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
Подпись Дремлюга Р.И.

«УТВЕРЖДАЮ»
И.о. директора департамента
Боршевников А.Е.
«27» сентября 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Прикладная криптография
Направление подготовки - 09.04.01 Информатика и вычислительная техника
(Кибербезопасность)
Форма подготовки очная

курс 2 семестр 3
лекции 00 час.
практические занятия 54 час.
лабораторные работы 00 час.
в том числе с использованием МАО практические занятия 36 час.
всего часов аудиторной нагрузки 54 час.
самостоятельная работа 90 час.
в том числе на подготовку к экзамену 00 час.
контрольные работы (количество) не предусмотрены
курсовая работа / курсовой проект не предусмотрены
зачет с оценкой 3 семестр
экзамен не предусмотрен

Рабочая программа дисциплины разработана в соответствии с требованиями Федерального государственного образовательного стандарта по направлению подготовки 09.04.01 Информатика и вычислительная техника, утвержденного приказом Министерства образования и науки Российской Федерации от 19.09.2017 г. № 918 (с изменениями и дополнениями)

Рабочая программа обсуждена на заседании департамента информационной безопасности протокол № 1 от 27 сентября 2021 г.

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

Составитель (ли): Антонова А.А.

Владивосток
2021

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)

I. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель: дать слушателям специализированные знания о технологиях прикладной криптографии.

Задачи:

Предоставить слушателям программы теоретические и практические знания криптографии, через раскрытие следующих тем:

- Протоколы, алгоритмы, исходные тексты на языке С(Си)»;
- Принципы работы, реализации и примеры использования криптографических алгоритмов.

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные/ профессиональные компетенции.

Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы, характеризуют формирование следующих компетенций:

Код и наименование профессиональной компетенции (результат освоения)	**Код и наименование индикатора достижения компетенции**
ПК-1 Способен разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей	ПК-1.1 Применяет на практике знания нормативно-правовых актов, национальных, межгосударственных и международных стандартов в области защиты информации
	ПК-1.2 Анализирует компьютерную систему с целью определения необходимого уровня защищенности и доверия; формулирует задания по безопасности компьютерных систем
	ПК-1.3 Разрабатывает требования по защите и умеет формировать политики безопасности компьютерных систем и сетей

Код и наименование индикатора достижения компетенции	**Наименование показателя оценивания (результата обучения по дисциплине)**
ПК-1.1 Применяет на практике знания нормативно-правовых актов, национальных, межгосударственных и международных стандартов в области защиты информации	Знает корректные нормативно-правовые акты, национальных, межгосударственных и международных стандартов в области защиты информации
	Умеет применять нормативно-правовые акты, национальных, межгосударственных и международных стандартов в области защиты информации
	Владеет методами определения ключевых аспектов нормативно-правовых актов, национальных, межгосударственных и международных стандартов в области защиты информации
ПК-1.2 Анализирует компьютерную систему с целью определения	Знает основные методы анализа компьютерных систем с целью определения необходимого уровня защищенности и доверия

Код и наименование индикатора достижения компетенции	Наименование показателя оценивания (результата обучения по дисциплине)
необходимого уровня защищенности и доверия; формулирует задания по безопасности компьютерных систем	Умеет подбирать методы анализа по безопасности компьютерных систем
	Владеет навыками формулировки задания по безопасности компьютерных систем
ПК-1.3 Разрабатывает требования по защите и умеет формировать политики безопасности компьютерных систем и сетей	Знает требования по защите компьютерных систем и сетей
	Умеет формировать политики безопасности компьютерных систем и сетей
	Владеет методами проектирования безопасности компьютерных систем и сетей

II. ТРУДОЁМКОСТЬ ДИСЦИПЛИНЫ И ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ ПО ДИСЦИПЛИНЕ

Общая трудоемкость дисциплины составляет 4 зачётных единицы (144 академических часа).

Видами учебных занятий и работы обучающегося по дисциплине могут являться:

Обозначение	Виды учебных занятий и работы обучающегося
Пр	Практические занятия
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 текущего контроля успеваемости и промежуточной аттестации
			Лек	Лаб	Пр	ОК	СР	Контроль	
1	Методологические основы проектной деятельности	3			18		36		УО-1, ПР-7;
2	Основы проектирования и визуальной коммуникации	3			18		36		УО-1, ПР-7, ПР-9;
	Итого:				36		72		Зачет с оценкой

III. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

IV. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА И САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Практические занятия (54 час.)

Практическая работа №1 Введение и история криптографии (6 час)

Актуальность задач, решаемых в криптографии. Классическая схема Шеннона с секретным ключом. История криптографии. Исторические шифры. Шифр Цезаря. Взлом

шифра Цезаря.

Практическая работа №2 Основы криптографии с открытым ключом. (6 час)

Односторонние функции. Задача дискретного логарифмирования. Быстрый алгоритм возведения в степень и его сложность. Задача хранения паролей в компьютере. Система «свой – чужой» в авиации. Задача, возникающая в сетях с удаленным доступом.

Практическая работа №3. Элементы теории чисел(6 час)

Простые числа. Основная теорема арифметики. Разложение числа на простые множители. Функция Эйлера. Теоремы Эйлера и Ферма. Алгоритм Евклида. Обобщенный алгоритм Евклида и решение диофантова уравнения. Нахождение инверсий по заданному модулю.

Практическая работа №4 Системы с открытым ключом(6 час)

Система Диффи-Хеллмана. Шифр Шамира. Шифр Эль-Гамаля. Односторонняя функция с лазейкой и шифр RSA.

Практическая работа №5 Криптографические протоколы(6 час)

Протоколы аутентификации и электронной подписи. Электронные деньги. Подбрасывание монеты по телефону. Ментальный покер. Доказательства с нулевым знанием. Электронные деньги. Голосование через Интернет.

Практическая работа №6 Общие методы взлома систем с открытым ключом (6 час)

«Шаг младенца, шаг великана». Теоретико-числовые алгоритмы. Алгоритм исчисления порядка.

Практическая работа №7 Блоковые шифры(6 час)

Принципы построения блоковых шифров и требования, предъявляемые к ним**.** Режимы функционирования блоковых шифров: ECB, CBC, OFB, CTR. Сеть Фейстеля. Шифры DES, ГОСТ, AES. Криптоанализ блоковых шифров. Сценарии атак на шифры. Основные атаки на блоковые шифры: линейный и дифференциальный криптоанализ. Связь блоковых шифров и генераторов псевдослучайных чисел**.**

Практическая работа №8. Потоковые шифры(6 час)

Принципы построения и современные требования к потоковым шифрам. Криптографически стойкие генераторы псевдослучайных чисел и потоковые шифры. Классификация потоковых шифров. Основные потоковые шифры.

Практическая работа №9. Криптографические хеш-функции(6 час)

Принципы построения и современные требования к хеш-функциям. Применение хешфункций в криптографии. Хеш-функция MD5 и семейство SHA. Хеш-функции, базирующиеся на блоковых шифрах.

V. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

План-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию.

Примерная дата проведения	**Наименование контрольного мероприятия**	**Форма контроля**	**Нормы времени на выполнение**
1-3 недели	Конспектирование литературы	Просмотр и проверка выполнения самостоятельной работы преподавателем	22 час.
4-7 недели	Работа с конспектом, работа с литературой, подготовка к проектной работе	Просмотр и проверка выполнения самостоятельной работы преподавателем, обсуждение результатов выполненной работы на занятии	24 час.
8-17 недели	Подготовка проектов Подготовка к практическим занятиям	Презентация проектов	22 час.
17-18 недели	Подготовка к практическим занятиям	Сообщение	22 час.
Экзаменационная сессия	Подготовка к экзамену	Сдача экзамена	90 час.

Учебно-методическое обеспечение самостоятельной работы студента по дисциплине «Прикладная криптография» предусматривает:

- поиск дополнительной литературы, к которой студенты могут приобщаться при возникновении особой заинтересованности в конкретной теме;

- определение перечня контрольных вопросов, позволяющих студентам самостоятельно проверить качество полученных знаний;
- организацию консультаций преподавателя со студентами для разъяснения вопросов, вызывающих у студентов затруднения при самостоятельном освоении учебного материала.

Дополнительными формами самостоятельной работы являются групповые и индивидуальные задания, выступающие продолжением аудиторных занятий и направленные на овладение практическими навыками по основным разделам дисциплины.

Материалы для организации самостоятельной работы студентов

Самостоятельная работа студентов состоит из подготовки к практическим занятиям, работы над рекомендованной литературой, написания докладов по теме занятия, подготовки презентаций, решения творческих задач, подготовка проектов.

При организации самостоятельной работы преподаватель должен учитывать уровень подготовки каждого студента и предвидеть трудности, которые могут возникнуть при выполнении самостоятельной работы. Преподаватель дает каждому студенту индивидуальные и дифференцированные задания. Некоторые из них могут осуществляться в группе (например, подготовка доклада и презентации по одной теме могут делать несколько студентов с разделением своих обязанностей – один готовит научно-теоретическую часть, а второй проводит анализ практики).

Рекомендации к самостоятельной работе на лекции

Студенту необходимо быть готовым к лекции до прихода лектора в аудиторию, так как именно в первую минуту объявляется тема, формулируется основная цель, дается перечень важнейших вопросов. Без этого дальнейшее понимание лекции затрудняется.

Эффективность познавательной деятельности студента при слушании всецело зависит от направленности его внимания. Внимание обусловлено единством субъективных и объективных причин. В зависимости от действия этих причин оно может быть непроизвольным, т.е. возникает помимо сознательного намерения человека, и произвольным, сознательно регулируемым, направляемым. Работа студента на лекции − сложный процесс, включающий в себя слушание, осмысливание и собственно конспектирование (запись).

Умение студента слышать на лекции преподавателя является лишь первым шагом в процессе осмысленного слушания, который включает в себя несколько этапов, начиная от восприятия речи и кончая оценкой сказанного.

Лекцию необходимо записывать, вести краткие конспекты, где формулировались бы наиболее важные моменты, основные положения,

излагаемые лектором. Обычно запись производится в специальной тетради. При оформлении конспекта лекции необходимо оставлять поля, где студент может записать свои собственные мысли, возникающие параллельно с мыслями, высказанными лектором, а также вопросы, которые могут возникнуть в процессе слушания, чтобы получить на них ответы при самостоятельной проработке материала лекции, при изучении рекомендованной литературы или непосредственно у преподавателя в конце лекции.

Основное отличие конспекта от текста − отсутствие или значительное снижение избыточности, то есть удаление отдельных слов или частей текста, не выражающих значимой информации, а также замена развернутых оборотов текста более лаконичными словосочетаниями (свертывание). При конспектировании основную информацию следует записывать подробно, а дополнительные и вспомогательные сведения, примеры − очень кратко. Умение отделять основную информацию от второстепенной − одно из основных требований к конспектирующему. Хорошие результаты в выработке умения выделять основную информацию дает известный приём, названный условно приемом фильтрации и сжатия текста, который включает в себя две операции:

1. Разбивку текста на части по смыслу.

2. Нахождение в каждой части текста одного слова краткой фразы или обобщающей короткой формулировки, выражающих основу содержания этой части.

Рекомендуется применять систему условных сокращений. В первую очередь сокращаются длинные слова и те, что повторяются в речи лектора чаще всего. При этом само сокращение должно быть по возможности кратким. Основные термины, повторяющиеся наиболее часто, могут быть выделены как ключевые слова и обозначены начальными заглавными буквами этих слов (сокращение, называемое аббревиатурой). Ключевые слова записываются первый раз полностью, после чего в скобках дается их аббревиатура. Процесс записи значительно облегчается при использовании сокращений общепринятых вспомогательных слов. В самостоятельной работе над лекцией целесообразным является использование студентами логических схем. Они в наглядной форме раскрывают содержание и взаимосвязь категорий, законов, понятий, наиболее важных фактов.

Прослушанный материал лекции студент должен проработать. Насколько эффективно он это сделает, зависит и прочность усвоения знаний. Опыт показывает, что только многоразовая, планомерная и целенаправленная обработка лекционного материала обеспечивает его надежное закрепление в долговременной памяти человека.

Повторение нужно разнообразить. При первом повторении изучаются все параграфы и абзацы, при втором, возможно, будет достаточно рассмотреть только отдельные параграфы, а в дальнейшем лишь тему лекции.

Необходимым является подготовка студента к предстоящей лекции. Основным требованием, предъявляемым к такой работе, является, прежде всего, систематичность ее проведения. Она включает ряд важных познавательно-практических этапов: чтение записей, сделанных в процессе слушания и конспектирования предыдущей лекции, вынесение на поля всего, что требуется при дальнейшей работе с конспектом и учебником; техническое оформление записей (подчеркивание, выделение главного, выводов, доказательств); выполнение практических заданий преподавателя; знакомство с материалом предстоящей лекции по учебнику и дополнительной литературе.

Методические рекомендации для написания конспектов

Конспекты, написанные от руки, предоставляются преподавателю для оценки (зачёт/незачёт). Учитывая, что в большинстве случаев тексты первоисточников весьма объёмные, для конспектирования можно выбрать только страницы, разделы или главы (30-50 стр. печатного текста). Объём законспектированного текста в тетради определяется самим студентом.

Методические указания к самостоятельному выполнению проектного задания

Выполнение проектного задания (ТЗ) в рамках дисциплины является обязательным и предполагает индивидуальную или групповую работу.

Этапы работы над творческим заданием:

1. Определение темы проекта. На этом этапе следует определить, будет ли выполняться проект индивидуально или в группе.

2. Формулировка проблемы, постановка цели и задач.

3. Организация деятельности. Если проект выполняется в группе, следует организовать рабочую группу, определить роли каждого участника рабочей группы, спланировать совместную или индивидуальную деятельность по решению задач проекта.

4. Активная и самостоятельная работа над проектом; консультации преподавателя; оформление полученных результатов.

5. Подготовка к защите проекта.

Проект считается выполненным полностью в случае

1. Предоставления полного объема учебных материалов по заранее утвержденной теме, полностью раскрывающих заявленную тему;

2. Предоставления материалов на электронном носителе и в печатном виде;

3. Соответствия представленных материалов требованиям по оформлению;

4. Наличия в материалах проекта описания методики использования ЦОР;

5. Успешной презентации и защиты проекта

Методические рекомендации для подготовки презентаций

Общие требования к презентации:

- презентация не должна быть меньше 10 слайдов;
- первый лист – это титульный лист, на котором обязательно должны быть представлены: название проекта; фамилия, имя, отчество автора;
- следующим слайдом должно быть содержание, где представлены основные этапы (моменты) презентации; желательно, чтобы из содержания по гиперссылке можно перейти на необходимую страницу и вернуться вновь на содержание;
- дизайн-эргономические требования: сочетаемость цветов, ограниченное количество объектов на слайде, цвет текста;
- последними слайдами презентации должны быть глоссарий и список литературы.

Презентация должна отражать тематику реализуемого проекта.

VI. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

Для текущей аттестации при изучении дисциплины «Прикладная криптография» используются следующие оценочные средства:

1) Устный опрос (УО):

Собеседование (консультация с преподавателем) (УО-1)

2) Письменные работы (ПР):

Конспект (ПР-7)

Проект (ПР-9)

№ п/п	Контролируемые разделы / темы дисциплины	Код и наименование индикатора достижения	Результаты обучения	Оценочные средства	
				текущий контроль	промежуточная аттестация
	Раздел 1. Методологические основы проектной деятельности	УК-2.1 Проводит предпроектный и проектный анализ; формулирует цели и задачи исследования; применяет известные методы разработки проектных	знает	УО-1	Вопросы к экзамену 1-7,
			умеет	ПР-7	
			владеет		

		идей			
		УК-2.2 Предлагает способы решения поставленных задач, формулирует ожидаемые результаты, оценивает предложенные альтернативные варианты реализации проекта с точки зрения соответствия целям проекта	знает	УО-1	Вопросы к зачету 25-40
			умеет	ПР-7	
			владеет	ПР-9	
		УК-2.3 Осуществляет координацию и контроль реализации на всех этапах жизненного цикла проекта, корректирует отклонения, вносит дополнительные изменения в план реализации в случае необходимости, определяет зоны ответственности членов команды	знает	УО-1	Вопросы к экзамену 8-10
			умеет	ПР-7	
			владеет		
	Раздел 2. Основы проектирования и визуальной коммуникации	УК-3.1 формирует стратегию командной работы на основе совместного обсуждения целей и направлений деятельности для их реализации	знает	УО-1	Вопросы к экзамену 11-13
			умеет	ПР-7	
			владеет	ПР-9	

		УК-3.2 организует работу команды с учетом объективных условий (технология, внешние факторы, ограничения), индивидуальных особенностей поведения и возможностей членов команды	знает	УО-1	
			умеет	ПР-7	
			владеет	ПР-9	
		УК-3.3 обеспечивает выполнение поставленных задач на основе мониторинга командной работы и своевременного реагирования на существенные отклонения	знает	УО-1	Вопросы к экзамену 13-19
			умеет	ПР-7	
			владеет	ПР-9	

VII. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

(печатные и электронные издания)

1. Райтман М.А. Искусство легального, анонимного и безопасного доступа к ресурсам интернета: учебное пособие. - СПб: БХВ-Петербург, 2016. - 624 с. - Режим доступа: http://znanium.com/catalog/product/944786
2. Смирнова Е.И. Введение в проектную деятельность. Синергетический подход / И.В. Кузнецова [и др.].— Электрон. текстовые данные.— Саратов: Вузовское образование, 2020.— 166 с.— Режим доступа: http://www.iprbookshop.ru/92644.html.
3. Титова Л.Н. Куратор информационных ресурсов / Титова Л.Н., Жилко Е.П., Миниярова Л.В.— Саратов: Вузовское образование, 2017.— 166 с.— Режим доступа: http://www.iprbookshop.ru/71734.html.

4. Томас, Д. Логическое проектирование на SystemVerylog / Д. Томас. — Москва: ДМК Пресс, 2019. — 384 с. Режим доступа: https://e.lanbook.com/book/131680

Дополнительная литература

(печатные и электронные издания)

1. Баринов, В. А. Организационное проектирование/ В.А. Баринов; Институт экономики и финансов "Синергия". - Москва: ИНФРА-М, 2009. - 384 с. Режим доступа: https://znanium.com/catalog/product/196383
2. Елисеенков Г.С. Дизайн-проектирование / Елисеенков Г.С., Мхитарян Г.Ю.— Электрон. текстовые данные. — Кемерово: Кемеровский государственный институт культуры, 2016.— 150 с. Режим доступа: http://www.iprbookshop.ru/66376.html
3. Зайцева К.Н. Дипломное проектирование/ Зайцева К.Н., Рудзит Л.С.— Оренбург: Оренбургский государственный университет, ЭБС АСВ, 2012.— 43 с. Режим доступа: http://www.iprbookshop.ru/21574.html.
4. Эффективное кодирование и цифровое представление изображений [Электронный ресурс]: практикум № 37/ — Электрон. текстовые данные. — Москва: Московский технический университет связи и информатики, 2014.— 19 с.— Режим доступа: http://www.iprbookshop.ru/61581.html

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. «ИТ-образование в Рунете». Образовательные ресурсы Рунета: http://ifets.ieee.org/russian/depository/resourse.htm
2. «Российский общеобразовательный портал»: http://www.school.edu.ru/
3. «Издание литературы в электронном виде»: http://www.magister.msk.ru/library/library.htm
4. Annual Reviiew: http://www.annualreviews.org/ebvc
5. Scopus - мультидисциплинарная реферативная база данных: http://www.scopus.com/
6. Единая коллекция образовательных ресурсов: http://school-collection.edu.ru/catalog/
7. Информационные ресурсы Российской Библиотечной Ассоциации (РБА): http://www.rba.ru/
8. Каталог электронных ресурсов научной библиотеки ДВФУ: http://www.dvfu.ru/web/library/elib
9. Коллекция журналов издательства Elsevier на портале ScienceDirect: http://www.sciencedirect.com/.
10. Научная электронная библиотека (НЭБ): http://www.elibrary.ru/

11. Портал «Гуманитарное образование» http://www.humanities.edu.ru/index.html
12. Российская государственная библиотека (электронный каталог): http://www.rsl.ru/
13. Университетская информационная система Россия (УИС Россия): http://uisrussia.msu.ru
14. Электронная библиотечная система «Айбукс»: http://ibooks.ru/
15. Электронная библиотечная система «Университетская библиотека»: www.biblioclub.ru.
16. Электронная библиотечная система издательства «Лань»: http://e.lanbook.com/
17. Электронная коллекция Оксфордского Российского Фонда: http://www.oxfordrussia.com

Перечень информационных технологий и программного обеспечения

При осуществлении образовательного процесса студентами и профессорско-преподавательским составом используется следующее программное обеспечение: Microsoft Office (Access, Excel, PowerPoint, Word и т. д), Open Office, Skype, программное обеспечение электронного ресурса сайта ДВФУ, включая ЭБС ДВФУ.

VIII.МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Работа с теоретическими материалами. Изучение дисциплины следует начинать с проработки тематического плана лекций, уделяя особое внимание структуре и содержанию темы и основных понятий. Изучение «сложных» тем следует начинать с составления логической схемы основных понятий, категорий, связей между ними. Целесообразно прибегнуть к классификации материала, в частности при изучении тем, в которых присутствует большое количество незнакомых понятий, категорий, теорий, концепций, либо насыщенных информацией типологического характера. Студенты должны составлять конспекты лекций, систематически готовиться к практическим занятиям, вести глоссарий и быть готовы ответить на контрольные вопросы в ходе лекций и аудиторных занятий. Успешное освоение программы курса предполагает прочтение ряда оригинальных работ и выполнение практических заданий.

Подготовка и выполнение практических заданий. По каждой теме дисциплины предлагаются вопросы и практические задания. Перед выполнением заданий изучите теорию вопроса, предполагаемого к исследованию. Самостоятельная работа студентов заключается:

- в подготовке к практическим занятиям в форме консультаций и дискуссий;

- в выполнении индивидуальных и групповых заданий,

- в подготовке к защите курсовой работы,

- в подготовке к итоговому собеседованию.

Цель практических (семинарских) занятий – научить студентов самостоятельно анализировать учебную и научную литературу и вырабатывать у них опыт самостоятельного мышления по проблемам курса, а также выработать навыки практического применения теоретических знаний. Как правило, семинары проводятся в виде практик-консультаций с элементами дискуссии. При этой форме работы отдельным студентам могут поручаться сообщения по тому или иному вопросу, а также ставя дополнительные вопросы, как всей аудитории, так и определенным участникам обсуждения.

Самостоятельная работа студентов, предусмотренная учебным планом, соответствует более глубокому усвоению изучаемого курса, формирует навыки исследовательской работы и ориентирует на умение применять теоретические знания на практике.

Материалом для подготовки могут стать конспекты лекций, профессиональная литература, учебно-методическое обеспечение дисциплины.

Методические рекомендации для написания конспектов

Конспекты, написанные от руки, предоставляются преподавателю для оценки (зачёт/незачёт). Учитывая, что в большинстве случаев тексты первоисточников весьма объёмные, для конспектирования можно выбрать только страницы, разделы или главы (30-50 стр. печатного текста). Объём законспектированного текста в тетради определяется самим студентом.

Методические указания к выполнению проектного задания

Выполнение проектного задания в рамках дисциплины является обязательным и предполагает индивидуальную или групповую работу.

Проект – совокупность мероприятий, направленных на достижение определённой и четко структурированной цели в конкретные сроки с привлечением оптимальных средств и ресурсов.

Проект представляет собой конечный продукт, получаемый в результате планирования и выполнения комплекса учебных и исследовательских заданий. Позволяет оценить умения обучающихся самостоятельно конструировать свои знания в процессе решения практических задач и проблем, ориентироваться в информационном пространстве и уровень сформированности аналитических, исследовательских навыков, навыков

практического и творческого мышления. Может выполняться в индивидуальном порядке или группой обучающихся.

Технология разработки проектов включает в себя следующие этапы:

разработка замысла проекта в соответствии с требованиями программы по следующей структуре:

- аудитория проекта (т.е. характеристика проблем целевой группы и лиц, непосредственно получающих пользу от проекта);
- цели и задачи проекта;
- содержание проекта;
- организация-исполнитель (или форма реализации проекта);
- планируемые результаты и критерии эффективности.

Проект считается выполненным полностью в случае

1. Предоставления полного объема учебных материалов по заранее утвержденной теме, полностью раскрывающих заявленную тему;

2. Предоставления материалов на электронном носителе и в печатном виде;

3. Соответствия представленных материалов требованиям по оформлению;

4. Наличия в материалах проекта описания методики использования ЦОР;

5. Успешной презентации и защиты проекта

Проект считается выполненным полностью в случае

1. Предоставления полного объема учебных материалов по заранее утвержденной теме, полностью раскрывающих заявленную тему;

2. Предоставления материалов на электронном носителе и в печатном виде;

3. Соответствия представленных материалов требованиям по оформлению;

4. Наличия в материалах проекта описания методики использования ЦОР;

5. Успешной презентации и защиты проекта

Задание на проектирование:

1. Разработка концепции и решения IT-проекта.
2. Кураторский проект
3. Проект с акцентом на визуализацию.
4. Проект с акцентом на свободную тему.

IX. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Учебные занятия по дисциплине проводятся в помещениях, оснащенных соответствующим оборудованием и программным обеспечением.

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
Мультимедийная аудитория: G467	Проектор DLP, 3000 ANSI Lm, WXGA 1280x800, 2000:1 EW330U Mitsubishi,; Моноблок HP ProOne 440 G3 23.8" All-in-One, диагональ экрана 23.8", разрешение экрана 1920x1080, Bluetooth, Wi-Fi, операционная система: Windows 10 Enterprise, оптический привод DVD, процессор: Intel Core i5-7500T, размер оперативной памяти: 8 ГБ, видеопроцессор: Intel HD Graphics 630, объем жесткого диска: 1Tb. Беспроводные ЛВС для обучающихся обеспечены системой на базе точек доступа 802.11a/b/g/n 2x2 MIMO(2SS). AfterEffects	Techdesigner, MAX8, VVVV, Adobe Photoshop, Adobe Premier, Adobe
Мультимедийная аудитория: G469	Проектор DLP, 4000 ANSI Lm, 1920x1080, 2000:1 FD630u Mitsubishi; Проектор DLP, 2800 ANSI Lm, 1920x1080, 2000:1 GT1080 Optoma; Проектор DLP, 3000 ANSI Lm, WXGA 1280x800, 2000:1 EW330U Mitsubishi; Беспроводные ЛВС для обучающихся обеспечены системой на базе точек доступа 802.11a/b/g/n 2x2 MIMO(2SS). Специализированное оборудование: Платформа Adruino UNO, Бесконтактный сенсорный Microsoft Kinnect 2.0, Аудио система Dialog 2.0, MIDI контроллер Playtron, Одноплатный компьютер Raspberry PI	Techdesigner, MAX8, VVVV, Adobe Photoshop, Adobe Premier, Adobe

Рабочие места для людей с ограниченными возможностями здоровья оснащены дисплеями и принтерами Брайля; оборудованы: портативными устройствами для чтения плоскопечатных текстов, сканирующими и читающими машинами, видеоувеличителем с возможностью регуляции

цветовых спектров; увеличивающими электронными лупами и ультразвуковыми маркировщиками.

В целях обеспечения специальных условий обучения инвалидов и лиц с ограниченными возможностями здоровья в ДВФУ все здания оборудованы пандусами, лифтами, подъемниками, специализированными местами, оснащенными туалетными комнатами, табличками информационно-навигационной поддержки.

X. ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ

Критерии оценочных средств

Для дисциплины «Прикладная криптография» используются следующие оценочные средства:

1. Устный опрос (УО-1),
2. Конспект (ПР-7),
3. Проект (ПР-9).

	Наименование оценочного средства	**Краткая характеристика оценочного средства**	**Представление оценочного средства в фонде**
УО-1	Устный опрос	Средство контроля усвоения учебного материала темы, раздела или разделов дисциплины, организованное как учебное занятие в виде собеседования преподавателя с обучающимися.	Вопросы по темам/разделам дисциплины
ПР-7	Конспект	Продукт самостоятельной работы обучающегося, отражающий основные идеи заслушанной лекции, сообщения	Литература для конспектирования
ПР-9	Проект	Конечный продукт, получаемый в результате планирования и выполнения комплекса учебных исследовательских заданий. Позволяет оценить умения обучающихся самостоятельно конструировать свои знания в процессе	Задания для проекта

Текущая аттестация студентов

Текущая аттестация студентов по дисциплине «Прикладная криптография» проводится в соответствии с локальными нормативными актами ДВФУ и является обязательной.

Текущая аттестация по дисциплине «Прикладная криптография» проводится в форме контрольных мероприятий (устного опроса, выступления с проектом, тестирования, конспекта первоисточника) по оцениванию фактических результатов обучения студентов и осуществляется

ведущим преподавателем.

Объектами оценивания выступают:

− учебная дисциплина (активность на занятиях, своевременность выполнения различных видов заданий, посещаемость всех видов занятий по аттестуемой дисциплине);

− степень усвоения теоретических знаний;

− уровень овладения практическими умениями и навыками по всем видам учебной работы;

− результаты самостоятельной работы.

Каждому объекту оценивания присваивается конкретный балл. Составляется календарный план контрольных мероприятий по дисциплине и внесения данных в АРС. По окончании семестра студент набирает определенное количество баллов, которые переводятся в пятибалльную систему оценки.

Критерии оценки устного опроса:

Результат работы студента в ходе устного ответа в виде собеседования с преподавателем оценивается по следующим критериям: полнота раскрытия вопросов; степень самостоятельности выполнения задания; и его презентация; исполнение сроков предоставления выполненных заданий; способность отвечать на вопросы преподавателя и студентов в ходе устного опроса по заданной тематике.

✓ 100-86 баллов выставляется, если студент выразил своё мнение по сформулированной проблеме, аргументировал его, точно определив ее содержание и составляющие. Продемонстрировано знание и владение навыком самостоятельной исследовательской работы по теме вопроса. Фактических ошибок, связанных с пониманием проблемы, нет

✓ 85-76 баллов работа студента характеризуется смысловой цельностью, связностью и последовательностью изложения; допущено не более 1 ошибки при объяснении смысла или содержания проблемы. Для аргументации приводятся данные отечественных и зарубежных авторов. Продемонстрированы исследовательские умения и навыки. Фактических ошибок, связанных с пониманием проблемы, нет.

✓ 75-61 баллов проведен достаточно самостоятельный анализ основных этапов и смысловых составляющих проблемы; понимание базовых основ и теоретического обоснования выбранной темы. Привлечены основные источники по рассматриваемой теме. Допущено не более 2 ошибок в смысле или содержании проблемы

✓ 60-50 баллов если работа представляет собой пересказанный или полностью переписанный исходный текст без каких бы то ни было комментариев, анализа. Не раскрыта структура и теоретическая

составляющая темы. Допущено три или более трех ошибок смыслового содержание раскрываемой проблемы.

Критерии оценки конспекта:

- ✓ 100-85 баллов - выставляется студенту, если студент выразил своё мнение по сформулированной проблеме, аргументировал его, точно определив ее содержание и составляющие. Приведены данные отечественной и зарубежной литературы, статистические сведения, информация нормативно-правового характера. Студент знает и владеет навыком самостоятельной исследовательской работы по теме исследования; методами и приемами анализа теоретических и/или практических аспектов изучаемой области. Фактических ошибок, связанных с пониманием проблемы, нет; графически работа оформлена правильно
- ✓ 85-76 баллов - работа характеризуется смысловой цельностью, связностью и последовательностью изложения; допущено не более 1 ошибки при объяснении смысла или содержания проблемы. Для аргументации приводятся данные отечественных и зарубежных авторов. Продемонстрированы исследовательские умения и навыки. Фактических ошибок, связанных с пониманием проблемы, нет. Допущены одна-две ошибки в оформлении работы
- ✓ 75-61 балл – студент проводит достаточно самостоятельный анализ основных этапов и смысловых составляющих проблемы; понимает базовые основы и теоретическое обоснование выбранной темы. Привлечены основные источники по рассматриваемой теме. Допущено не более 2 ошибок в смысле или содержании проблемы, оформлении работы
- ✓ 60-50 баллов – если работа представляет собой пересказанный или полностью переписанный исходный текст без каких бы то ни было комментариев, анализа. Не раскрыта структура и теоретическая составляющая темы. Допущено три или более трех ошибок в смысловом содержании раскрываемой проблемы, в оформлении работы.

Критерии оценки студента по выполнению проекта

Баллы	**Оценка** (стандартная)	**Требования к сформированным компетенциям**
100-86	*«отлично» («зачтено»)*	Оценка **«отлично»** («зачтено») выставляется студенту, если он разработал и реализовал проект в соответствии со всеми требованиями (проблема; цель, задачи и целевая аудитория проекта; методы и средства реализации проекта; анализ проекта и рекомендации). Проект может быть рекомендован для дальнейшего использования.

85-76	*«хорошо» («зачтено»)*	Оценка **«хорошо»** («зачтено») выставляется студенту, если он разработал проект в соответствии с основными требованиями, но допустил некоторые ошибки в его подготовке и реализации (например, неправильно выбрал методы и средства для его реализации; не учёл особенности целевой аудитории и т.п.). Проект нуждается в корректировке.
75-61	*«удовлетворительно» («зачтено»)*	Оценка **«удовлетворительно»** («зачтено») выставляется студенту, если он разработал проект, но проект не соответствует предъявляемым требованиям.
60-50	*«неудовлетворительно» («не зачтено»)*	Оценка **«неудовлетворительно»** («не зачтено») выставляется студенту, если он не разработал проект.

Критерии оценки презентации проекта

Оценка	**50-60 баллов (неудовлетворительно)**	**61-75 баллов (удовлетворительно)**	**76-85 баллов (хорошо)**	**86-100 баллов (отлично)**
Критерии	**Содержание критериев**			
Раскрытие Проблемы	Проблема не раскрыта. Отсутствуют выводы	Проблема раскрыта не полностью. Выводы не сделаны и/или выводы не обоснованы	Проблема раскрыта. Проведен анализ проблемы без привлечения дополнительной литературы. Не все выводы сделаны и/или обоснованы	Проблема раскрыта полностью. Проведен анализ проблемы с привлечением дополнительной литературы. Выводы обоснованы
Представление	Представляемая информация логически не связана. Не использованы профессиональные термины	Представляемая информация не систематизирована и/или не последовательна. Использовано 1-2 профессиональных термина	Представляемая информация не систематизирована и последовательна. Использовано более 2 профессиональных терминов	Представляемая информация систематизирована, последовательна и логически связана. Использовано более 5 профессиональных терминов
Оформление	Не использованы технологии Power Point. Больше 4 ошибок в представляемой информации	Использованы технологии Power Point частично. 3-4 ошибки в представляемой информации	Использованы технологии Power Point. Не более 2 ошибок в представляемой информации	Широко использованы технологии (Power Point и др.). Отсутствуют ошибки в представляемой информации

Ответы на вопросы	Нет ответов на вопросы	Только ответы на элементарные вопросы	Ответы на вопросы полные и/или частично полные	Ответы на вопросы полные, с привидением примеров и/или пояснений

Оценочные средства для промежуточной аттестации

Промежуточная аттестация студентов по дисциплине «Прикладная криптография» проводится в соответствии с локальными нормативными актами ДВФУ и является обязательной.

Согласно учебному плану видом промежуточной аттестации по дисциплине «Прикладная криптография» предусмотрен зачет с оценкой, который выставляется по результатам работы в семестре. зачет с оценкой проводится в устной форме по билетам.

Оценочные средства для промежуточной аттестации

Вопросы к зачету с оценкой

Описать алгоритм шифра Цезаря.

2. Как провести криптоанализ шифра Цезаря?

3. Что такое односторонняя функция?

4. Что такое дискретное логарифмирование?

5. Описать алгоритм быстрого возведения в степень. Оценить его сложность.

6. Как решаются проблема хранения паролей и проблема ПВО с помощью
односторонней функции?

7. Чем отличается криптосистема с открытым ключом от криптосистемы с секретным
ключом?

8. Описать первую криптосистему с открытым ключом? Какие проблемы она
позволяет решать?

9. Описать алгоритм Евклида и обобщенный алгоритм Евклида.

10. Дать определение инверсии. Как вычислять инверсию, используя алгоритм
Евклида?

11. Дать определение функции Эйлера и привести пример ее вычисления.

12. Описать алгоритм «Решето Эратосфена».

13. Описать методы дискретного логарифмирования. Оценить их сложность.

14. Как построить цифровую подпись на басе шифра RSA?
15. Как построить цифровую подпись на басе шифра Эль-Гамаля?

Критерии выставления оценки студенту на зачете по дисциплине «Прикладная криптография»:

Баллы (рейтинговой оценки)	**Оценка экзамена** (стандартная)	**Требования к сформированным компетенциям**
100-85	*«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, обозначает особенности применения тех или иных методов работы в зависимости от ситуаций, свободно справляется с задачами, вопросами и другими видами применения знаний, владеет разносторонними навыками и приемами выполнения практических задач, способен использовать современные технические средства для оптимизации, унификации и модернизации работы.
85-76	*«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. Использует основной терминологический, -правовые акты, влияющие на способы и методы работы.
75-61	*«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, не владеет способами и методами работы не применяет их.