Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский ядерный университет «МИФИ»

ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ

КАФЕДРА КРИПТОЛОГИИ И ДИСКРЕТНОЙ МАТЕМАТИКИ

ОДОБРЕНО
УМС ИИКС Протокол №УМС-575/01-1 от 30.08.2021 г.
НТС ЛАПЛАЗ Протокол №3 от 30.08.2021 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ВВЕДЕНИЕ В ОБЩУЮ АЛГЕБРУ И ТЕОРИЮ ЧИСЕЛ

Направление подготовки (специальность)

[1] 10.03.01 Информационная безопасность
[2] 01.03.02 Прикладная математика и информатика

Семестр	Трудоемкость, кред.	Общий объем курса, час.	Лекции, час.	Практич. занятия, час.	Лаборат. работы, час.	В форме практической подготовки/ В	СРС, час.	КСР, час.	Форма(ы) контроля, экз./зач./КР/КП
4, 2	3	108	45	15	0		48	0	З
Итого	3	108	45	15	0	0	48	0	

Москва, 2020

АННОТАЦИЯ

Цель дисциплины — формирование у студентов знаний в области теории множеств и отображений, основ алгебры, дополнительных разделов линейной алгебры, элементарной теории чисел, необходимых для дальнейшего изучения и понимания основных математических методов, лежащих в основе криптографических методов обеспечения информационной безопасности.

Задачи дисциплины:

- изучение понятий множества и отображения, их базовых свойств;
- изучение основ алгебры, включая элементы теории групп, колец и полей;
- освоение методов решения линейных и нелинейных уравнений и сравнений в различных алгебраических структурах (в т. ч. в группах подстановок, в кольцах вычетов, в конечных полях);
- освоение методов расчета параметров графа линейного преобразования линейного пространства над конечным полем (на основе использования аппарата линейной алгебры);
- формирование способности у студента применять изучаемый в курсе математический аппарат для исследования свойств криптографических преобразований.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Цель дисциплины — формирование у студентов знаний в области теории множеств и отображений, основ алгебры, дополнительных разделов линейной алгебры, элементарной теории чисел, необходимых для дальнейшего изучения и понимания основных математических методов, лежащих в основе криптографических методов обеспечения информационной безопасности.

Задачи дисциплины:

- изучение понятий множества и отображения, их базовых свойств;
- изучение основ алгебры, включая элементы теории групп, колец и полей;
- освоение методов решения линейных и нелинейных уравнений и сравнений в различных алгебраических структурах (в т. ч. в группах подстановок, в кольцах вычетов, в конечных полях);
- освоение методов расчета параметров графа линейного преобразования линейного пространства над конечным полем (на основе использования аппарата линейной алгебры);
- формирование способности у студента применять изучаемый в курсе математический аппарат для исследования свойств криптографических преобразований.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Полученные знания используются при изучении различных математических дисциплин и дисциплин специализации

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
ОПК-2 [1] – Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	З-ОПК-2 [1] – знать программные средства системного и прикладного назначения, информационно-коммуникационные технологии для решения профессиональных задач У-ОПК-2 [1] – уметь применять программные средства системного и прикладного назначения, информационно-коммуникационные технологии для решения профессиональных задач В-ОПК-2 [1] – владеть принципами работы программных средств системного и прикладного назначения, информационно-коммуникационных технологий для решения профессиональных задач
ОПК-3 [1] – Способен использовать необходимые математические методы для решения задач профессиональной деятельности	З-ОПК-3 [1] – основные математические методы для решения задач обеспечения защиты информации У-ОПК-3 [1] – уметь использовать основные математические методы для решения задач обеспечения защиты информации В-ОПК-3 [1] – владеть основными математическими методами для решения задач обеспечения защиты информации
УКЕ-1 [1] – Способен использовать знания естественнонаучных дисциплин, применять методы математического анализа и моделирования, теоретического и экспериментального исследования в поставленных задачах	З-УКЕ-1 [1] – знать: основные законы естественнонаучных дисциплин, методы математического анализа и моделирования, теоретического и экспериментального исследования У-УКЕ-1 [1] – уметь: использовать математические методы в технических приложениях, рассчитывать основные числовые характеристики случайных величин, решать основные задачи математической статистики; решать типовые расчетные задачи В-УКЕ-1 [1] – владеть: методами математического анализа и моделирования; методами решения задач анализа и расчета характеристик физических систем, основными приемами обработки экспериментальных данных, методами работы с прикладными программными продуктами
ОПК-1 [2] – Способен применять фундаментальные знания, полученные в области математических и (или) естественных наук, и использовать их в профессиональной деятельности	З-ОПК-1 [2] – знать естественнонаучные методы познания окружающего мира, знать фундаментальный математический аппарат; У-ОПК-1 [2] – уметь применять естественнонаучные и математические методы исследования различных явлений, процессов и задач В-ОПК-1 [2] – владеть навыками исследования различных явлений и процессов с использованием естественнонаучного и математического подхода
ОПК-3 [2] – Способен применять и	З-ОПК-3 [2] – знать принципы построения

модифицировать математические модели для решения задач в области профессиональной деятельности	математических моделей физических явлений и процессов У-ОПК-3 [2] – уметь формулировать математические модели различных явлений и процессов на основе физических принципов и законов В-ОПК-3 [2] – владеть навыками построения математических моделей физических явлений и процессов

Профессиональные компетенции в соотвествии с задачами и объектами (областями знаний) профессиональной деятельности:

Задача профессиональной деятельности (ЗПД)	**Объект или область знания**	**Код и наименование профессиональной компетенции; Основание (профессиональный стандарт-ПС, анализ опыта)**	**Код и наименование индикатора достижения профессиональной компетенции**
научно-исследовательский			
Изучение и систематизация новых научных результатов, научной литературы или научно-исследовательских проектов в соответствии с профилем профессиональной деятельности.	Научные статья и тезисы конференций, научно-технические отчеты, опубликованные результаты научных исследований, соответствующая документация.	ПК-1 [2] - Способен собирать, обрабатывать и интерпретировать результаты научных исследований в области прикладной математики и информационных технологий *Основание:* Профессиональный стандарт: 40.011	З-ПК-1[2] - знать основные методы научного познания, методы сбора и анализа информации;; У-ПК-1[2] - уметь анализировать информацию, строить логические схемы, интерпретировать результаты научных исследований, критически мыслить, сравнивать результаты различных исследований, формировать собственную позицию в рамках рассматриваемой задачи;; В-ПК-1[2] - владеть навыками работы с научной литературой и навыками интерпретации результатов научных исследований;
Разработка математических моделей, алгоритмов и методов для	Математические модели и алгоритмы.	ПК-2 [2] - Способен понимать, применять и совершенствовать современный	З-ПК-2[2] - знать современный математический аппарат,

решения различных задач.		математический аппарат *Основание:* Профессиональный стандарт: 06.001	используемый при описании, решении и анализе различных прикладных задач; У-ПК-2[2] - использовать современный математический аппарат для построения математических моделей и алгоритмов решения различных прикладных задач; В-ПК-2[2] - владеть навыками применения современного математического аппарата для построения математических моделей различных процессов, для обработки экспериментальных, статистических и теоретических данных, для разработки новых алгоритмов и методов исследования задач различных типов

4. ВОСПИТАТЕЛЬНЫЙ ПОТЕНЦИАЛ ДИСЦИПЛИНЫ

Направления/цели воспитания	Задачи воспитания (код)	Воспитательный потенциал дисциплин
Профессиональное воспитание	Создание условий, обеспечивающих, формирование ответственности за профессиональный выбор, профессиональное развитие и профессиональные решения (В18)	Использование воспитательного потенциала дисциплин профессионального модуля для формирования у студентов ответственности за свое профессиональное развитие посредством выбора студентами индивидуальных образовательных траекторий, организации системы общения между всеми участниками образовательного процесса, в том числе с использованием новых информационных технологий.
Профессиональное	Создание условий,	1.Использование воспитательного

воспитание	обеспечивающих, формирование научного мировоззрения, культуры поиска нестандартных научно-технических/практических решений, критического отношения к исследованиям лженаучного толка (В19)	потенциала дисциплин/практик «Научно-исследовательская работа», «Проектная практика», «Научный семинар» для: - формирования понимания основных принципов и способов научного познания мира, развития исследовательских качеств студентов посредством их вовлечения в исследовательские проекты по областям научных исследований. 2.Использование воспитательного потенциала дисциплин "История науки и инженерии", "Критическое мышление и основы научной коммуникации", "Введение в специальность", "Научно-исследовательская работа", "Научный семинар" для: - формирования способности отделять настоящие научные исследования от лженаучных посредством проведения со студентами занятий и регулярных бесед; - формирования критического мышления, умения рассматривать различные исследования с экспертной позиции посредством обсуждения со студентами современных исследований, исторических предпосылок появления тех или иных открытий и теорий.
Профессиональное воспитание	Создание условий, обеспечивающих, формирование профессионально значимых установок: не производить, не копировать и не использовать программные и технические средства, не приобретённые на законных основаниях; не нарушать признанные нормы авторского права; не нарушать тайны передачи сообщений, не практиковать вскрытие информационных систем и сетей передачи данных; соблюдать конфиденциальность доверенной информации (В40)	1. Использование воспитательного потенциала дисциплин "Информатика (Основы программирования)", Программирование (Объектно-ориентированное программирование)", "Программирование (Алгоритмы и структуры данных)" для формирования культуры написания и оформления программ, а также привития навыков командной работы за счет использования систем управления проектами и контроля версий. 2.Использование воспитательного потенциала дисциплины

		"Проектная практика" для формирования культуры решения изобретательских задач, развития логического мышления, путем погружения студентов в научную и инновационную деятельность института и вовлечения в проектную работу. 3.Использование воспитательного потенциала профильных дисциплин для формирования навыков цифровой гигиены, а также системности и гибкости мышления, посредством изучения методологических и технологических основ обеспечения информационной безопасности и кибербезопасности при выполнении и защите результатов учебных заданий и лабораторных работ по криптографическим методам защиты информации в компьютерных системах и сетях. 4.Использование воспитательного потенциала дисциплин " "Информатика (Основы программирования)", Программирование (Объектно-ориентированное программирование)", "Программирование (Алгоритмы и структуры данных)" для формирования культуры безопасного программирования посредством тематического акцентирования в содержании дисциплин и учебных заданий. 5.Использование воспитательного потенциала дисциплины "Проектная практика" для формирования системного подхода по обеспечению информационной безопасности и кибербезопасности в различных сферах деятельности посредством исследования и перенятия опыта постановки и решения научно-практических задач организациями-партнерами.

Введение в общую алгебру и теорию чисел

5. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Разделы учебной дисциплины, их объем, сроки изучения и формы контроля:

№ п.п	Наименование раздела учебной дисциплины	Недели	Лекции/ Практ. (семинары)/ Лабораторные работы, час.	Обязат. текущий контроль (форма*, неделя)	Максимальный балл за раздел**	Аттестация раздела (форма*, неделя)	Индикаторы освоения компетенции
	2 Семестр						
1	Первый раздел	1-8			25	КИ-8	З-ОПК-1, У-ОПК-1, В-ОПК-1, З-ОПК-3, У-ОПК-3, В-ОПК-3, З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-2, У-ПК-2, В-ПК-2, З-УК-1, У-УК-1
2	Второй раздел	9-15			25	КИ-15	З-ОПК-1,

							У-ОПК-1, В-ОПК-1, З-ОПК-3, У-ОПК-3, В-ОПК-3, З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-2, У-ПК-2, В-ПК-2, З-УК-1, У-УК-1, В-УК-1
	Итого за 2 Семестр		45/15/0		50		
	Контрольные мероприятия за 2 Семестр				50	З	З-ОПК-2, У-ОПК-2, В-ОПК-2, З-ОПК-3, У-ОПК-3, В-ОПК-3,

							З-УКЕ-1, У-УКЕ-1, В-УКЕ-1, З-ОПК-1, У-ОПК-1, В-ОПК-1, З-ОПК-3, У-ОПК-3, В-ОПК-3, З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-2, У-ПК-2, В-ПК-2

* – сокращенное наименование формы контроля

** – сумма максимальных баллов должна быть равна 100 за семестр, включая зачет и (или) экзамен

Сокращение наименований форм текущего контроля и аттестации разделов:

Обозначение	**Полное наименование**
КИ	Контроль по итогам
З	Зачет

КАЛЕНДАРНЫЙ ПЛАН

Недели	Темы занятий / Содержание	Лек., час.	Пр./сем., час.	Лаб., час.
	2 Семестр	45	15	0
1-8	**Первый раздел**	24	8	
1 - 8	**Множества и их свойства** Множества и операции над множествами. Отображения. Бинарные отношения и их свойства. Основные алгебраические структуры. Основы теории групп. Основы теории колец. Линейные сравнения	Всего аудиторных часов		
		24	8	
		Онлайн		
9-15	**Второй раздел**	21	7	
9 - 15	**Преобразования множеств** Нелинейные сравнения. Основы теории полей. λ-матрицы над полем. Граф линейного преобразования. Линейные рекуррентные последовательности	Всего аудиторных часов		
		21	7	
		Онлайн		

Сокращенные наименования онлайн опций:

Обозначение	Полное наименование
ЭК	Электронный курс
ПМ	Полнотекстовый материал
ПЛ	Полнотекстовые лекции
ВМ	Видео-материалы
АМ	Аудио-материалы
Прз	Презентации
Т	Тесты
ЭСМ	Электронные справочные материалы
ИС	Интерактивный сайт

6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Основными образовательными технологиями в освоении дисциплин профессионального цикла являются традиционные технологии лекций и лабораторных работ. Интерактивные методики обеспечиваются решением индивидуальных задач студентами и коллективным обсуждением результатов и методов решения.

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств по дисциплине обеспечивает проверку освоения планируемых результатов обучения (компетенций и их индикаторов) посредством мероприятий текущего, рубежного и промежуточного контроля по дисциплине.

Связь между формируемыми компетенциями и формами контроля их освоения представлена в следующей таблице:

Компетенция	Индикаторы освоения	Аттестационное мероприятие (КП 1)
ОПК-2	З-ОПК-2	З

	У-ОПК-2	З
	В-ОПК-2	З
ОПК-3	З-ОПК-3	З
	У-ОПК-3	З
	В-ОПК-3	З
УКЕ-1	З-УКЕ-1	З
	У-УКЕ-1	З
	В-УКЕ-1	З
ОПК-1	З-ОПК-1	З, КИ-8, КИ-15
	У-ОПК-1	З, КИ-8, КИ-15
	В-ОПК-1	З, КИ-8, КИ-15
ОПК-3	З-ОПК-3	З, КИ-8, КИ-15
	У-ОПК-3	З, КИ-8, КИ-15
	В-ОПК-3	З, КИ-8, КИ-15
ПК-1	З-ПК-1	З, КИ-8, КИ-15
	У-ПК-1	З, КИ-8, КИ-15
	В-ПК-1	З, КИ-8, КИ-15
ПК-2	З-ПК-2	З, КИ-8, КИ-15
	У-ПК-2	З, КИ-8, КИ-15
	В-ПК-2	З, КИ-8, КИ-15

Шкалы оценки образовательных достижений

Шкала каждого контрольного мероприятия лежит в пределах от 0 до установленного максимального балла включительно. Итоговая аттестация по дисциплине оценивается по 100-балльной шкале и представляет собой сумму баллов, заработанных студентом при выполнении заданий в рамках текущего и промежуточного контроля.

Итоговая оценка выставляется в соответствии со следующей шкалой:

<table>
<tr><th>Сумма баллов</th><th>Оценка по 4-ех балльной шкале</th><th>Оценка ECTS</th><th>Требования к уровню освоению учебной дисциплины</th></tr>
<tr><td>90-100</td><td>5 – «отлично»</td><td>A</td><td>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, использует в ответе материал монографической литературы.</td></tr>
<tr><td>85-89</td><td rowspan="3">4 – «хорошо»</td><td>B</td><td rowspan="3">Оценка «хорошо» выставляется студенту, если он твёрдо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.</td></tr>
<tr><td>75-84</td><td>C</td></tr>
<tr><td>70-74</td><td rowspan="2">D</td></tr>
<tr><td>65-69</td><td rowspan="2">3 – «удовлетворительно»</td><td rowspan="2">Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные</td></tr>
<tr><td>60-64</td><td>E</td></tr>
</table>

			формулировки, нарушения логической последовательности в изложении программного материала.
Ниже 60	2 – «*неудовлетворительно*»	F	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине.

Оценочные средства приведены в Приложении.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. ЭИ З-80 Алгебра. Основной курс с решениями и указаниями : электронное издание, Москва: Лаборатория знаний, 2018

2. ЭИ К 58 Сборник задач по дискретной математике : учебное пособие, Санкт-Петербург: Лань, 2021

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

Специальное программное обеспечение не требуется

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

https://online.mephi.ru/

http://library.mephi.ru/

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Специальное материально-техническое обеспечение не требуется

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ

Введение в общую алгебру и теорию чисел

11. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

Введение в общую алгебру и теорию чисел

Автор(ы):

Епишкина Анна Васильевна, к.т.н.