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
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.
всего часов аудиторной нагрузки 126 час.
в том числе с использованием МАО 46 час.
самостоятельная работа 90 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 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.

Составители: Добржинский Ю.В.

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)

Цели и задачи освоения дисциплины:

Цель: 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:

- 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.

Общепрофессиональные компетенции выпускников и индикаторы их достижения:

Наименование категории (группы) общепрофессиональных компетенций	**Код и наименование общепрофессиональной компетенции (результат освоения)**	**Код и наименование индикатора достижения компетенции**
	ОПК-2.1 Способен разрабатывать алгоритмы, реализующие современные математические методы защиты информации	ОПК-2.1.2 Анализирует и выбирает современные математические методы защиты информации
		ОПК-2.1.3 Осуществляет разработку алгоритмов, реализующих современные математические методы защиты информации
	ОПК-2.2 Способен разрабатывать и анализировать математические модели механизмов защиты информации	ОПК-2.2.3 Разрабатывает математические модели механизмов защиты информации

Код и наименование индикатора достижения общепрофессиональной компетенции	**Наименование показателя оценивания (результата обучения по дисциплине)**
ОПК-2.1.2 Анализирует и выбирает современные математические методы защиты информации	Знает групповой закон, эндоморфизмы, функции Вейерштрасса, модулярные формы, комплексное умножение Умеет оценивать качество криптографической защиты Владеет навыками формирования требований, предъявляемых к криптографическим средствам защиты информации
ОПК-2.1.3 Осуществляет разработку алгоритмов, реализующих современные математические методы защиты информации	Знает эллиптические кривые над кольцами Умеет выбирать параметры эллиптических кривых для реализации средств защиты информации Владеет способами расчета характеристик методов криптографического анализа в зависимости от их параметров
ОПК-2.2.3 Разрабатывает	Знает основные понятия алгебраической геометрии: аффинные и

математические модели механизмов защиты информации	проективные пространства, алгебраические многообразия, дивизоры Умеет выбирать параметры эллиптических кривых для достижения заданных свойств Владеет навыками криптоанализа асимметричных систем шифрования

1. Трудоёмкость дисциплины и видов учебных занятий по дисциплине

Общая трудоемкость дисциплины составляет 6 зачётных единиц (216 академических часов).

(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
Лаб	Лабораторные работы
СР	Самостоятельная работа обучающегося в период теоретического обучения
Контроль	Самостоятельная работа обучающегося и контактная работа обучающегося с преподавателем в период промежуточной аттестации

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	1. Введение	6	4	4	8				
2	2. Общие сведения о криптографических протоколах	6	6	6	8				
3	3. Криптографические хеш-функции и коды аутентификации	6	6	6	8				
4	4. Схемы электронных подписей	6	6	6	10	-	54	36	экзамен
5	5. Протоколы идентификации и аутентификации	6	6	6	10				
6	6. Протоколы распределения ключей	6	8	8	10				
	Итого:		36	36	54	-	54	36	

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Тема 1. Введение

Основные понятия и определения. Функции — сервисы безопасности. Понятие криптографического протокола. Конфиденциальность. Целостность. Аутентификация. Невозможность отказа от авторства (электронная подпись).

Тема 2. Общие сведения о криптографических протоколах

Свойства, характеризующие безопасность протоколов. Основные атаки на безопасность протоколов. Основные виды криптографических протоколов. Формальные методы анализа криптопротоколов.

Тема 3. Криптографические хеш-функции и коды аутентификации

Требования к криптографическим хеш-функциям. Бесключевые хеш-функции. Основы построения хеш-функций. Хеш-функция на основе блочного алгоритма. Хеш-функция MD4 и MD5. Стандарты на хеш-функции. Хеш-функции, задаваемые ключом. Коды аутентификации сообщений – MAC.

Тема 4. Схемы электронных подписей

Определение схемы электронной подписи. Алгоритм цифровой подписи RSA. Семейство схем типа Эль-Гамаля. Схема подписи Fiat-Shamir. Инфраструктура открытых ключей PKI. Рекомендации X.509. Электронные подписи с дополнительными функциональными свойствами.

Тема 5. Протоколы идентификации и аутентификации

Протоколы аутентификации на основе паролей. Протоколы идентификации типа «запрос-ответ» и рукопожатие. Понятие проколов интерактивного доказательства и доказательства знания. Протоколы с нулевым разглашением. Протоколы Фиата-Шамира, Гиллу-Кискатра и Шнорра. Протоколы с самосертифицируемыми ключами.

Тема 6. Протоколы распределения ключей

Протоколы генерации и передачи ключей. Примеры протоколов передачи ключей на основе симметричного и открытого шифрования. Двух и трех сторонние протоколы, Kerberos. Функции доверенной третьей стороны. Передача ключей с использованием асимметричного шифрования. Открытое распределение ключей. Протокол Диффи-Хеллмана и его модификации. Схемы предварительного распределения ключей. Групповые протоколы. Протоколы разделения секрета и распределения ключей для конференцсвязи. Способы установления ключей для конференцсвязи.

II.СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Лабораторные работы

Лабораторная работа 1. Функции — сервисы безопасности.

Лабораторная работа 2. Методы анализа криптопротоколов.

Лабораторная работа 3. Криптографические хеш-функции и коды аутентификации.

Лабораторная работа 4. Электронные подписи типа Эль-Гамаля. Схема подписи Fiat-Shamir.

Лабораторная работа 5. Протоколы аутентификации на основе паролей.

Лабораторная работа 6. Двух и трех сторонние протоколы, Kerberos. Функции доверенной третьей стороны.

Практические занятия

Занятие №1. Практическая работа. Конфиденциальность. Целостность. Аутентификация.

Занятие №2. Практическая работа. Формальные методы анализа криптопротоколов.

Занятие №3. Практическая работа. Построение хеш-функций. Хеш-функция на основе блочного алгоритма. Хеш-функция MD4 и MD5. Хеш-функции, задаваемые ключом. Коды аутентификации сообщений – MAC.

Занятие №4. Практическая работа. Электронные подписи с дополнительными функциональными свойствами.

Занятие №5 Практическая работа. Протоколы идентификации типа «запрос-ответ» и рукопожатие. Протоколы с самосертифицируемыми ключами.

Занятие №6 Практическая работа. Передача ключей с использованием асимметричного шифрования. Открытое распределение ключей. Протокол Диффи-Хеллмана и его модификации.

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	1-18 недели обучения	Изучение литературы, конспектов лекций. Подготовка к лабораторным и практическим занятиям.	54	ПР-6
2	Сессия	Подготовка к экзамену	36	Экзамен

Рекомендации по самостоятельной работе студентов

Самостоятельная работа студента включает в себя подготовку к практическим и лабораторным занятиям, изучение литературы, подготовку к экзамену.

Подготовка к практическим и лабораторным занятиям предполагает повторение лекционного материала, а также самостоятельную работу с дополнительными источниками из списка рекомендаций. В результате

самостоятельной подготовки студент должен быть готов к выполнению практических и лабораторных работ.

Самостоятельная работа при подготовке к экзамену состоит из повторения всего материала, изученного на лекционных, лабораторных и практических занятиях, с использованием основных и дополнительных источников информации.

Подготовка отчетов к лабораторным и практическим занятиям предполагает повторение лекционного материала и выполнение практических и лабораторных работ. В результате студент должен представить отчеты о проделанной работе.

Методические рекомендации к работе с литературными источниками

В процессе подготовки к практическим занятиям, студентам необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у студентов свое отношение к конкретной проблеме. Более глубокому раскрытию вопросов способствует знакомство с дополнительной литературой, рекомендованной преподавателем.

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.

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	1. Введение	ОПК-2.1.2 ОПК-2.1.3 ОПК-2.2.3	Знает Умеет Владеет	ПР-7 ПР-6	экзамен
2	2. Общие сведения о криптографических протоколах	ОПК-2.1.2 ОПК-2.1.3 ОПК-2.2.3	Знает Умеет Владеет	ПР-7 ПР-6	экзамен
3	3. Криптографические хеш-функции и коды аутентификации	ОПК-2.1.2 ОПК-2.1.3 ОПК-2.2.3	Знает Умеет Владеет	ПР-7 ПР-6	экзамен
4	4. Схемы электронных подписей	ОПК-2.1.2 ОПК-2.1.3 ОПК-2.2.3	Знает Умеет Владеет	ПР-7 ПР-6	экзамен
5	5. Протоколы идентификации и аутентификации	ОПК-2.1.2 ОПК-2.1.3 ОПК-2.2.3	Знает Умеет Владеет	ПР-7 ПР-6	экзамен
6	6. Протоколы распределения ключей	ОПК-2.1.2 ОПК-2.1.3 ОПК-2.2.3	Знает Умеет Владеет	ПР-7 ПР-6	экзамен

V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

1. Земор, Ж. Курс криптографии [Электронный ресурс] / Ж. Земор. — Электрон. текстовые данные. — Москва, Ижевск: Регулярная и хаотическая динамика, Ижевский институт компьютерных исследований, 2006. — 256 c. — 5-93972-510-4. — Режим доступа: http://www.iprbookshop.ru/16547.html.
2. Коржик, В. И. Основы криптографии [Электронный ресурс]: учебное пособие / В. И. Коржик, В. А. Яковлев. — Электрон. текстовые данные. — СПб.: Интермедия, 2017. — 312 c.— Режим доступа: http://www.iprbookshop.ru/66798.html.
3. Лапонина, О. Р. Основы сетевой безопасности. Криптографические алгоритмы и протоколы взаимодействия [Электронный ресурс] / О.Р. Лапонина. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 242 c.

— 5-9556-00020-5. — Режим доступа: http://www.iprbookshop.ru/52217.html.
4. Ожиганов, А. А. Криптография [Электронный ресурс] : учебное пособие / А. А. Ожиганов. — Электрон. текстовые данные. — СПб. : Университет ИТМО, 2016. — 142 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/67231.html.

Дополнительная литература

(печатные и электронные издания)

1. Аграновский, А. В. Практическая криптография. Алгоритмы и их программирование [Электронный ресурс] / А.В. Аграновский, Р.А. Хади. — Электрон. текстовые данные. — М. : СОЛОН-ПРЕСС, 2009. — 256 с.— Режим доступа: http://www.iprbookshop.ru/8641.html
2. Кукина, Е. Г. Введение в криптографию [Электронный ресурс]: сборник задач и упражнений / Е.Г. Кукина, В.А. Романьков. — Электрон. текстовые данные. — Омск: Омский государственный университет им. Ф.М. Достоевского, 2013. — 91 с.— Режим доступа: http://www.iprbookshop.ru/24876.html
3. Романьков, В. А. Алгебраическая криптография [Электронный ресурс] : монография / В.А. Романьков. — Электрон. текстовые данные. — Омск: Омский государственный университет им. Ф.М. Достоевского, 2013. — 136 с. — Режим доступа: http://www.iprbookshop.ru/24868.html
4. Семенов, Ю. А. Процедуры, диагностики и безопасность в Интернет [Электронный ресурс] / Ю.А. Семенов. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 581 с. — Режим доступа: http://www.iprbookshop.ru/62827.html.
5. Черемушкин, А. В. Криптографические протоколы. Основные свойства и уязвимости.- М., Академия, 2009. – 272 с.
6. Швечкова, О. В. Алгоритмы электронной подписи. Схема Эль-Гамаля. – Рязань, РГРТА, 2013. – 16 с.
7. Фороузан Бехроуз А. Криптография и безопасность сетей [Электронный ресурс] : учебное пособие / БехроузА. Фороузан. — Электрон. текстовые данные. — Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. — 782 с.— Режим доступа: http://www.iprbookshop.ru/72337.html

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Электронно-библиотечная система «Лань». https://e.lanbook.com/

2. Электронно-библиотечная система «IPRbooks». https://iprbookshop.ru/.

3. Библиотека и форум по программированию. http://www.cyberforum.ru

4. Национальный открытый университет ИНТУИТ. http://www.intuit.ru/

5. Информационно-справочная система http://window.edu.ru

6. Научная электронная библиотека КиберЛенинка http://cyberleninka.ru

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, практические занятия) планируется самостоятельная работа. 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, практические занятия.

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 и лабораторные 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.

Методические указания для подготовки к лабораторным и практическим занятиям

Структура отчета по лабораторной/практической работе

Отчеты по работам представляются в электронной форме, подготовленные как текстовые документы в редакторе MSWord.

Отчет должен быть обобщающим документом, включать всю информацию по выполнению заданий, в том числе таблицы список литературы необходимыми пояснениями и иллюстрациями.

Структурно отчет по работе, как текстовый документ, комплектуется по следующей схеме:

- ✓ *Титульный лист – обязательная* компонента отчета, первая страница отчета, по принятой для лабораторных работ форме (титульный лист отчета должен размещаться в общем файле, где представлен текст отчета);
- ✓ *Исходные данные к выполнению заданий* – обязательная компонента отчета, с новой страницы, содержат указание варианта, темы и т.д.);
- ✓ *Основная часть* – материалы выполнения заданий, разбивается по рубрикам, соответствующих заданиям работы, с иерархической структурой: разделы – подразделы – пункты – подпункты и т. д.

Рекомендуется в основной части отчета заголовки рубрик (подрубрик) давать исходя из формулировок заданий, в форме отглагольных существительных;

- ✓ *Выводы* – обязательная компонента отчета, содержит обобщающие выводы по работе (какие задачи решены, оценка результатов, что освоено при выполнении работы);
- ✓ *Список литературы* – обязательная компонента отчета, с новой страницы, содержит список источников, использованных при выполнении работы, включая электронные источники (список нумерованный, в соответствии с правилами описания библиографии);
- ✓ *Приложения* – необязательная компонента отчета, с новой страницы, содержит дополнительные материалы к основной части отчета.

Оформление отчета по лабораторной/практической работе

Необходимо обратить внимание на следующие аспекты в оформлении отчетов работ:

- набор текста;
- структурирование работы;
- оформление заголовков всех видов (рубрик-подрубрик-пунктов-подпунктов, рисунков, таблиц, приложений);
- оформление перечислений (списков с нумерацией или маркировкой);
- оформление таблиц;
- оформление иллюстраций (графики, рисунки, фотографии, схемы, «скриншоты»);

- набор и оформление математических выражений (формул);
- оформление списков литературы (библиографических описаний) и ссылок на источники, цитирования.

Набор текста

Набор текста осуществляется на компьютере, в соответствии со следующими требованиями:

✓ печать – на одной стороне листа белой бумаги формата А4 (размер 210 на 297 мм.);

✓ интервал межстрочный – полуторный;

✓ шрифт – TimesNewRoman;

✓ размер шрифта – 14 пт., в том числе в заголовках (в таблицах допускается 10-12 пт.);

✓ выравнивание текста – «по ширине»;

✓ поля страницы – левое - 30 мм., правое - 10 мм., верхнее и нижнее - 20 мм.;

✓ нумерация страниц – в правом нижнем углу страницы (для страниц с книжной ориентацией), сквозная, от титульного листа до последней страницы, арабскими цифрами (первой страницей считается титульный лист, на котором номер не ставиться, на следующей странице проставляется цифра «2» и т. д.).

✓ режим автоматического переноса слов, за исключением титульного листа и заголовков всех уровней (перенос слов для отдельного абзаца блокируется средствами MSWord с помощью команды «Формат» – абзац при выборе опции «запретить автоматический перенос слов»).

Если рисунок или таблица размещены на листе формата больше А4, их следует учитывать, как одну страницу. Номер страницы в этих случаях допускается не проставлять.

Список литературы и все *приложения* включаются в общую сквозную нумерацию страниц работы.

Подготовка к экзамену. К сдаче экзамена 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.	Помещение укомплектовано специализированной учебной мебелью (посадочных мест –	1) IBM SPSS Statistics Premium Campus Edition. Поставщик ЗАО Прогностические решения. Договор

10, корпус L, ауд. L 506, специализированная лаборатория кафедры компьютерных систем: Лаборатория электроники и сверхвысоких частот. Учебная аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	15) Оборудование: 3 4-х канальных цифровых модуля визуализ. сигналов: Цифровой осциллограф С1-65, 4 вольтметра GVT-417B, столы лабораторные и стулья, доска аудиторная, переносной компьютер (ноутбук Lenovo) с сумкой – 1 шт	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.

VIII. ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ

Код и наименование индикатора достижения общепрофессиональной компетенции	**Наименование показателя оценивания (результата обучения по дисциплине)**
ОПК-2.1.2 Анализирует и выбирает современные математические методы защиты информации	Знает групповой закон, эндоморфизмы, функции Вейерштрасса, модулярные формы, комплексное умножение Умеет оценивать качество криптографической защиты Владеет навыками формирования требований, предъявляемых к криптографическим средствам защиты информации
ОПК-2.1.3 Осуществляет разработку алгоритмов, реализующих современные математические методы защиты информации	Знает эллиптические кривые над кольцами Умеет выбирать параметры эллиптических кривых для реализации средств защиты информации Владеет способами расчета характеристик методов криптографического анализа в зависимости от их параметров
ОПК-2.2.3 Разрабатывает математические модели механизмов защиты информации	Знает основные понятия алгебраической геометрии: аффинные и проективные пространства, алгебраические многообразия, дивизоры Умеет выбирать параметры эллиптических кривых для достижения заданных свойств Владеет навыками криптоанализа асимметричных систем шифрования

Контроль достижения целей курса

№ п/п	**Контролируемые разделы / темы дисциплины**	**Код и наименование индикатора достижения**	**Результаты обучения**	**Оценочные средства**	
				текущий контроль	**промежуточная аттестация**
1	1. Введение	ОПК-2.1.2	Знает	ПР-7	экзамен

		ОПК-2.1.3 ОПК-2.2.3	Умеет Владеет	ПР-6	
2	2. Общие сведения о криптографических протоколах	ОПК-2.1.2 ОПК-2.1.3 ОПК-2.2.3	Знает Умеет Владеет	ПР-7 ПР-6	экзамен
3	3. Криптографические хеш-функции и коды аутентификации	ОПК-2.1.2 ОПК-2.1.3 ОПК-2.2.3	Знает Умеет Владеет	ПР-7 ПР-6	экзамен
4	4. Схемы электронных подписей	ОПК-2.1.2 ОПК-2.1.3 ОПК-2.2.3	Знает Умеет Владеет	ПР-7 ПР-6	экзамен
5	5. Протоколы идентификации и аутентификации	ОПК-2.1.2 ОПК-2.1.3 ОПК-2.2.3	Знает Умеет Владеет	ПР-7 ПР-6	экзамен
6	6. Протоколы распределения ключей	ОПК-2.1.2 ОПК-2.1.3 ОПК-2.2.3	Знает Умеет Владеет	ПР-7 ПР-6	экзамен

Для дисциплины используются следующие оценочные средства:

1. Конспект (ПР-7)
2. Лабораторные работы (ПР-6)
3. Практические работы (ПР-6)

Текущая аттестация

ПР-7 Конспект - продукт самостоятельной работы обучающегося, отражающий основные идеи заслушанной лекции.

Цели конспектирования состоят в:

- развитии умений систематизировать знания и выделять причинно-следственные связи, выявлять закономерности;
- развитии умений перерабатывать любую информацию, придавая ей иной вид, тип, форму;
- развитии навыков осмысленной переработки текста, структурирования информации, использования основных категорий анализа, работы с большими объемами информации;
- создании модели проблемы (понятийную или структурную).

Требования к представлению и оцениванию материалов (результатов):

В связи с объективным характером конспектирования не предлагается единых и обязательных параметров конспектируемого текста (степень сокращения информации). Объем законспектированного текста определяется

самим студентом. Конспект должен быть подготовлен каждым студентом самостоятельно и отражать основные идеи изученной темы.

Перечень вопросов, необходимых для конспектирования определяется темой лекционного занятия. Конспекты выполняются во время лекционных занятий, и проверяются преподавателем в конце семестра.

Критерии оценки:

Уровень освоения	Критерии оценки результатов обучения	Количество баллов / оценка
Повышенный	Конспекты лекций в наличии. Студент демонстрирует отчетливое и свободное владение концептуально-понятийным аппаратом, научным языком и терминологией соответствующей научной области. Логически корректное изложение материала.	100-86 Зачтено
Базовый	Конспекты лекций в наличии. Студент показывает умение пользоваться концептуально-понятийным аппаратом. В целом логически корректное, но не всегда точное изложение материала.	85-76 Зачтено
Пороговый	Конспекты лекций в наличии. Студент показывает затруднение с использованием научно-понятийного аппарата; частичные затруднения с выполнением конспекта.	75-61 Зачтено
Уровень не достигнут	Конспекты лекций отсутствуют или студент показывает отрывочное представление о теме.	60-0 Не зачтено

Лабораторная работа (ПР-6) – средство для закрепления и практического освоения материала по определенной теме.

Цель лабораторных работ – выработка у учащихся профессиональных умений применять полученные знания для решения практических задач, умений и навыков пользоваться подходами и методами информационной безопасности для осуществления профессиональной деятельности.

Во всех лабораториях существуют особые правила поведения студентов, которые необходимо неукоснительно соблюдать – правила техники безопасности. За знание правил техники безопасности и обязательство их выполнять каждый студент должен расписаться в соответствующем журнале.

Обработка результатов и оформление отчета проводится в течение недели после выполнения работы. Студент, не сдавший отчета в срок, к следующей работе не допускается.

Требования к представлению и оцениванию материалов (результатов):

Выполнение лабораторной работы осуществляется студентом самостоятельно в часы лабораторных занятий.

При оценке работы студента преподаватель учитывает все этапы работы студента над отчетом. Если отчет не был принят преподавателем и возвращен для доработки, то все исправления вносятся в тот же экземпляр отчета.

При оценке учитывается правильность выполнения отчета. Выставляется дифференцированный зачет.

Критерии оценки:

Уровень освоения	Критерии оценки результатов обучения	Количество баллов / оценка
Повышенный	Студент показал прочные знания основных понятий и их взаимосвязей, сущности процессов, рассматриваемых в работе, и умение их объяснить, знание методов, используемых в работе, методики обработки результатов. Показано хорошее понимание профессиональной значимости изучаемых вопросов. При выполнении экспериментальной части работы и оформлении отчета студент показал умение работать с данными и владение навыками представления и обработки результатов, умение делать выводы по результатам работы. Отчет по работе оформлен аккуратно, в соответствии с требованиями, структурирован, не содержит ошибок; правильно и полно сформулирован вывод по работе.	100 – 86 Зачтено (отлично)
Базовый	Студент показал знания основных понятий и их взаимосвязей, сущности процессов, рассматриваемых в работе, и умение их объяснить, знание методов, используемых в работе, методики обработки результатов. Показано хорошее понимание профессиональной значимости изучаемых	85-76 Зачтено (хорошо)

	вопросов. При выполнении экспериментальной части работы и оформлении отчета студент показал умение работать с данными и владение навыками представления и обработки результатов, умение делать выводы по результатам работы. Отчет по работе оформлен аккуратно, в основном – в соответствии с требованиями, структурирован; правильно и полно сформулирован вывод по работе. Допускаются не более 2-х недочетов в оформлении отчета.	
Пороговый	Студент показал базовые знания основных понятий и их взаимосвязей, сущности процессов, рассматриваемых в работе, и умение их объяснить, демонстрирует, в целом, знание методов, используемых в работе, методики обработки результатов. При выполнении экспериментальной части работы и оформлении отчета студент в целом показал умение работать с данными и владение навыками представления и обработки результатов, умение делать выводы по результатам работы. Отчет по работе оформлен аккуратно, в основном в соответствии с требованиями, не содержит грубых ошибок, вывод по работе сформулирован.	75-61 Зачтено (удовлетворительно)
Уровень не достигнут	Студент не выполнил лабораторную работу, либо показал незнание основных понятий, сущности процессов, рассматриваемых в работе, демонстрирует плохое знание или незнание методов, методики обработки результатов. Слабо сформировано или не сформировано умение работать с данными, отсутствуют выводы по результатам работы. Отчет не соответствует требованиям, не сделан или сделан с грубыми ошибками.	60-0 Не зачтено (неудовлетворительно)

Практическая работа (ПР-6) – средство для закрепления и практического освоения материала по определенной теме.

Цель практических работ – выработка у учащихся профессиональных умений применять полученные знания для решения практических задач.

Обработка результатов и оформление отчета проводится в течение недели после выполнения работы. Студент, не сдавший отчета в срок, к следующей работе не допускается.

Требования к представлению и оцениванию материалов (результатов):

Выполнение практических работ осуществляется студентом в часы практических занятий.

При оценке работы студента преподаватель учитывает все этапы работы студента над отчетом. Если отчет не был принят преподавателем и возвращен для доработки, то все исправления вносятся в тот же экземпляр отчета.

При оценке учитывается правильность выполнения отчета. Выставляется дифференцированный зачет.

Критерии оценки:

Уровень освоения	Критерии оценки результатов обучения	Количество баллов / оценка
Повышенный	Студент показал прочные знания основных понятий и их взаимосвязей, сущности процессов, рассматриваемых в работе, и умение их объяснить, знание методов, используемых в работе, методики обработки результатов. Показано хорошее понимание профессиональной значимости изучаемых вопросов. При оформлении отчета студент показал умение работать с данными и владение навыками представления и обработки результатов, умение делать выводы по результатам работы. Отчет по работе оформлен аккуратно, в соответствии с требованиями, структурирован, не содержит ошибок; правильно и полно сформулирован вывод по работе.	100 – 86 Зачтено (отлично)
Базовый	Студент показал знания основных понятий и их взаимосвязей, сущности процессов, рассматриваемых в работе, и умение их объяснить, знание методов, используемых в работе, методики обработки результатов. Показано хорошее понимание профессиональной значимости изучаемых вопросов. При оформлении отчета студент показал умение работать с данными и владение навыками представления и обработки результатов, умение делать выводы по результатам работы. Отчет по работе оформлен аккуратно, в основном – в соответствии с требованиями, структурирован; правильно и	85-76 Зачтено (хорошо)

	полно сформулирован вывод по работе. Допускаются не более 2-х недочетов в оформлении отчета.	
Пороговый	Студент показал базовые знания основных понятий и их взаимосвязей, сущности процессов, рассматриваемых в работе, и умение их объяснить, демонстрирует, в целом, знание методов, используемых в работе, методики обработки результатов. При оформлении отчета студент в целом показал умение работать с данными и владение навыками представления и обработки результатов, умение делать выводы по результатам работы. Отчет по работе оформлен аккуратно, в основном в соответствии с требованиями, не содержит грубых ошибок, вывод по работе сформулирован.	75-61 Зачтено (удовлетворительно)
Уровень не достигнут	Студент не выполнил работу, либо показал незнание основных понятий, сущности процессов, рассматриваемых в работе, демонстрирует плохое знание или незнание методов, методики обработки результатов. Слабо сформировано или не сформировано умение работать с данными, отсутствуют выводы по результатам работы. Отчет не соответствует требованиям, не сделан или сделан с грубыми ошибками.	60-0 Не зачтено (неудовлетворительно)

Оценочные средства для промежуточной аттестации

Оценочные средства для промежуточной аттестации

Промежуточная аттестация студентов по дисциплине проводится в соответствии с локальными нормативными актами ДВФУ и является обязательной. Форма отчётности по дисциплине – экзамен (6-й, весенний семестр). Промежуточная форма аттестации по данной дисциплине – экзамен.

Для допуска к экзамену необходимо сдать все практические и лабораторные работы. В случае, если ко дню проведения экзамена обучающийся не сдал какие-либо отчеты, он получает возможность сдать их на экзамене.

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

При определении оценки ответа обучающегося на экзамене учитываются:

-соблюдение норм литературной речи;

-полнота и содержательность ответа;

-умение привести примеры;

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

Методические указания по сдаче экзамена

Во время проведения экзамена 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 экзамене, должно составлять не более 30 минут. По истечении данного времени студент должен быть готов к ответу.

Присутствие на экзамене 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/директора департамента), не допускается. Инвалиды и лица с ограниченными возможностями здоровья, не имеющие возможности самостоятельного передвижения, допускаются на экзамен с сопровождающими.

Вопросы к экзамену

1. Функции — сервисы безопасности.
2. Понятие криптографического протокола.
3. Конфиденциальность. Целостность. Аутентификация.
4. Невозможность отказа от авторства (электронная подпись).
5. Свойства, характеризующие безопасность протоколов.
6. Основные атаки на безопасность протоколов.
7. Основные виды криптографических протоколов.
8. Формальные методы анализа криптопротоколов.
9. Требования к криптографическим хеш-функциям.
10. Бесключевые хеш-функции.
11. Основы построения хеш-функций.
12. Хеш-функция на основе блочного алгоритма.
13. Хеш-функция MD4 и MD5.

14. Стандарты на хеш-функции.

15. Хеш-функции, задаваемые ключом.

16. Коды аутентификации сообщений – MAC.

17. Определение схемы электронной подписи.

18. Алгоритм цифровой подписи RSA.

19. Семейство схем типа Эль-Гамаля.

20. Схема подписи Fiat-Shamir.

21. Инфраструктура открытых ключей PKI. Рекомендации X.509.

22. Электронные подписи с дополнительными функциональными свойствами.

23. Протоколы аутентификации на основе паролей.

24. Протоколы идентификации типа «запрос-ответ» и рукопожатие.

25. Понятие проколов интерактивного доказательства и доказательства знания.

26. Протоколы с нулевым разглашением.

27. Протоколы Фиата-Шамира, Гиллу-Кискатра и Шнорра.

28. Протоколы с самосертифицируемыми ключами.

29. Протоколы генерации и передачи ключей.

30. Примеры протоколов передачи ключей на основе симметричного и открытого шифрования.

31. Двух и трех сторонние протоколы, Kerberos.

32. Функции доверенной третьей стороны.

33. Передача ключей с использованием асимметричного шифрования.

34. Открытое распределение ключей. Протокол Диффи-Хеллмана и его модификации.

35. Схемы предварительного распределения ключей.

36. Групповые протоколы.

37. Протоколы разделения секрета и распределения ключей для конференцсвязи.

38. Способы установления ключей для конференцсвязи.

Критерии выставления оценки студенту на экзамене:

Баллы (рейтинговой оценки)	Оценка (стандартная)	Требования к сформированным компетенциям
86-100	«отлично»	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал монографической литературы, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач.
76-85	«хорошо»	Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения.
61-75	«удовлетворительно»	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ.
0-60	«неудовлетворительно»	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ результатов обучения по дисциплине				
Оценка / виды оценочных средств	2 (не зачтено)	3 (зачтено)	4 (зачтено)	5 (зачтено)

Знания *(виды оценочных средств: конспект, практическая работа, лабораторная работа)*	Отсутствие знаний	Фрагментарные знания	Общие, но не структурированные знания	Сформированные систематические знания
Умения *(виды оценочных средств: практическая работа, лабораторная работа)*	Отсутствие умений	В целом успешное, но не систематическое умение	В целом успешное, но содержащее отдельные пробелы умение (допускает неточности непринципиального характера)	Успешное и систематическое умение
Навыки (владения, опыт деятельности)	Отсутствие навыков (владений, опыта)	Наличие отдельных навыков (наличие фрагментарного опыта)	В целом, сформированные навыки (владения), но используемые не в активной форме	Сформированные навыки (владения), применяемые при решении задач