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 54 час.
лабораторные работы 36 час.
в том числе с использованием МАО лек. 0 / пр. 0 / лаб. 0 час.
всего часов аудиторной нагрузки 108 час.
в том числе с использованием МАО 00 час.
самостоятельная работа 54 час.
в том числе на подготовку к экзамену 36 час.
контрольные работы (количество) не предусмотрены
курсовая работа / курсовой проект не предусмотрены семестр
зачет не предусмотрен Семестр
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: Власов А.А.

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 , 5 credits
Instructor: Borshevnikov A.E.
At the beginning of the course a student should be able to:

- ability to apply research methods in professional activities, including in the work on interdisciplinary and innovative projects (OPK-4);
- the ability to use programming languages and systems, tools for solving professional, research and applied tasks (OPK-8);
- ability to independently build the algorithm, conduct its analysis and implementation 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 discipline "Cryptographic Protocols" is logically and meaningfully connected with such courses as "Mathematical Logic and Theory of Algorithms", "Discrete Mathematics", "Cryptographic Methods of Information Security".

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

Form of final control: *exam.*

Аннотация к рабочей программе дисциплины

«Криптографические протоколы»

Рабочая программа дисциплины «Криптографические протоколы» предназначен для обучения студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав базовых дисциплин учебного плана Б1.Б.12.06.

Трудоёмкость дисциплины составляет 5 зачетных единиц, в академических часах – 180 часов. Среди них на лекции выделено 36 часов, практические занятия 54 часов, лабораторные работы 36 часов, самостоятельная работа 18 часов, а также 36 часов на подготовку к экзамену. 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».

Цель изучения дисциплины «Криптографические протоколы» заключается в формировании у студентов представления об использовании криптографических протоколов для защиты информации, о принципах применения совершенных информационных технологий.

Задачи дисциплины:

- 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 методы научных исследований в профессиональной деятельности, в том числе в работе над

междисциплинарными и инновационными проектами (ОПК-4);

- способность использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач (ОПК-8);

- 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, профессиональные 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 понятия и задачи векторной алгебры и аналитической геометрии; основные свойства алгебраических структур; основы линейной алгебры над произвольными полями; основы теории групп и теории групп подстановок; свойства векторных пространств; свойства кольца многочленов; основные понятия и методы дискретной математики; основные понятия математической логики и теории алгоритмов; основные понятия и методы теории вероятностей, математической статистики и теории случайных процессов; основные понятия и методы информации
	Умеет	решать основные задачи векторной алгебры и аналитической геометрии; решать системы линейных уравнений над полями; использовать математический аппарат дискретной математики, в том числе применять аппарат производящих функций и рекуррентных соотношений для решения перечисленных задач; находить представление и исследовать свойства булевых и многозначных функций формулами в различных базисах; определять возможность применения методов математического анализа
	Владеет	навыками использования методов аналитической геометрии и векторной алгебры в смежных дисциплинах и физике; навыками решения систем линейных

		уравнений над полем и кольцом вычетов; основами построения математических моделей текстовой информации и моделей систем передачи информации
ОПК-9 – способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации	Знает	основные виды политик управления доступом и информационными потоками в компьютерных системах
	Умеет	основные виды политик управления доступом и информационными потоками в компьютерных системах; основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков
	Владеет	разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками

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: лабораторные работы (ПР-6), конспект (ПР-6), собеседование (ОУ-1), коллоквиум (ОУ-2).

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 (4 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 (54 час.)

Занятие 1. Анализ уязвимостей криптографических протоколов передачи сообщений (27 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 (27 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	Коды и этапы формирования	Оценочные средства - наименование

	дисциплины	компетенций		текущий контроль	промежуточная аттестация
1	Раздел I. Основные понятия	ОПК-2, ОПК-9	знает	собеседование (ОУ-1), коллоквиум (ОУ-2).	1-5
			умеет	лабораторные работы (ПР-6)	1-5
			владеет	конспект (ПР-7),	1-5
2	Раздел II. Криптографические протоколы передачи сообщений	ОПК-2, ОПК-9	знает	собеседование (ОУ-1), коллоквиум (ОУ-2).	6-9
			умеет	лабораторные работы (ПР-6)	6-9
			владеет	конспект (ПР-7),	6-9
3	Раздел III. Протоколы аутентификации	ОПК-2, ОПК-9	знает	собеседование (ОУ-1), коллоквиум (ОУ-2).	10-13
			умеет	лабораторные работы (ПР-6)	10-13
			владеет	конспект (ПР-7),	10-13
4	Раздел IV. Протоколы аутентифицированного ключевого обмена	ОПК-2, ОПК-9	знает	собеседование (ОУ-1), коллоквиум (ОУ-2).	14-18
			умеет	лабораторные работы (ПР-6)	14-18
			владеет	конспект (ПР-7),	14-18
5	Раздел V. Криптографические протоколы электронных платёжных систем	ОПК-2, ОПК-9	знает	собеседование (ОУ-1), коллоквиум (ОУ-2).	19-21
			умеет	лабораторные работы (ПР-6)	19-21
			владеет	конспект (ПР-7),	19-21
6	Раздел VI. Прикладные протоколы	ОПК-2, ОПК-9	знает	собеседование (ОУ-1), коллоквиум (ОУ-2).	22-25
			умеет	лабораторные работы (ПР-6)	22-25
			владеет	конспект (ПР-7),	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)

Дополнительная литература

(печатные и электронные издания)

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

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

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

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 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 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 «Криптографические протоколы», составляет 126 часов. На самостоятельную работу – 18 часов, в том числе 36 часов на подготовку к экзамену. При этом аудиторная нагрузка состоит из 36 лекционных часов и 54 часа 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, 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: "Мультимедийное оборудование: Экран проекционный Projecta Elpro Large Electron, 300x173 см, размер рабочей области 290x163 Документ-камера Avervision CP 355 AF Мультимедийный проектор, Mitsubishi FD630U, 4000 ANSI Lumen, 1920x1080 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.

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»
Специальность 10.05.01 Компьютерная безопасность
(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 недели обучения	Подготовка практического задания (выполнение отчетов к практическим работам № 1-2)	18	Отчеты о выполнении
2	Сессия	Подготовка к экзамену	36	Экзамен

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 экзамену включает изучение теоретического материала с использованием лекционных материалов, а также основной и дополнительной литературы из списка рекомендуемых источников. Список вопросов для подготовки к экзамену, 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 «Криптографические протоколы»
Специальность 10.05.01 Компьютерная безопасность

(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 задачи векторной алгебры и аналитической геометрии; основные свойства алгебраических структур; основы линейной алгебры над произвольными полями; основы теории групп и теории групп подстановок; свойства векторных пространств; свойства кольца многочленов; основные понятия и методы дискретной математики; основные понятия математической логики и теории алгоритмов; основные понятия и методы теории вероятностей, математической статистики и теории случайных процессов; основные понятия и методы информации
	Умеет	решать основные задачи векторной алгебры и аналитической геометрии; решать системы линейных уравнений над полями; использовать математический аппарат дискретной математики, в том числе применять аппарат производящих функций и рекуррентных соотношений для решения перечисленных задач; находить представление и исследовать свойства булевых и многозначных функций формулами в различных базисах; определять возможность применения методов математического анализа
	Владеет	навыками использования методов аналитической геометрии и векторной алгебры в смежных дисциплинах и физике; навыками решения систем линейных уравнений над полем и кольцом вычетов; основами построения математических моделей текстовой информации и моделей систем передачи информации
ОПК-9 – способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации	Знает	основные виды политик управления доступом и информационными потоками в компьютерных системах
	Умеет	основные виды политик управления доступом и информационными потоками в компьютерных системах; основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков

	Владеет	разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками

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

6	Раздел VI. Прикладные протоколы	ОПК-2, ОПК-9		работы (ПР-6)	
			владеет	конспект (ПР-7),	19-21
			знает	собеседование (ОУ-1), коллоквиум (ОУ-2).	22-25
			умеет	лабораторные работы (ПР-6)	22-25
			владеет	конспект (ПР-7),	22-25

Шкала оценивания уровня сформированности компетенций

Код и формулировка компетенции	**Этапы формирования компетенции**		**критерии**	**показатели**
(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 (пороговый уровень)	базовые протоколы проверки подлинности и обмена ключами; основные криптологические аспекты проектирования и развертывания технологии PKI в корпоративных сетях (стандарт X.509); протоколы обеспечения безопасности в сети Internet; основные подходы к конструированию систем защиты информации с использованием криптографических протоколов различной направленности.	полнота и системность знаний	изложение полученных знаний полное, в соответствии с требованиями учебной программы; ошибки отсутствуют или несущественны, обучающийся способен самостоятельно исправить.
	умеет (продвинутый)	проектировать и внедрять схемы аутентификации на основе типовых стандартизирован	степень самостоятельности выполнения действия (умения);	обучающийся способен свободно проектировать и внедрять схемы аутентификации на основе типовых стандартизированных

		ных механизмов; использовать схемы разделения секрета для хранения критической информации; осуществлять распределение аутентифицированных криптографических ключей в корпоративных сетях; анализировать защищенность системы, использующей криптографические протоколы, в модели уязвимой среды Долева-Яо; квалифицированно оценивать информационные риски, возникающие при использовании конкретных криптографических протоколов в защищаемой информационной системе.	осознанность действия (умения).	механизмов самостоятельно; свободно отвечает на вопросы, касающиеся выполняемых действий.
	владеет (высокий)	навыком настройки параметров протоколов используемых для аутентификации и обмена ключами в операционных системах семейства Windows; навыком генерирования ключевых пар с использованием пакета open-ssh; навыком	степень умения отбирать и интегрировать имеющиеся знания и навыки исходя из поставленной цели, проводить самоанализ и самооценку.	обучающийся способен самостоятельно настраивать параметры протоколов, используемых для аутентификации и обмена ключами в операционных системах семейства Windows.

		использования и администрирования современных средств электронной цифровой подписи; навыком самостоятельной работы с современными международными стандартами криптографических протоколов.		
(ОПК-9) способность разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации	знает (пороговый уровень)	базовые протоколы проверки подлинности и обмена ключами; основные криптологические аспекты проектирования и развертывания технологии PKI в корпоративных сетях (стандарт X.509); протоколы обеспечения безопасности в сети Internet; основные подходы к конструированию систем защиты информации с использованием криптографических протоколов различной направленности.	полнота и системность знаний	изложение полученных знаний полное, в соответствии с требованиями учебной программы; ошибки отсутствуют или несущественны, обучающийся способен самостоятельно исправить.
	умеет (продвинутый)	проектировать и внедрять схемы аутентификации на основе типовых стандартизированных механизмов; использовать схемы разделения секрета для	степень самостоятельности выполнения действия (умения); осознанность действия (умения).	обучающийся способен свободно проектировать и внедрять схемы аутентификации на основе типовых стандартизированных механизмов самостоятельно; свободно отвечает на вопросы, касающиеся

		хранения критической информации; осуществлять распределение аутентифицированных криптографических ключей в корпоративных сетях; анализировать защищенность системы, использующей криптографические протоколы, в модели уязвимой среды Долева-Яо; квалифицированно оценивать информационные риски, возникающие при использовании конкретных криптографических протоколов в защищаемой информационной системе.		выполняемых действий.
	владеет (высокий)	навыком настройки параметров протоколов используемых для аутентификации и обмена ключами в операционных системах семейства Windows; навыком генерирования ключевых пар с использованием пакета open-ssh; навыком использования и администрирования современных средств	степень умения отбирать и интегрировать имеющиеся знания и навыки исходя из поставленной цели, проводить самоанализ и самооценку.	обучающийся способен самостоятельно настраивать параметры протоколов, используемых для аутентификации и обмена ключами в операционных системах семейства Windows.

		электронной цифровой подписи; навыком самостоятельной работы с современными международными стандартами криптографически х протоколов.		

Методические рекомендации, определяющие процедуры оценивания результатов освоения дисциплины

Промежуточная форма аттестации по данной дисциплине - экзамен.

Для допуска к экзамену необходимо сдать все практические задания. В случае, если ко дню проведения экзамена обучающийся не сдал какие-либо из практических заданий, он получает возможность сдать их на консультации перед экзаменом. Экзамен выставляется на основании сдачи всех практических заданий и сдачи экзаменационного билета.

При определении оценки ответа обучающегося как на экзамене, так и на практическом занятии учитываются:

- соблюдение норм литературной речи;
- полнота и содержательность ответа;
- умение привести примеры;
- умение пользоваться дополнительной литературой при подготовке к занятиям;
- соответствие представленной в ответах информации материалам лекций и учебной литературы, актуальным сведениям из информационных ресурсов Интернет.

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.

Каждый экзаменационный билет содержит два вопроса из списка выше. Результаты экзамена оцениваются по четырёхбалльной системе («отлично», «хорошо», «удовлетворительно», «неудовлетворительно») и заносятся в экзаменационную ведомость и зачетную книжку. В зачетную книжку заносятся только положительные оценки.

При определении оценки учитываются:

- полнота и содержательность ответа;

- умение привести примеры;

- умение пользоваться дополнительной литературой при подготовке к занятиям;

- соответствие представленной в ответах информации материалам лекций и учебной литературы, сведениям из информационных ресурсов Интернет.

Оценка **«отлично».** Ответы на поставленные вопросы в билете излагаются логично, последовательно и не требуют дополнительных пояснений. Делаются обоснованные выводы. Демонстрируются глубокие знания дисциплины. Соблюдаются нормы литературной речи.

Оценка **«хорошо».** Ответы на поставленные вопросы излагаются систематизировано и последовательно. Материал излагается уверенно. Демонстрируется умение анализировать материал, однако не все выводы носят аргументированный и доказательный характер. Соблюдаются нормы литературной речи.

Оценка **«удовлетворительно».** Допускаются нарушения в последовательности изложения. Демонстрируются поверхностные знания вопроса. Имеются затруднения с выводами. Допускаются нарушения норм литературной речи.

Оценка **«неудовлетворительно».** Материал излагается непоследовательно, сбивчиво, не представляет определенной системы знаний по дисциплине. Имеются заметные нарушения норм литературной речи.

В случае неявки студента на экзамен в экзаменационной ведомости делается отметка «не явился».

Оценочные средства для текущей аттестации

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

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