценку.	обучающийся способен самостоятельно создать вычислительную сеть для решения прикладных инженерных задач.

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	ПК-1	знает	ПР-1	1-4
			умеет	ПР-1	1-4
			владеет	ПР-1	1-4
2	Раздел II. Криптографические протоколы передачи сообщений	ПК-7, ПК-17	знает	ПР-2	5-12
			умеет	ПР-2	5-12
			владеет	ПР-2	5-12
3	Раздел III. Протоколы аутентификации	ПК-7, ПК-17	знает	ПР-2	13-20
			умеет	ПР-2	13-20
			владеет	ПР-2	13-20
4	Раздел IV. Протоколы аутентифицированного ключевого обмена	ПК-7, ПК-17	знает	ПР-2	21-24
			умеет	ПР-2	21-24
			владеет	ПР-2	21-24
5	Раздел V. Криптографические протоколы электронных платёжных систем	ПК-7, ПК-17	знает	ПР-2	25-28
			умеет	ПР-2	25-28
			владеет	ПР-2	25-28
6	Раздел VI. Прикладные протоколы	ПК-7, ПК-17	знает	ПР-2	29-36
			умеет	ПР-2	29-36
			владеет	ПР-2	29-36

Оценочные средства для промежуточной аттестации
Список вопросов на экзамен

1 Понятие криптографического протокола.

2 Классификация криптографических протоколов.

3 Основные виды уязвимостей и атак на криптографические протоколы

4 Основные защитные меры в криптографических протоколах

5 Криптографический протокол передачи сообщений с обеспечением свойства целостности.

6 Криптографический протокол передачи сообщений с обеспечением

свойства конфиденциальности.

7 Криптографический протокол передачи сообщений с обеспечением свойства неотказуемости.

8 Комбинированные криптографические протоколы.

9 Односторонняя и двухсторонняя аутентификация.

10 Протоколы аутентификации на основе паролей

11 Протоколы аутентификации на основе рукопожатия

12 Протоколы аутентификации типа запрос-ответ.

13 Протоколы генерации и передачи ключей на основе симметричных и асимметричных шифрсистем

14 Двух и трех сторонние протоколы передачи и распределения ключей.

15 Функции доверенной третьей стороны и выполняемые ею роли.

16 Схемы предварительного распределения ключей.

17 Групповые протоколы.

18 Протокол ключевого обмена Диффи-Хеллмана.

19 Свойства неотслеживаемости и несвязывемости криптографических протоколов электронных платежных систем.

20 Протоколы битовых обязательств.

21 Автономные схемы электронных платежей.

22 Базовый протокол Kerberos.

23 Протоколы IPsec.

24 Протоколы SKIP, SSL/TLS.

25 Протоколы OCSP и TSP