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

ИНСТИТУТ МАТЕМАТИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ (ШКОЛА)

«СОГЛАСОВАНО»
Руководитель ОП
_____ Добржинский Ю.В.
(подпись) (Ф.И.О.)

«УТВЕРЖДАЮ»
И.о. директора департамента
_____ Боршевников А.Е.
«25» марта 2022 г.

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

курс 5 семестр 10
лекции 34 час.
практические занятия 34 час.
лабораторные работы 0 час.
в том числе с использованием МАО лек. 0 / пр. 0 / лаб. 0 час.
всего часов аудиторной нагрузки 68 час.
в том числе с использованием МАО 0 час.
самостоятельная работа 40 час.
в том числе на подготовку к экзамену 0 час.
контрольные работы (количество) не предусмотрены
курсовая работа / курсовой проект не предусмотрены
зачет 10 семестр
экзамен не предусмотрен

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта по специальности 10.05.01 Компьютерная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 26 ноября 2020 г. № 1459

Рабочая программа обсуждена на заседании департамента информационной безопасности протокол № 5а от «15» февраля 2022 г.

И.о. директора департамента информационной безопасности Боршевников А.Е.

Составитель: Боршевников А.Е., ст. преп.

Владивосток
2022

Оборотная сторона титульного листа РПД

I. Рабочая программа пересмотрена на заседании департамента:

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

Директор департамента _____ _____
(подпись) (И.О. Фамилия)

II. Рабочая программа пересмотрена на заседании департамента:

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

Директор департамента _____ _____
(подпись) (И.О. Фамилия)

III. Рабочая программа пересмотрена на заседании департамента:

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

Директор департамента _____ _____
(подпись) (И.О. Фамилия)

IV. Рабочая программа пересмотрена на заседании департамента:

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

Директор департамента _____ _____
(подпись) (И.О. Фамилия)

Аннотация к рабочей программе дисциплины

«Дополнительные главы криптографических протоколов»

Рабочая программа учебной дисциплины «Дополнительные главы криптографических протоколов» разработана для студентов, обучающихся по специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав дисциплин вариативной части учебного плана Б1.В.02.

1. Цели и задачи освоения дисциплины:

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

Задачи:

- дать общие представления об эллиптических кривых над конечными полями,

- изучить криптографических особенностях применения интеллектуальных картах и специфических криптографических протоколах.

Общепрофессиональные компетенции выпускников и индикаторы их достижения:

Наименование категории (группы) универсальных компетенций	Код и наименование универсальной компетенции (результат освоения)	Код и наименование индикатора достижения компетенции
	ПК-9 Способен производить проверки технического состояния и профилактические осмотры технических средств защиты информации	ПК-9.1 Понимает методологию организации технологического процесса защиты информации ограниченного доступа
	ПК-10 Способен проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем	ПК-10.1 Способен выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций
		ПК-10.2 Использует защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях

2. Трудоёмкость дисциплины и видов учебных занятий по дисциплине

Общая трудоемкость дисциплины составляет 3 зачётных единицы (108 академических часа).

(1 зачетная единица соответствует 36 академическим часам)

Видами учебных занятий и работы обучающегося по дисциплине могут являться:

Обозначение	Виды учебных занятий и работы обучающегося
Лек	Лекции
Пр	Практические занятия
СР	Самостоятельная работа обучающегося в период теоретического обучения

Структура дисциплины:

Форма обучения – очная.

№	Наименование раздела дисциплины	Семестр	Количество часов по видам учебных занятий и работы обучающегося						Формы промежуточной аттестации
			Лек	Лаб	Пр	ОК	СР	Контроль	
1	Стандарты на цифровую подпись и функцию хеширования	10	9	-	9	-	40	-	ПР-7; ОУ-1; ОУ-2
2	Специфические криптографические протоколы		8		8				
3	Практические криптографические протоколы		12		12				
4	Особенности применения криптографических алгоритмов на ИК		5		5				
	Итого:		34	-	34	-	40	-	

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Лекционные занятия (34 час.)

1. **Раздел I. Стандарты на цифровую подпись и функцию хеширования (9 час.)**

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

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

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

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

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

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

2. Раздел II. Специфические криптографические протоколы (8 час.)

Тема 1. Специфические подписи (3 час.)

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

Тема 2. Специфические протоколы (3 час.)

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

Тема 3. Безопасные выборы (2 час.)

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

Раздел III. Практические криптографические протоколы (12 час.)

Тема 1. Общие понятия (4 час.)

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

Тема 2. Протокол SSL (4 час.)

2 уровня подпротоколов. Протокол записи. Протокол извещения.

Протокол изменения параметров шифрования. Протокол квитирования. Схема работы протокола квитирования. Используемые криптопримитивы.

Тема 3. Протокол IPSec (4 час.)

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

Раздел IV. Особенности применения криптографических алгоритмов на ИК (5 час).

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

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

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

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

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА И САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Практические занятия (34 час.)

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

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

Занятие 2. Изучение специфических криптографических протоколов (11 час.)

1. Специфические подписи.
2. Специфические протоколы.

Занятие 3 Изучение практических криптографических протоколов (11 час.)

1. Протокол SSL
2. Протокол IPSec

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

План-график выполнения самостоятельной работы по дисциплине

№ п/п	Дата/сроки выполнения	Вид самостоятельной работы	Примерные нормы времени на выполнение	Форма контроля
1	1-10 недели обучения	Подготовка практических заданий (выполнение отчетов к практическим работам № 1-2)	16	Отчеты о выполнении
2	10-17 недели обучения	Подготовка практического задания (выполнение отчета к практической работе № 3)	16	Отчет о выполнении
3	18 недели обучения	Подготовка к зачету	4	Зачет

Рекомендации по самостоятельной работе студентов

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

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

Самостоятельная работа при подготовке к зачету включает изучение теоретического материала с использованием лекционных материалов, а также основной и дополнительной литературы из списка рекомендуемых источников.

Критерии оценки выполнения самостоятельной работы

Контроль самостоятельной работы студентов предусматривает:

- соотнесение содержания контроля с целями обучения;
- объективность контроля;
- валидность контроля (соответствие предъявляемых заданий тому, что предполагается проверить);
- дифференциацию контрольно-измерительных материалов.

Формы контроля самостоятельной работы

1. Просмотр и проверка выполнения самостоятельной работы преподавателем.
2. Самопроверка, взаимопроверка выполненного задания в группе.
3. Обсуждение результатов выполненной работы на занятии.
4. Тестирование.

Критерии оценки результатов самостоятельной работы

Критериями оценок результатов внеаудиторной самостоятельной работы студента являются:

- уровень освоения студентов учебного материала;
- умения студента использовать теоретические знания при выполнении практических задач;
- умения студента активно использовать электронные образовательные ресурсы, находить требующуюся информацию, изучать ее и применять на практике;
- обоснованность и четкость изложения ответа;
- оформление материала в соответствии с требованиями;
- умение ориентироваться в потоке информации, выделять главное;
- умение четко сформулировать проблему, предложив ее решение, критически оценить решение и его последствия;
- умение показать, проанализировать альтернативные возможности, варианты действий;
- умение сформировать свою позицию, оценку и аргументировать ее.

Критерии оценки выполнения контрольных заданий для

самостоятельной работы

Процент правильных ответов	**Оценка**
Более 61 %	зачет

IV. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

№ п/п	Контролируемые разделы / темы дисциплины	Код и наименование индикатора достижения	Результаты обучения	Оценочные средства	
				текущий контроль	промежуточная аттестация
1	Раздел I. Стандарты на цифровую подпись и функцию хеширования	ПК-9.1	знает	Собеседование (ОУ-1)	1-9
			умеет	Коллоквиум (ОУ-2)	1-9
			владеет	Конспект (ПР-7)	1-9
2	Раздел II. Специфические криптографические протоколы	ПК-10.1	знает	Собеседование (ОУ-1)	10-19
			умеет	Коллоквиум (ОУ-2)	10-19
			владеет	Конспект (ПР-7)	10-19
3	Раздел III. Практические криптографические протоколы	ПК-10.2	знает	Собеседование (ОУ-1)	20-28
			умеет	Коллоквиум (ОУ-2)	20-28
			владеет	Конспект (ПР-7)	20-28
4	Раздел IV. Особенности применения криптографических алгоритмов на ИК	ПК-9.1	знает	Собеседование (ОУ-1)	29-38
			умеет	Коллоквиум (ОУ-2)	29-38
			владеет	Конспект (ПР-7)	29-38

V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

(электронные и печатные издания)

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

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

Дополнительная литература

(печатные и электронные издания)

1. Де, К. Просто криптография / К. Де ; пер. с англ. Жуковой М — Санкт-Петербург : , 2014. — 208 с. — Режим доступа: https://e.lanbook.com/book/102340

2. Глухов, М.М. Введение в теоретико-числовые методы криптографии: учебное пособие / М.М. Глухов, И.А. Круглов, А.Б. Пичкур, А.В. Черемушкин — Санкт-Петербург : Лань, 2011. — 400 с. — Режим доступа: https://e.lanbook.com/book/68466

3. Серёдкин, А.Н. Основы защиты информации и информационные технологии. В 3 частях. Кн. 2: Криптография, криптоанализ и методы защиты информации в ИС и ИТ: учебное пособие / А.Н. Серёдкин, В.Р. Роганов, В.О. Филиппенко. — Пенза : ПензГТУ, 2013. — 180 с. — Режим доступа: https://e.lanbook.com/book/62755

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Основные виды криптографических протоколов [Электронный ресурс]. – Электрон. дан. – Режим доступа : http://infoprotect.net/varia/kriptograficheskie_protokolyi

2. ГОСТ Р 34.11-2012 [Электронный ресурс]. – Электрон. дан. – Режим доступа : https://fintender.ru/star/gost/r-34-11-2012

3. ГОСТ Р 34.11-94 [Электронный ресурс]. – Электрон. дан. – Режим доступа : https://fintender.ru/star/gost/r-34-11-94

VI.МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Планирование и организация времени, отведенного на изучение дисциплины. Приступить к освоению дисциплины следует незамедлительно в самом начале учебного семестра. Рекомендуется изучить структуру и основные положения Рабочей программы дисциплины. Обратить внимание, что кроме аудиторной работы (лекции, лабораторные занятия) планируется самостоятельная работа, итоги которой влияют на окончательную оценку по

итогам освоения учебной дисциплины. Все задания (аудиторные и самостоятельные) необходимо выполнять и предоставлять на оценку в соответствии с графиком.

В процессе изучения материалов учебного курса предлагаются следующие формы работ: чтение лекций, лабораторные занятия, задания для самостоятельной работы.

Лекционные занятия ориентированы на освещение вводных тем в каждый раздел курса и призваны ориентировать студентов в предлагаемом материале, заложить научные и методологические основы для дальнейшей самостоятельной работы студентов.

Практические занятия акцентированы на наиболее принципиальных и проблемных вопросах курса и призваны стимулировать выработку практических умений.

Особо значимой для профессиональной подготовки студентов является *самостоятельная работа* по курсу. В ходе этой работы студенты отбирают необходимый материал по изучаемому вопросу и анализируют его. Студентам необходимо ознакомиться с основными источниками, без которых невозможно полноценное понимание проблематики курса.

Освоение курса способствует развитию навыков обоснованных и самостоятельных оценок фактов и концепций. Поэтому во всех формах контроля знаний, особенно при сдаче зачета, внимание обращается на понимание проблематики курса, на умение практически применять знания и делать выводы.

Работа с литературой. Рекомендуется использовать различные возможности работы с литературой: фонды научной библиотеки ДВФУ и электронные библиотеки (http://www.dvfu.ru/library/), а также доступные для использования другие научно-библиотечные системы.

Подготовка к зачету. К сдаче зачета допускаются обучающиеся, выполнившие все задания (самостоятельные), предусмотренные учебной программой дисциплины, посетившие не менее 85% аудиторных занятий.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Перечень материально-технического и программного обеспечения дисциплины приведен в таблице.

Материально-техническое и программное обеспечение дисциплины

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты

		подтверждающего документа
Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 546, Компьютерный класс, аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	1) IBM SPSS Statistics Premium Campus Edition. Поставщик ЗАО Прогностические решения. Договор ЭА-442-15 от 18.01.16 лот 5. Срок действия договора 30.06.2016. Лицензия бессрочно. 2) SolidWorks Campus 500. Поставщик Солид Воркс Р. Договор 15-04-101 от 23.12.2015. Срок действия договора 15.03.2016. Лицензия бессрочно. 3) АСКОН Компас 3D v17. Поставщик Навиком. Договор 15-03-53 от 20.12.2015. Срок действия договора 31.12.2015. Лицензия бессрочно. 4) MathCad Education Universety Edition. Поставщик Софт Лайн Трейд. Договор 15-03-49 от 02.12.2015. Срок действия договора 30.11.2015. Лицензия бессрочно. 5) Corel Academic Site. Поставщик Софт Лайн Трейд. Договор ЭА-442-15 от 18.01.16 лот 4. Срок действия договора 30.06.2016. Лицензия закончилась 28.01.2019. 6) Microsoft Office, Microsoft Visual Studio. Поставщик Софт Лайн Трейд. Договор ЭА-261-18 от 02.08.18 лот 4. Срок действия договора 20.09.2018. Лицензия до 30.06.2020.	Перечень ПО
Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 546, Компьютерный класс, аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 15) Оборудование: Компьютер (твердотельный диск - объемом 128 ГБ; жесткий диск - объем 1000 ГБ; форм-фактор - Tower; комплектуется клавиатурой, мышью, монитором AOC i2757Fm; комплектом шнуров эл. питания) модель - M93p 1 Мультимедийное оборудование: Экран проекционный ScreenLine Trim White Ice 50 см черная кайма сверху, размер рабочей области 236x147 см Документ-камера Avervision CP355AF ЖК-панель 47"", Full HD, LG M4716 CCBA Мультимедийный проектор, Mitsubishi EW33OU, 3000 ANSI Lumen, 1280x800 Сетевая видеокамера Multipix MP-HD718"	Перечень ПО

VIII. ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ

Для дисциплины «Дополнительные главы криптографических протоколов» используются следующие оценочные средства:

Устный опрос:

1. Собеседование (УО-1)
2. Коллоквиум (УО-2)

Письменные работы:

1. Конспект (ПР-7)

Устный опрос

Устный опрос позволяет оценить знания и кругозор студента, умение логически построить ответ, владение монологической речью и иные коммуникативные навыки.

Собеседование (УО-1) – средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п.

Коллоквиум (УО-2) – средство контроля усвоения учебного материала темы, раздела или разделов дисциплины, организованное как учебное занятие в виде собеседования преподавателя с обучающимися.

Письменные работы

Письменный ответ приучает к точности, лаконичности, связности изложения мысли. Письменная проверка используется во всех видах контроля и осуществляется как в аудиторной, так и во внеаудиторной работе.

Конспект (ПР-7) – продукт самостоятельной работы обучающегося, отражающий основные идеи заслушанной лекции, сообщения и т.д.

Методические рекомендации, определяющие процедуры оценивания результатов освоения дисциплины

Оценочные средства для промежуточной аттестации

Промежуточная аттестация студентов по дисциплине «Дополнительные главы криптографических протоколов» проводится в соответствии с локальными нормативными актами ДВФУ и является обязательной. Форма отчётности по дисциплине – зачет (10-й, весенний семестр).

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

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.

Методические указания по сдаче зачета

Зачет принимается ведущим преподавателем. При большом количестве групп у одного преподавателя или при большой численности потока по распоряжению заведующего кафедрой (заместителя директора по учебной и воспитательной работе) допускается привлечение в помощь ведущему преподавателю других преподавателей. В первую очередь привлекаются преподаватели, которые проводили лабораторные занятия по дисциплине в группах.

В исключительных случаях, по согласованию с заместителем директора Школы по учебной и воспитательной работе, заведующий кафедрой имеет право принять зачет в отсутствие ведущего преподавателя.

Форма проведения зачета (устная, письменная и др.) утверждается на заседании кафедры по согласованию с руководителем в соответствии с рабочей программой дисциплины.

Во время проведения зачета студенты могут пользоваться рабочей программой дисциплины, а также с разрешения преподавателя, проводящего зачет, справочной литературой и другими пособиями (учебниками, учебными пособиями, рекомендованной литературой и т.п.).

Время, предоставляемое студенту на подготовку к ответу на зачете, должно составлять не более 20 минут. По истечении данного времени студент должен быть готов к ответу.

Присутствие на зачете посторонних лиц (кроме лиц, осуществляющих проверку) без разрешения соответствующих лиц (ректора либо проректора по учебной и воспитательной работе, директора Школы, руководителя ОПОП или заведующего кафедрой), не допускается. Инвалиды и лица с ограниченными возможностями здоровья, не имеющие возможности самостоятельного передвижения, допускаются зачет с сопровождающими.

При промежуточной аттестации обучающимся устанавливается оценка «зачтено» или «не зачтено».

В зачетную книжку студента вносится только запись «зачтено», запись «не зачтено» вносится только в экзаменационную ведомость. При неявке студента на зачет в ведомости делается запись «не явился».

Вопросы к зачету

1. Задачи, которые позволяет решать ЦП.
2. Сложностью каких задач определяется надежность ЦП.
3. Перечислить 3 класса ЦП.
4. В чем заключается проблема инфраструктуры открытых ключей.

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

38. Мощность конечного поля, количество элементов мультипликативной группы поля

Критерии выставления оценки студенту на зачете

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

При определении оценки учитываются:

- знание основных терминов и понятий курса;
- знание и владение методами и средствами решения задач;
- последовательное изложение материала курса;
- умение формулировать некоторые обобщения по теме вопросов;
- достаточно полные ответы на вопросы;
- умение использовать фундаментальные понятия из базовых естественнонаучных и общепрофессиональных дисциплин при ответе.

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

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

Оценочные средства для текущей аттестации

В качестве оценочных средств для текущей аттестации применяется конспект (ПР-7).

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

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

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

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

Вопросы для собеседования / устного опроса

В качестве оценочных средств для текущей аттестации применяется конспект (ПР-7).

Темы конспектов соответствуют темам теоретической части курса из Раздела II РПУД. Критерии оценки по данному виду оценочных средств представлены в таблице:

Критерии оценивания

Оценка	Требования
«зачтено»	Студент показал развернутый ответ на вопрос, знание литературы, обнаружил понимание материала, обоснованность суждений, неточности в ответе исправляет самостоятельно.
«не зачтено»	Студент обнаруживает незнание вопроса, неуверенно излагает ответ.

Тематика контрольно-расчетных работ

1. Контрольно-расчетная работа представлена индивидуальным домашним заданием, последовательно охватывающим все темы курса.

Критерии оценки контрольно-расчетных работ

Оценка	Требования
«зачтено»	Студент выполнил контрольно-расчетную работу в полном объёме с соблюдением необходимой последовательности этапов проведения работы, самостоятельно строит профиль под контролем преподавателя, при необходимости задает наводящие вопросы. Допускается неточность тех линий, по которым нет достаточной информации, но в логических пределах.
«не зачтено»	Студент выполнил работу не полностью, объём выполненной части не позволяет самостоятельно выстроить профиль; в ходе работы допускает грубые ошибки, которые не может исправить. Контрольно-расчетная работа не выполнена.