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**
Алгебраические основы криптографии

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

курс 1 семестр 2
лекции 18 час.
практические занятия 18 час.
самостоятельная работа студентов 72
контрольные работы не предусмотрены
всего часов аудиторной нагрузки 36 час.
в том числе с использованием МАО 27 час.
зачет 2 семестр
экзамен не предусмотрен

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** - развитие логического и алгоритмического мышления.

**Задачи** преподавания дисциплины:

1. 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 строго доказывать утверждение, сформулировать результат, увидеть следствия полученного результата;
4. применение полученных знаний при изучении явлений природы и общества и исследование простейших моделей с помощью методов теории групп, колец и полей.

Для успешного изучения дисциплины «Алгебраические основы криптографии» 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<br><br>(результат освоения) | Код и наименование индикатора достижения компетенции |
|---|---|---|
| проектно-технологический | ПК-5 Способен разрабатывать и применять математические методы для решения задач научной и проектно-технологической деятельности | ПК-5.1 Выбирает оптимальные системы программирования, наиболее подходящие для решения поставленной задачи |
| | | ПК-5.2 Применяет на практике методы моделирования информационных процессов, осуществляет работы над производственным проектом в составе группы научных специалистов |
| проектно-технологический | ПК-6 Способен разрабатывать концептуальные и теоретические модели решаемых задач проектной и производственно-технологической | 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 |

| Тип задач | Код и наименование профессиональной компетенции<br><br>(результат освоения) | Код и наименование индикатора достижения компетенции |
|---|---|---|
| | деятельности | построения, анализа и применения математических моделей для оценки состояния, и прогноза развития экономических процессов и явлений в работе над проектом по выбранной тематике |

| Код и наименование индикатора достижения компетенции | Наименование показателя оценивания (результата обучения по дисциплине) |
|---|---|
| ПК-5.1 Выбирает оптимальные системы программирования, наиболее подходящие для решения поставленной задачи | Знает современные методы цифровой обработки изображений |
| | Умеет анализировать поставленную задачу и находить алгоритм ее решения |
| | Знает современные методы цифровой обработки изображений;<br>Владеет навыками отбора оптимальных систем программирования, наиболее подходящих для решения поставленной задачи |
| ПК-5.2 Применяет на практике методы моделирования информационных процессов, осуществляет работы над производственным проектом в составе группы научных специалистов | Знает средства компьютерной графики |
| | Умеет применять методы моделирования информационных процессов |
| | Владеет навыками работы над производственным проектом в составе группы научных специалистов |
| 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 |

Трудоёмкость дисциплины и видов учебных занятий по дисциплине

Общая трудоемкость дисциплины составляет 3 зачётные единицы (108 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 |
|---|---|
| Лек | Лекции |
| Пр | Практические 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

**(18 час.)**

**Тема 1. Конечные группы. Представление групп подстановками (4 час.)**

Группы. Индекс подгруппы. Теорема Лагранжа. Подстановки и их криптографические свойства. Теорема Кели.

Занятие проводится с использованием метода активного обучения «лекция-беседа».

**Тема 2. Кольца и поля (4 час.)**

Идеалы колец и факторкольца. Характеристика кольца. Конечные расширения полей. Теоремы о строении конечных полей

Занятие проводится с использованием метода активного обучения «лекция-беседа».

**Тема 3. Линейные рекуррентные последовательности над конечными полями (4 час.)**

Характеризация последовательностей с помощью матриц и полиномов. Оценка периода ЛРП. Применение последовательностей в криптографических целях

Занятие проводится с использованием метода активного обучения «лекция-беседа».

**Тема 4. Полугруппы и конечные автоматы (2 час.)**

Определение автомата и представление с помощью графа и полугруппы

Занятие проводится с использованием метода активного обучения «лекция-беседа».

**Тема 5. Решетки и решеточно продолженные булевы функции (4 час.)**

Булевы функции и булевы решетки. Продолжение булевых функций с единичного куба на множество рациональных точек

Занятие проводится с использованием метода активного обучения «лекция-беседа».

## I. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА И САМОСТОЯТЕЛЬНОЙ РАБОТЫ

### Практические занятия (18 час.)

### Занятие 1. Конечные группы (3 часа).

Группы. Индекс подгруппы. Теорема Лагранжа. Подстановки и их криптографические свойства. Теорема Кели.

### Занятие 2. Кольца и поля (3 часа).

Идеалы колец и факторкольца. Характеристика кольца. Конечные поля и их алгебраические расширения. Теорема о строении конечных полей. Вычисления в конечных полях.

Занятие проводится с использованием метода активного обучения «групповая консультация».

### Занятие 3. Линейные рекуррентные последовательности над конечными полями (3 часа).

Рекуррентные соотношения. Характеризация последовательностей с помощью матриц и полиномов. Вычисление периода последовательности. Криптографические приложения последовательностей.

### Занятие 4. Полугруппы и конечные автоматы (3 часа).

Полугруппы и их представления. Конечные автоматы и их связь с полугруппами. Представление автомата графом. Криптографические приложения автоматов.

Занятие проводится с использованием метода активного обучения «групповая консультация».

### Занятие 5. Решетки и решеточные продолжения булевых функций (3 часа).

Определение решетки. Дистрибутивные решетки. Булевы функции и решетки. Криптоанализ блочных шифров и дистрибутивные решетки.

### Занятие 6. Эллиптические кривые (3 часа).

Эллиптические кривые над конечными полями. Группа точек эллиптической кривой. Вычисление порядка группы эллиптической кривой и порядка элементов группы. Криптографические приложения эллиптических кривых.

Занятие проводится с использованием метода активного обучения «групповая консультация».

## Примеры контрольных работ
## Тема: Группы и поля

Вариант 1

1. Вычислить порядок группы порожденной подстановками:

(123), (24), (15)

2. Построить расширение поля $F_3$ присоединением корня полинома

$x^2+3x+1$

3. Доказать, что кольце $F_3[x]$ все идеалы главные

## Тема: Многочлены

1 вариант

1. Разложите многочлен $8x^4+8x^3-27x-27$ на множители.
2. Найдите наибольший общий делитель двух многочленов и его линейное представление:
   $x^5+3x^4+x^3-5x^2-6x-2$ и $x^5+2x^4-3x^2-4x-2$.
3. Отделите кратные множители:
   $x^7+6x^6-5x^5-80x^4-185x^3-194x^2-99x-20$.
4. Решите уравнение 3 степени: $x^3+3x^2-3x+4=0$.
5. Решите уравнение 4 степени: $x^4-2x^3+2x^2+4x-8=0$.
6. Для многочлена $3x^5+2x^4+x^3-10x-8$ определите кратность корня с=-1.
7. Разложите многочлен $x^4-8x^3+24x^2-50x+22$ по степеням $x-2$.
8. Найдите многочлен наименьшей степени с вещественными коэффициентами, имеющий тройной корень $i$, простые корни 2 и 3.
9. Найдите коэффициент $a$ так, чтобы многочлен $x^5-ax^2-ax+1$ имел $-1$ корнем не ниже второй кратности.
10. Запишите в лексикографическом виде: $2x^2y-3x^2y^2+y^5+4x^3y^2+7xy-2x+3$.
11. Выразите через элементарные симметрические многочлены: $x_1^3+x_2^3+x_3^3-3x_1x_2x_3$.

12. Представьте в виде суммы простейших дробей над полем действительных чисел: $\frac{2x^4+3}{x^3(x^2-1)}$.

**Примеры индивидуальных домашних заданий**

**Тема: Кольца и поля**

1. Докажите, что в кольце многочленов над конечным полем все идеалы главные.
2. Постройте пример бесконечного поля простой характеристики.
3. Найти все автоморфизмы поля комплексных чисел, которые оставляют на месте действительные числа.
4. Определите условия, прикоторых факторкольцо кольца многочленов над полем будет полем.

**Тема: Группы**

Пусть $A, B, C$ подгруппы конечной группы $G$. Докажите, что

1) если $B \le A$, то $|A:B| \ge |C \cap A : C \cap B|$;
2) $|G:A \cap B| \le |G:A||G:B|$;
3) $A \cup B$ является подгруппой $G$, если и только если $A \subseteq B$ или $B \subseteq A$;
4) если $G = AA^g$ для некоторого $g \in G$, тогда $G = A$.
5) группа $G$ имеет четный порядок, если и только если число инволюций (элементов второго порядка) нечетно;
6) если каждый элемент группы имеет порядок два, то группа абелева;
7) если группа содержит точно одну максимальную подгруппу, то она циклическая.

## III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Алгебраические основы криптографии» 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. Теория групп | 28.02 - 8.03 | индивидуальное домашнее задание | 1 неделя |
| 2. Кольца и поля | 8.03 - 28.03 | индивидуальное домашнее задание | 1 неделя |
| 3. Линейные рекуррентные последовательности | 28.03 – 14.04 | индивидуальное домашнее задание | 1 неделя |
| 4. Полугруппы и конечные автоматы | 14.04 - 28.04 | индивидуальное домашнее задание | 1 неделя |
| 5. Решетки и булевы функции | 28.04 - 10.05 | индивидуальное домашнее задание | 1 неделя |
| 6. Эллиптические кривые | 10.05 - 28.05 | 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 зачету.

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 | Конечные группы<br>Кольца и поля<br>Линейные рекуррентные последовательности над конечными полями | ПК-5.1 Выбирает оптимальные системы программирования, наиболее подходящие для решения поставленной задачи | Знает современные методы цифровой обработки изображений | Коллоквиум (УО-2) | Вопросы к зачету 1-5 |
| | | | Умеет анализировать поставленную задачу и находить алгоритм ее решения | Индивидуальное домашнее задание (ПР-6) | ИДЗ |
| | | | Владеет навыками отбора оптимальных систем программирования, наиболее подходящих для решения поставленной задачи | Коллоквиум (УО-2) | |
| 2 | Полугруппы и конечные автоматы<br>Решетки и решеточные продолжения булевых функций | ПК-5.2 Применяет на практике методы моделирования информационных процессов, осуществляет работы над производственным проектом в составе группы научных специалистов | Знает средства компьютерной графики | Индивидуальное домашнее задание (ПР-6) | Вопросы к зачету 6-10 |
| | | | Умеет применять методы моделирования информационных процессов | Коллоквиум (УО-2) | |
| | | | Владеет навыками работы над производственным проектом в составе группы научных специалистов | Индивидуальное домашнее задание (ПР-6) | |
| 3 | Конечные группы<br>Кольца и поля<br>Линейные рекуррентные последовательности над конечными полями | ПК-6.1 Обосновывает необходимость работы над конкретным проектом, проводит анализ и дает оценку его эффективности, осуществляет | Знает основные подходы к организации предметной среды математики | | Вопросы к зачету 11-12 |
| | | | Умеет обосновывать и защищать предлагаемый проект, доказывать его эффективность и востребованность на выбранном рынке | Индивидуальное домашнее задание (ПР-6) | ИДЗ |
| | | | Владеет опытом выражения | Индивид | |

| | | | | | |
|---|---|---|---|---|---|
| | | защиту предлагаемого проекта, показывает его востребованность на выбранном рынке | своих мыслей и мнения, навыками оценки эффективности проекта | уальное домашне е задание (ПР-6) | |
| 4 | Полугруппы и конечные автоматы Решетки и решеточные продолжения булевых функций | 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 | Индивид уальное домашне е задание (ПР-6) | Вопросы к зачету 13-14 |
| | | | Умеет выбирать методы построения, анализа и применения математических моделей при решении задач проектно-технологической деятельности | Коллокви ум (УО-2) | ИДЗ |
| | | | 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 | Коллокви ум (УО-2)) | |
| 5 | Конечные группы Кольца и поля Линейные рекуррентные последовательности над конечными полями | ПК-5.1 Выбирает оптимальные системы программирования, наиболее подходящие для решения поставленной задачи | Знает современные методы цифровой обработки изображений | Коллокви ум (УО-2) | Вопросы к зачету 15 |
| | | | Умеет анализировать поставленную задачу и находить алгоритм ее решения | Индивид уальное домашне е задание (ПР-6) | ИДЗ |
| | | | Владеет навыками отбора оптимальных систем программирования, наиболее подходящих для решения поставленной задачи | Коллокви ум (УО-2) | |
| 6 | Полугруппы и конечные автоматы | ПК-5.2 Применяет на практике методы моделирования информационных процессов, осуществляет работы над производственным проектом в составе группы научных специалистов | Знает средства компьютерной графики | Коллокви ум (УО-2) | Вопросы к зачету 16-19 |
| | | | Умеет применять методы моделирования информационных процессов | Индивид уальное домашне е задание (ПР-6) | ИДЗ |
| | | | Владеет навыками работы над производственным проектом в составе группы научных | Индивид уальное домашне | |

| | | | | | |
|---|---|---|---|---|---|
| | | | специалистов | е 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. Алферов Н.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии, М. Гелиос АРВ, 2012 г. http://lib.dvfu.ru:8080/lib/item?id=chamo:1640&theme=FEFU
2. Сагалович Ю.Л. Введение в алгебраические коды : учебное пособие, Институт проблем передачи информации РАН. 2014 г.
3. Романьков В.А. Алгебраическая криптография: монография**,** Изд-во Омского государственного университета им. Ф.М. Достоевского, 2013 https://e.lanbook.com/book/75405
4. Мартынов Л.М. Алгебра для криптографии. Часть 1: учебное пособие**,** Изд-во Омского государственного университета путей сообщения, 2015 https://e.lanbook.com/book/129189
5. Мартынов Л.М. Алгебра для криптографии. Часть 2: учебное пособие**,** Изд-во Омского государственного университета путей сообщения, 2015 https://e.lanbook.com/book/129188
6. 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 (лекции, практические занятия) планируется самостоятельная работа, итоги которой влияют на окончательную оценку по итогам освоения учебной дисциплины. Все задания (аудиторные и самостоятельные) необходимо выполнять и предоставлять на оценку в соответствии с графиком.

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

*Лекционные занятия* ориентированы на освещение вводных тем в каждый раздел курса и призваны ориентировать студентов в предлагаемом

материале, заложить научные и методологические основы для дальнейшей самостоятельной работы студентов.

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

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

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

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

**Подготовка к зачету.** К сдаче зачета допускаются обучающиеся, выполнившие все задания (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.<br><br>Реквизиты подтверждающего документа |
|---|---|---|
| 690922, Приморский край, г. Владивосток, остров Русский, полуостров Саперный, поселок Аякс, 10, корпус D, ауд. D732.<br><br>Учебная аудитория для проведения занятий лекционного типа, групповых и | Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 45)<br><br>Оборудование:<br><br>ЖК-панель 47", Full HD, LG | |

| | | |
|---|---|---|
| индивидуальных консультаций, текущего контроля и промежуточной аттестации | М4716 ССВА – 1 шт.<br><br>Доска аудиторная. | |
| 690922, Приморский край, г.Владивосток, остров Русский, полуостров Саперный, поселок Аякс, 10, корп. А (Лит. П), Этаж 10, каб.А1017.<br><br>Аудитория для самостоятельной работы | Оборудование:<br><br>Моноблок Lenovo C360G-i34164G500UDK – 15 шт.<br><br>Интегрированный сенсорный дисплей Polymedia FlipBox - 1 шт.<br><br>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 «Алгебраические основы криптографии» 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 «Алгебраические основы криптографии» проводится в соответствии с локальными нормативными актами ДВФУ и является обязательной. Форма отчётности по дисциплине – зачет (2-й, осенний семестр). Зачет по дисциплине включает ответы на 3 вопроса. Два вопроса носят теоретический характер, один вопрос носит практический характер.

**Методические указания по сдаче зачета**

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

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

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

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

Время, предоставляемое студенту на подготовку к ответу на зачете, должно составлять не более 30 минут. По истечении данного времени студент должен быть готов к ответу.

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

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

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

**Вопросы к сдаче зачета**

1. Группы. Теорема Лагранжа.
2. Циклические группы.
3. НОД. Алгоритм Евклида. Теорема и линейном представлении НОД. НОК. Взаимно простые числа. Теорема Евклида.
4. Бесконечность количества простых чисел. Основная теорема арифметики.
5. Формула для вычисления функции Эйлера. Целая часть числа.
6. Свойства сравнений. Полная и приведенная системы представителей.
7. Теорема Эйлера. Малая теорема Ферма. Кольцо классов вычетов. Поле классов вычетов по простому модулю.
8. Гомоморфизмы групп.
9. Факторгруппы и нормальные подгруппы.
10. Действия групп на множествах, теорема о стабилизаторе.
11. Идеалы в кольцах многочленов.
12. Неприводимые многочлены. Основная теорема арифметики кольца многочленов.
13. Характеристика поля.
14. Сочетания. Перестановки. Группа подстановок. Инверсии. Транспозиции.
15. Алгебраические расширения конечных полей.
16. Рекуррентные последовательности над конечными полями.
17. Алгоритм Берлекемпа-Месси.
18. Эллиптические кривые над конечными полями.
19. Теорема о порядке группы точек эллиптической кривой.

**Критерии выставления оценки студенту на зачете**

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

| Оценка | Требования к сформированным компетенциям |
|---|---|
| ***«зачтено»*** | 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. |
| ***«не зачтено»*** | 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.

## Критерии оценивания

| Оценка | Требования к сформированным компетенциям |
|---|---|
| | Студент показывает глубокое и систематическое |

| | |
|---|---|
| ***«зачтено»*** | 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. |
| ***«не зачтено»*** | Незнание, либо отрывочное представление о данной проблеме в рамках учебно-программного материала; неумение использовать понятийный аппарат; отсутствие логической связи в ответе. |