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
_____ Степанова А.А.
(подпись) (ФИО)

УТВЕРЖДАЮ
И.о. директора департамента
_____ Заболотский В.С.
(подпись) (ФИО)
«13» сентября 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Криптографические методы защиты информации

Направление подготовки: 01.04.01 Математика
Программа магистратуры «Алгебра»
Форма подготовки: очная

курс 2 семестр 3
лекции не предусмотрены
лабораторные занятия 50 час.
самостоятельная работа студентов 58 час.
контрольные работы не предусмотрены
всего часов аудиторной нагрузки 50 час.
зачет не предусмотрен
экзамен 3 семестр

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования, утвержденного приказом Министерства образования и науки РФ от 10 января 2018 г. № 12 (с изменениями и дополнениями)

Рабочая программа обсуждена на заседании департамента математики, протокол № 1 от 13 сентября 2021 г.

И.о. директора департамента математики Заболотский В.С.
Составитель: к.ф.-м.н, доцент С.Г. Чеканов

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)

Цели и задачи освоения дисциплины:

Цель: преподавания дисциплины «Криптографические методы защиты информации» является развитие логического и алгоритмического мышления.

Задачи преподавания дисциплины:

1. привить навыки математического исследования социальных, технических, экономических и других проблем науки и производства
2. умение мыслить научными категориями в области науки, техники, экономики и социальной сферы
3. умение математически корректно ставить естественнонаучные задачи

Для успешного изучения дисциплины «Криптографические методы защиты информации» у обучающихся должны быть сформированы следующие предварительные компетенции

- способность видеть методологические аспекты построения математических теорий;
- применять системный подход в формализации математических задач;
- способностью к абстрактному мышлению, анализу, синтезу.

Профессиональные компетенции выпускников и индикаторы их достижения:

Тип задач	Код и наименование профессиональной компетенции (результат освоения)	Код и наименование индикатора достижения компетенции
проектно-технологический	ПК-6 Способен разрабатывать концептуальные и теоретические модели решаемых задач проектной и производственно-технологической деятельности	ПК-6.1 Обосновывает необходимость работы над конкретным проектом, проводит анализ и дает оценку его эффективности, осуществляет защиту предлагаемого проекта, показывает его востребованность на выбранном рынке
		ПК-6.2 Применяет методы построения, анализа и применения математических моделей для оценки состояния, и прогноза развития экономических процессов и явлений в работе над проектом по выбранной тематике
организационно-управленческий	ПК-7 Способен к применению методов математического и алгоритмического моделирования для организации управленческой деятельности	ПК-7.1 Проводит анализ необходимых для реализации проекта ресурсов, оценивает временные затраты на реализацию проекта, собирает и обрабатывает информацию для принятия управленческих решений
		ПК-7.2 Применяет на практике математические методы анализа

Тип задач	Код и наименование профессиональной компетенции (результат освоения)	Код и наименование индикатора достижения компетенции
		данных в профессиональной сфере, технологии организации и распределения обязанностей в команде, реализующей проект

Код и наименование индикатора достижения компетенции	Наименование показателя оценивания (результата обучения по дисциплине)
ПК-6.1 Обосновывает необходимость работы над конкретным проектом, проводит анализ и дает оценку его эффективности, осуществляет защиту предлагаемого проекта, показывает его востребованность на выбранном рынке	Знает основные подходы к организации предметной среды математики
	Умеет обосновывать и защищать предлагаемый проект, доказывать его эффективность и востребованность на выбранном рынке
	Владеет опытом выражения своих мыслей и мнения, навыками оценки эффективности проекта
ПК-6.2 Применяет методы построения, анализа и применения математических моделей для оценки состояния, и прогноза развития экономических процессов и явлений в работе над проектом по выбранной тематике	Знает методы построения, анализа и применения математических моделей
	Умеет выбирать методы построения, анализа и применения математических моделей при решении задач проектно-технологической деятельности
	Владеет навыками работы над проектами по выбранной тематике; методами построения, анализа и применения математических моделей для оценки состояния и прогноза развития экономических процессов и явлений
ПК-7.1 Проводит анализ необходимых для реализации проекта ресурсов, оценивает временные затраты на реализацию проекта, собирает и обрабатывает информацию для принятия управленческих решений	Знает методы построения математической модели, необходимые для реализации проекта
	Умеет оценить временные затраты на реализацию проекта, определять ресурсы, находить профессиональную информацию
	Владеет навыками обработки информации для принятия управленческих решений
ПК-7.2 Применяет на практике математические методы анализа данных в профессиональной сфере, технологии организации и распределения обязанностей в команде, реализующей проект	Знает математические методы анализа данных о проекте;
	Умеет производить первичную обработку результатов посредством математических методов анализа данных, обеспечивать координацию деятельности членов команды;
	Владеет технологиями организации и распределения обязанностей в команде, реализующей проект

Трудоёмкость дисциплины и видов учебных занятий по дисциплине

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

(1 зачетная единица соответствует 36 академическим часам)

Видами учебных занятий и работы обучающегося по дисциплине являются:

Обозначение	Виды учебных занятий и работы обучающегося
ЛР	Лабораторные работы
СР	Самостоятельная работа обучающегося в период теоретического обучения
Контроль	Самостоятельная работа обучающегося и контактная работа обучающегося с преподавателем в период промежуточной аттестации

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Лекции не предусмотрены учебным планом

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА И САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Лабораторные работы (50 час.)

Лабораторная работа 1. Введение (6 часа).

Рассматриваются примеры шифров на основе группы подстановок конечного множества. Проводятся атаки на основе шифртекстов.

Лабораторная работа 2. Шифры простой замены (6 часа).

Изучаются шифры, построенные на основе конечных колец и групп. Шифруются открытые тексты и проводятся атаки на построенные шифры.

Лабораторная работа 3. Многоалфавитные шифры простой замены (6 часа).

Вычисляются статистические характеристики шифртекстов, полученных с помощью шифра Виженера. Выполняется анализ шифра по индивидуальному заданию.

Лабораторная работа 4. Совершенные шифры (6 часа).

Изучаются шифры совершенные по Шеннону. Строятся примеры шифров , которые проверяются на соответствие быть совершенными.

Лабораторная работа 5. Поточные шифры (5 часа).

Изучаются генераторы ключевых последовательностей для поточных шифров. Создаются собственные генераторы ключевых последовательностей для поточных шифров.

Лабораторная работа 6. Блочные шифры (6 часа).

Строятся блочные шифры. Изучаются стандарты шифрования DES, AES.

Лабораторная работа 7. Шифры с открытым ключом (5 часа).

Задача факторизации целых чисел. Логарифмирование в конечных абелевых группах. Схема шифрования RSA и Эль Гамаля. Изучаются возможные атаки на указанные шифры.

Лабораторная работа 8. Эллиптические кривые над конечными полями (5 часа).

Вычисляются группы точек эллиптических кривых для фиксированных конечных полей. Строятся алгоритмы кодировки текстов точками эллиптических кривых.

Лабораторная работа 9. Хеш функции (5 часа).

Строятся примеры хеш функций и оценивается их стойкость. Изучаются возможность построения криптографических протоколов на основе, построенных хеш функций.

Примеры индивидуальных заданий

1. **Введение**

1. В чем разница между протоколом и алгоритмом?
2. Пусть функция f отображает пространство 200-битовых целых чисел в пространство 100-битовых целых чисел по следующему правилу.

$f(x)$ =(старшие 100 бит числа x) $\oplus$ (младшие 100 бит числа x)

Обладает ли функция $f(x)$ свойствами функции хеширования?

3. Можно ли утверждать, что еще не взломанный криптографический алгоритм более стоек, чем взломанный?
4. Сложные системы подвержены ошибкам. Назовите еще одну причину, по которой сложные системы безопасности более уязвимы.

1. **Шифры простой замены**

1. Почему алгоритм шифрования не должен содержать секретных компонентов?
2. Постройте пример подстановочного шифра в алфавите русского языка и оцените его стойкость.
3. Является ли аффинный шифр более стойким, чем подстановочный шифр?
4. Укажите назначение перестановочного шифра в алгоритме DES.

2. **Многоалфавитные шифры простой замены**

1. Постройте пример многоалфавитного шифра простой замены.
2. Является ли шифр Вернама подстановочным?
3. Почему многоалфавитные шифры простой замены не являются совершенными?

4. Может ли шифр Виженера быть совершенным?

3. **Совершенные шифры**

1. Постройте алгорим вычисления энтропии естественного языка.
2. Постройте пример совершенного шифра с конечным числом открытых и шифртекстов.
3. Может ли подстановочный шифр быть совершенным?
4. Почему многие реальные шифры не являются совершенными?

4. **Поточные шифры**

1. Построить расширение поля F_3 с помощью полинома $x^2 + 2x + 1$.
2. Построить генератор линейной рекуррентной последовательности над простым конечным полем.
3. Разработать код над полем F_5.
4. На основе разработанного кода и генератора построить и реализовать на компьютере поточный шифр.

5. **Блочные шифры**

1 Сравнить криптографические характеристики поточных и блочных шифров.
2 Охарактеризовать алгоритм Фейстеля с криптографической точки зрения.
3 Оценить стойкость блочного шифра DES относительно атаки перебором ключей.
4 Построить аффинный блочный шифр размерности 5 над простым полем из пяти элементов.

6. **Шифры с открытым ключом**

1. Провести сравнительный анализ симметричных шифров и шифров с открытым ключом.
2. Привести пример алгоритма для решения проблемы факторизации целого числа.
3. Написать программу для вычислений с большими целыми числами.
4. Реализовать на компьютере алгоритм RSA.

7. **Хеш функции**

1. Почему практически невозможно инвертировать функцию хеширования?
2. Как можно имитировать случайный оракул в реальных приложениях?
3. Допустим, что пространство значений функции хеширования имеет размер 2^{160}. Какое время потребуется для обнаружения коллизии?
4. Построить пример функции хеширования.

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Криптографические методы защиты информации» включает в себя:

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

характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;

требования к представлению и оформлению результатов самостоятельной работы;

критерии оценки выполнения самостоятельной работы.

План-график выполнения самостоятельной работы по дисциплине

№ п/п	Дата/сроки выполнения	Вид самостоятельной работы	Примерные нормы времени на выполнение
1. Введение	20.09 - 27.09	индивидуальное домашнее задание	1 неделя
2. Шифры простой замены	28.09 - 5.10	индивидуальное домашнее задание	1 неделя
3. Многоалфавитные шифры простой замены	6.10 - 13.10	индивидуальное домашнее задание	1 неделя
4. Совершенные шифры	14.10 - 21.10	индивидуальное домашнее задание	1 неделя
5. Поточные шифры	22.10 - 29.10	индивидуальное домашнее задание	1 неделя
6. Блочные шифры	30.10 - 8.11	индивидуальное домашнее задание	1 неделя
7. Шифры с открытым ключем	8.11 -28.11	индивидуальное домашнее задание	1 неделя
8. Хеш функции	28.11 - 18.12	индивидуальное домашнее задание	1 неделя

Рекомендации по самостоятельной работе студентов

Планирование и организация времени, отведенного на выполнение заданий самостоятельной работы.

Изучив график выполнения самостоятельных работ, следует правильно её организовать. Рекомендуется изучить структуру каждого задания, обратить внимание на график выполнения работ, отчетность по каждому заданию предоставляется в последнюю неделю согласно графику. Обратить внимание, что итоги самостоятельной работы влияют на окончательную оценку по итогам
освоения учебной дисциплины.

Работа с литературой.

При выполнении ряда заданий требуется работать с литературой. Рекомендуется использовать различные возможности работы с литературой: фонды научной библиотеки ДВФУ (http://www.dvfu.ru/library/) и других ведущих вузов страны, а также доступных для использования научно-библиотечных систем.

В процессе выполнения самостоятельной работы, в том числе при написании эссе рекомендуется работать со следующими видами изданий:

а) Научные издания, предназначенные для научной работы и содержащие теоретические, экспериментальные сведения об исследованиях. Они могут публиковаться в форме: монографий, научных статей в журналах или в научных сборниках;

б) Учебная литература подразделяется на:

- учебные издания (учебники, учебные пособия, тексты лекций), в которых содержится наиболее полное системное изложение дисциплины или какого-то ее раздела;

- справочники, словари и энциклопедии – издания, содержащие краткие сведения научного или прикладного характера, не предназначенные для сплошного чтения. Их цель – возможность быстрого получения самых общих представлений о предмете.

Существуют два метода работы над источниками:

– сплошное чтение обязательно при изучении учебника, глав монографии или статьи, то есть того, что имеет учебное значение. Как правило, здесь требуется повторное чтение, для того чтобы понять написанное. Старайтесь при сплошном чтении не пропускать комментарии, сноски, справочные материалы, так как они предназначены для пояснений и помощи. Анализируйте рисунки (карты, диаграммы, графики), старайтесь понять, какие тенденции и закономерности они отражают;

– метод выборочного чтения дополняет сплошное чтение; он применяется для поисков дополнительных, уточняющих необходимых сведений в словарях, энциклопедиях, иных справочных изданиях. Этот метод крайне важен для повторения изученного и его закрепления, особенно при

подготовке к экзамену.

Для того чтобы каждый метод принес наибольший эффект, необходимо фиксировать все важные моменты, связанные с интересующей Вас темой.

Тезисы – это основные положения научного труда, статьи или другого произведения, а возможно, и устного выступления; они несут в себе больший объем информации, нежели план. Простые тезисы лаконичны по форме; сложные – помимо главной авторской мысли содержат краткое ее обоснование и доказательства, придающие тезисам более весомый и убедительный характер. Тезисы прочитанного позволяют глубже раскрыть его содержание; обучаясь излагать суть прочитанного в тезисной форме, вы сумеете выделять из множества мыслей авторов самые главные и ценные и делать обобщения.

Конспект – это способ самостоятельно изложить содержание книги или статьи в логической последовательности. Конспектируя какой-либо источник, надо стремиться к тому, чтобы немногими словами сказать о многом. В тексте конспекта желательно поместить не только выводы или положения, но и их аргументированные доказательства (факты, цифры, цитаты).

Писать конспект можно и по мере изучения произведения, например, если прорабатывается монография или несколько журнальных статей.

Составляя тезисы или конспект, всегда делайте ссылки на страницы, с которых вы взяли конспектируемое положение или факт, – это поможет вам сократить время на поиск нужного места в книге, если возникает потребность глубже разобраться с излагаемым вопросом или что-то уточнить при написании письменных работ.

IV. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

№ п/п	Контролируемые разделы / темы дисциплины	Код индикатора достижения компетенции	Результаты обучения	Оценочные средства	
				текущий контроль	промежуточная аттестация
1	Введение Шифры простой замены	ПК-6.1 Обосновывает необходимость работы над конкретным проектом, проводит анализ и дает оценку его эффективности, осуществляет защиту	Знает основные подходы к организации предметной среды математики;	Коллоквиум (УО-2)	Вопросы к экзамену 1-5
			Умеет обосновывать и защищать предлагаемый проект, доказывать его эффективность и востребованность на выбранном рынке;	Коллоквиум (УО-2)	
			Владеет опытом выражения своих мыслей и мнения, навыками оценки	Индивидуальное домашне	

		предлагаемого проекта, показывает его востребованность на выбранном рынке	эффективности проекта	е задание (ПР-6)	
2	Многоалфавитные шифры замены Совершенные шифры	ПК-6.2 Применяет методы построения, анализа и применения математических моделей для оценки состояния, и прогноза развития экономических процессов и явлений в работе над проектом по выбранной тематике	Знает методы построения, анализа и применения математических моделей;	Индивидуальное домашнее задание (ПР-6)	Вопросы к экзамену 6-9
			Умеет выбирать методы построения, анализа и применения математических моделей при решении задач проектно-технологической деятельности;	Коллоквиум (УО-2)	
			Владеет навыками работы над проектами по выбранной тематике; методами построения, анализа и применения математических моделей для оценки состояния и прогноза развития экономических процессов и явлений	Коллоквиум (УО-2)	
3	Поточные шифры Блочные шифры	ПК-7.1 Проводит анализ необходимых для реализации проекта ресурсов, оценивает временные затраты на реализацию проекта, собирает и обрабатывает информацию для принятия управленческих решений	Знает методы построения математической модели, необходимые для реализации проекта;		Вопросы к экзамену 10-14
			Умеет проводить анализ и обосновывать необходимость работы над данным проектом и оценивать его эффективность	Индивидуальное домашнее задание (ПР-6)	
			Умеет оценить временные затраты на реализацию проекта, определять ресурсы, находить профессиональную информацию; Владеет навыками обработки информации для принятия управленческих решений	Коллоквиум (УО-2)	
4	Шифры с открытым ключом Эллиптические кривые над конечными полями	ПК-7.2 Применяет на практике математические методы анализа данных в профессиональной сфере,	Знает принципы и подходы к организации предметной среды математики; научно-исследовательский и научно-образовательный потенциал конкретного региона, где осуществляется	Индивидуальное домашнее задание (ПР-6)	Вопросы к экзамену 15-21

	Хеш функции	технологии организации и распределения обязанностей в команде, реализующей проект	образовательная деятельность		
			Умеет обосновывать и защищать предлагаемый проект, доказывать его эффективность и востребованность на выбранном рынке	Коллоквиум (УО-2)	
			Владеет опытом выражения своих мыслей и мнения	Индивидуальное домашнее задание (ПР-6)	

Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков и (или) опыта деятельности, а также качественные критерии оценивания, которые описывают уровень сформированности компетенций, представлены в разделе VIII.

V. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) основная литература:

1. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации. Изд-во Горячая линия-Телеком, 2017 https://e.lanbook.com/book/111097
2. Криптографические методы защиты информации: лабораторный практикум. Изд-во Северо-Кавказского федерального университета, 2015 https://e.lanbook.com/book/155280
3. Мартынов Л.М. Алгебра для криптографии. Часть 1: учебное пособие**,** Изд-во Омского государственного университета путей сообщения, 2015 https://e.lanbook.com/book/129189
4. Мартынов Л.М. Алгебра для криптографии. Часть 2: учебное пособие**,** Изд-во Омского государственного университета путей сообщения, 2015 https://e.lanbook.com/book/129188
5. Мартынов Л.М. Алгебра для криптографии. Часть 3: учебное пособие**,** Изд-во Омского государственного университета путей сообщения, 2015 https://e.lanbook.com/book/129190

б) дополнительная литература:

1. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии, М.: МЦНМО, 2003 г. http://lib.dvfu.ru:8080/lib/item?id=chamo:5790&theme=FEFU
2. Коблиц Н. Курс теории чисел и криптографии, М.: ТВМ, 2001 г. http://lib.dvfu.ru:8080/lib/item?id=chamo:16477&theme=FEFU

3. Д. К. Фаддеев, И. С. Соминский. Задачи по высшей алгебре. – Санкт-Петербург, «Лань», 1998, - 288 с. http://lib.dvfu.ru:8080/lib/item?id=Lan:Lan-399&theme=FEFU
4. Виноградов И.М. Основы теории чисел. – СПб.: Лань, 2009. – 176 с. http://lib.dvfu.ru:8080/lib/item?id=Lan:Lan-46&theme=FEFU
5. Кострикин А.И. и др. Сборник задач по алгебре. – СПб.: Лань, 2011. – 450 с. http://lib.dvfu.ru:8080/lib/item?id=chamo:103102&theme=FEFU

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. http://e.lanbook.com/books/element.php?pl1_id=62755 Серёдкин А.Н., Роганов В.Р., Филиппенко В.О. Основы защиты информации и информационные технологии: Учебное пособие в 3 частях. – Кн. 2: Криптография, криптоанализ и методы защиты информации в ИС и ИТ: Изд-во ПензГТУ.-2013

Профессиональные базы данных и информационные справочные системы

1. База данных Scopus http://www.scopus.com/home.url
2. База данных Web of Science http://apps.webofknowledge.com/
3. Общероссийский математический портал Math-Net.Ru http://www.mathnet.ru
4. Электронная библиотека диссертаций Российской государственной библиотеки http://diss.rsl.ru/
5. Электронная библиотека Европейского математического общества https://www.emis.de/
6. Электронные базы данных EBSCO http://search.ebscohost.com/

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 (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: лабораторные занятия, задания для самостоятельной работы.

Лабораторные 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 и 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 экзамена, 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 экзамену. К сдаче экзамена допускаются обучающиеся, выполнившие все задания (практические, 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
690922, Приморский край, г. Владивосток, остров Русский, полуостров Саперный, поселок	Помещение укомплектовано специализированной учебной мебелью (посадочных мест –	

Аякс, 10, корпус D, ауд. D732. Учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	45) Оборудование: ЖК-панель 47", Full HD, LG M4716 CCBA – 1 шт. Доска аудиторная.	
690922, Приморский край, г.Владивосток, остров Русский, полуостров Саперный, поселок Аякс, 10, корп. А (Лит. П), Этаж 10, каб.А1017. Аудитория для самостоятельной работы	Оборудование: Моноблок Lenovo C360G-i34164G500UDK – 15 шт. Интегрированный сенсорный дисплей Polymedia FlipBox - 1 шт. Копир-принтер-цветной сканер в e-mail с 4 лотками Xerox WorkCentre 5330 (WC5330C – 1 шт.)	

Для проведения учебных занятий по дисциплине, а также для организации самостоятельной работы студентам доступно следующее лабораторное оборудование и специализированные кабинеты, соответствующие действующим санитарным и противопожарным нормам, а также требованиям техники безопасности при проведении учебных и научно-производственных работ.

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.

VIII ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ

Для дисциплины «Криптографические методы защиты информации» используются следующие оценочные средства:

Устный опрос:

1. Коллоквиум (УО-2)

Письменные работы:

1. Индивидуальное домашнее задание (ПР-6)

Устный опрос

Устный опрос позволяет оценить знания и кругозор студента, умение

логически построить ответ, владение монологической речью и иные коммуникативные навыки.

Обучающая функция состоит в выявлении деталей, которые по каким-то причинам оказались недостаточно осмысленными в ходе учебных занятий и при подготовке к зачёту.

Коллоквиум (УО-2) – 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.

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.

Индивидуальное домашнее задание (ПР-6) – средство для закрепления и практического освоения материала по определенному разделу.

Методические рекомендации, определяющие процедуры оценивания результатов освоения дисциплины

Оценочные средства для промежуточной аттестации

Промежуточная аттестация студентов по дисциплине «Криптографические методы защиты информации» проводится в соответствии с локальными нормативными актами ДВФУ и является обязательной. Форма отчётности по дисциплине – экзамен (3-й, осенний семестр). Экзамен по дисциплине включает ответы на 3 вопроса. Два вопроса носят теоретический характер, один вопрос носит практический характер.

Методические указания по сдаче экзамена

Экзамен 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 экзамен в отсутствие ведущего преподавателя.

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

Во время проведения экзамена студенты могут пользоваться рабочей программой дисциплины, а также с разрешения преподавателя, проводящего экзамен, 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), не допускается. Инвалиды и лица с ограниченными возможностями здоровья, не имеющие возможности самостоятельного передвижения, допускаются на экзамен с сопровождающими.

При промежуточной аттестации обучающимся устанавливается оценка «отлично», или «хорошо», или «удовлетворительно», или «неудовлетворительно».

В зачетную книжку студента вносится только запись «отлично», или «хорошо», или «удовлетворительно», запись «неудовлетворительно» вносится только в экзаменационную ведомость. При неявке студента на экзамен в ведомости делается запись «не явился».

Вопросы к экзамену в третьем семестре:

1. Шифр простой замены. Примеры.
2. Статистический метод криптоанализа шифра простой замены.
3. Омофоны и усиление шифров простой замены.
4. Многоалфавитные шифры простой замены.
5. Энтропия языка и способы ее вычисления.
6. Условная энтропия и теоретическая стойкость шифра.
7. Шифр Виженера и его криптоанализ.
8. Шифры не распространяющие ошибок.
9. Шифры гаммирования. Характеристики гаммы.
10. Шифр Вернама.
11. Линейные рекуррентные последовательности над конечными полями.
12. Генераторы слчайных последовательностей.
13. Генератор A5.
14. Блочные шифры.
15. Стандарт DES.
16. Асимметричные шифры.
17. Алгоритм RSA.

18.Шифр Эль Гамаля.
19.Сравнительный анализ симметричных и асимметричных шифров.
20.Хеш функции и их криптографические приложения.
21.Шифрсистемы на основе эллиптических кривых.

Критерии выставления оценки студенту на экзамене

К экзамену допускаются обучающиеся, выполнившие программу обучения по дисциплине, прошедшие все этапы текущей аттестации.

Оценка	Требования к сформированным компетенциям
«отлично»	Студент показывает глубокое и систематическое знание всего программного материала и структуры конкретного вопроса, а также основного содержания и новаций лекционного курса по сравнению с учебной литературой. Студент демонстрирует отчетливое и свободное владение концептуально-понятийным аппаратом, научным языком и терминологией соответствующей научной области. Знание основной литературы и знакомство с дополнительно рекомендованной литературой. Логически корректное и убедительное изложение ответа.
«хорошо»	Знание узловых проблем программы и основного содержания лекционного курса; умение пользоваться концептуально понятийным аппаратом в процессе анализа основных проблем в рамках данной темы; знание важнейших работ из списка рекомендованной литературы. В целом логически корректное, но не всегда точное и аргументированное изложение ответа.
«удовлетворительно»	Фрагментарные, поверхностные знания важнейших разделов программы и содержания лекционного курса; затруднения с использованием научно-понятийного аппарата и терминологии учебной дисциплины; неполное знакомство с рекомендованной литературой; частичные затруднения с выполнением предусмотренных программой заданий; стремление логически определенно и последовательно изложить ответ.
«неудовлетворительно»	Незнание, либо отрывочное представление о данной проблеме в рамках учебно-программного материала; неумение использовать понятийный аппарат; отсутствие логической связи в ответе.

Оценочные средства для текущей аттестации

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

Текущая аттестация проводится в форме контрольных мероприятий (коллоквиума, индивидуального домашнего задания) 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.

Составляется календарный план контрольных мероприятий по дисциплине. Оценка посещаемости, активности обучающихся на занятиях, своевременность выполнения различных видов заданий ведётся на основе журнала, который ведёт преподаватель в течение учебного семестра.