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 № 4/1/2023

от 25.04.2023 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ТЕОРЕТИКО-ЧИСЛОВЫЕ АЛГОРИТМЫ В КРИПТОГРАФИИ / SPECIAL ALGORITHMS IN CRYPTOGRAPHY

Направление подготовки (специальность) [1] 10.03.01 Информационная безопасность

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
8	1	36	0	20	0		16	0	З
Итого	1	36	0	20	0	0	16	0	

АННОТАЦИЯ

Целью освоения дисциплины является получение знаний, умений, навыков и опыта деятельности в области анализа и применения теоретико-числовых алгоритмов при решении задач информационной безопасности, характеризующих этапы формирования компетенций и обеспечивающих достижение планируемых результатов освоения образовательной программы.

Изучение дисциплины предусматривает приобретение теоретических и практических навыков при решении задач из области алгоритмической теории чисел, имеющих важные приложения в криптографии. Для практической реализации криптографических примитивов и обоснования стойкости криптографичесикх средств, а также для разработки методов их анализа необходимо владеть такими методами и алгоритмами, как алгоритмы проверки простоты целых чисел, методы факторизациицелых чисел, алгоритмы дискретного логарифмирования, чему и посвящен настоящий курс.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью освоения дисциплины является получение знаний, умений, навыков и опыта деятельности в области анализа и применения теоретико-числовых алгоритмов при решении задач информационной безопасности, характеризующих этапы формирования компетенций и обеспечивающих достижение планируемых результатов освоения образовательной программы.

Изучение дисциплины предусматривает приобретение теоретических и практических навыков при решении задач из области алгоритмической теории чисел, имеющих важные приложения в криптографии. Для практической реализации криптографических примитивов и обоснования стойкости криптографичесикх средств, а также для разработки методов их анализа необходимо владеть такими методами и алгоритмами, как алгоритмы проверки простоты целых чисел, методы факторизациицелых чисел, алгоритмы дискретного логарифмирования, чему и посвящен настоящий курс.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина по выбору

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции

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;**	**Код и наименование индикатора достижения**

		Основание (профессиональный стандарт-ПС, анализ опыта)	**профессиональной компетенции**
эксплуатационный			
эксплуатация технических и программно-аппаратных средств защиты информации	программно-аппаратные средства защиты информации	ПК-1 [1] - способен устанавливать, настраивать и проводить техническое обслуживание средств защиты информации *Основание:* Профессиональный стандарт: 06.032	З-ПК-1[1] - знать требования к проведению технического обслуживания средств защиты информации ; У-ПК-1[1] - уметь устанавливать, настраивать и проводить техническое обслуживание средств защиты информации; В-ПК-1[1] - владеть навыками проведения технического обслуживания средств защиты информации
организационно-управленческий			
организация работы по эксплуатации системы защиты информации	системы защиты информации	ПК-1.1 [1] - способен участвовать в разработке политик управления доступом и информационными потоками в компьютерных системах *Основание:* Профессиональный стандарт: 06.032	З-ПК-1.1[1] - знать способы разработки политик управления доступом и информационными потоками в компьютерных системах; У-ПК-1.1[1] - уметь разрабатывать политики управления доступом и информационными потоками в компьютерных системах; В-ПК-1.1[1] - владеть принципами формирования политики управления доступом и информационными потоками в компьютерных системах
проектно-технологический			
проектирование и разработка систем	технологии обеспечения	ПК-1.2 [1] - способен разрабатывать и	З-ПК-1.2[1] - знать алгоритмы решения

информационной безопасности	информационной безопасности компьютерных систем	анализировать алгоритмы решения профессиональных задач, реализовывать их в современных программных комплексах *Основание:* Профессиональный стандарт: 06.032	профессиональных задач; У-ПК-1.2[1] - уметь разрабатывать и анализировать алгоритмы решения профессиональных задач, реализовывать их в современных программных комплексах; В-ПК-1.2[1] - владеть принципами разработки и анализа алгоритмов решения профессиональных задач
проектирование и разработка систем информационной безопасности	технологии обеспечения информационной безопасности компьютерных систем	ПК-2 [1] - способен проектировать подсистемы безопасности информации с учетом действующих нормативных и методических документов *Основание:* Профессиональный стандарт: 06.032	З-ПК-2[1] - знать действующие нормативные и методические документы по проектированию подсистемы безопасности информации ; У-ПК-2[1] - уметь проектировать подсистемы безопасности информации с учетом действующих нормативных и методических документов; В-ПК-2[1] - владеть принципами проектирования подсистемы безопасности информации

4. ВОСПИТАТЕЛЬНЫЙ ПОТЕНЦИАЛ ДИСЦИПЛИНЫ

Направления/цели воспитания	Задачи воспитания (код)	Воспитательный потенциал дисциплин
Профессиональное воспитание	Создание условий, обеспечивающих, формирование культуры информационной безопасности (В23)	Использование воспитательного потенциала дисциплин профессионального модуля для формирование базовых навыков информационной безопасности через изучение последствий халатного

		отношения к работе с информационными системами, базами данных (включая персональные данные), приемах и методах злоумышленников, потенциальном уроне пользователям.

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
	8 Семестр						
1	Первый раздел	1-8	0/10/0		25	КИ-8	З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-1.1, У-ПК-1.1, В-ПК-1.1, З-ПК-1.2, У-ПК-1.2, В-ПК-1.2, З-ПК-2, У-ПК-2, В-ПК-2
2	Второй раздел	9-15	0/10/0		25	КИ-15	З-ПК-

							1, У-ПК-1, В-ПК-1, З-ПК-1.1, У-ПК-1.1, В-ПК-1.1, З-ПК-1.2, У-ПК-1.2, В-ПК-1.2, З-ПК-2, У-ПК-2, В-ПК-2
	Итого за 8 Семестр		0/20/0		50		
	Контрольные мероприятия за 8 Семестр				50	З	З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-1.1, У-ПК-1.1, В-ПК-1.1, З-ПК-1.2, У-ПК-1.2, В-ПК-1.2, 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.**
	8 Семестр	0	20	0
1-8	**Первый раздел**	0	10	0
	Основы теории алгоритмов Понятие алгоритма, примеры алгоритмов. Понятие рекурсивной функции. Основные требования к алгоритмам. Типы алгоритмических моделей. Машина Тьюринга и ее элементы. Система команд. Программа машины, конфигурация, активная зона конфигурации, машинное слово. Эквивалентность машин Тьюринга. Функции, правильно вычислимые по Тьюрингу. Тезис Тьюринга. Машина произвольного доступа и вычислимые функции. Тезис Черча для машины произвольного доступа. Рекурсия как метод определения арифметических функций. Класс частично рекурсивных функций. Базисные функции. Операции над функциями. Общерекурсивные и примитивно-рекурсивные функции. Тезис Черча для частично-рекурсивных функций. Способы доказательства вычислимости функций. Теорема о вычислимости суперпозиции. Теорема о вычислимости рекурсии. Теорема о вычислимости минимизации. Теорема о частичной рекурсивности функций, вычислимых на машине произвольного доступа. Алгоритмически неразрешимые проблемы. Характеристики сложности вычислений: временная и емкостная сложность. Классы сложности P и NP и их взаимосвязь. Понятие недетерминированной машины Тьюринга. Полиномиальная сводимость задач. NP-полные и NP-трудные задачи. Формулировка теоремы Кука.	Всего аудиторных часов 0 Онлайн 0	10 0	0 0
9-15	**Второй раздел**	0	10	0
	Криптографические алгоритмы	Всего аудиторных часов		

	Простое число. Каноническое разложение натурального числа. Методы проверки простоты чисел. Метод пробных делений. Решето Эратосфена. Тест на основе малой теоремы Ферма. Тесты на простоту для чисел специального вида. Числа Мерсенна. (N±1)-методы проверки простоты чисел и построения больших простых чисел. Алгоритм Конягина – Померанса. Вероятностные тесты на простоту. Тест Соловея – Штрассена. Тест Рабина – Миллера. Современные методы проверки простоты чисел. Понятие факторизации целых чисел. Алгоритм Ферма. (P 1)-метод Полларда и оценка его сложности. ρ-метод Полларда. Метод Шермана – Лемана. Алгоритм Ленстры. Алгоритм Полларда – Штрассена. Алгоритм Диксона. Стратегия LP и использование больших простых чисел. Стратегия PS и алгоритм Полларда – Штрассена. Стратегия EAS – стратегия раннего обрыва. Квадратичное решето. Субэкспоненциальные вероятностные алгоритмы. Методы Шнорра – Ленстры и Ленстры – Померанса. Алгоритмы решета числового поля. Задача дискретного логарифмирования. Алгоритм согласования. Алгоритм Полига – Хеллмана. ρ-метод Полларда для дискретного логарифмирования. Дискретное логарифмирование в простых полях. Дискретное логарифмирование в полях Галуа. Дискретное логарифмирование и решето числового поля.	0	10	0
		Онлайн		
		0	0	0

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

Образовательные технологии сочетают в себе совокупность методов и средств для реализации определенного содержания обучения и воспитания в рамках дисциплины, влючают решение дидактических и воспитательных задач, формируя основные понятия дисциплины, технологии проведения занятиий, усвоения новых знаний, технологии повторения и контроля материала, самостоятельной работы.

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)**
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-1.1	З-ПК-1.1	З, КИ-8, КИ-15
	У-ПК-1.1	З, КИ-8, КИ-15
	В-ПК-1.1	З, КИ-8, КИ-15
ПК-1.2	З-ПК-1.2	З, КИ-8, КИ-15
	У-ПК-1.2	З, КИ-8, КИ-15
	В-ПК-1.2	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:

Сумма баллов	Оценка по 4-ех балльной шкале	Оценка ECTS	Требования к уровню освоению учебной дисциплины
90-100	5 – *«отлично»*	A	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.
85-89	4 – «*хорошо*»	B	Оценка «хорошо» выставляется студенту, если он твёрдо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.
75-84		C	
70-74		D	
65-69			Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала,
60-64		E	

			но не усвоил его деталей, допускает неточности, недостаточно правильные 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.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

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

Студенты должны своевременно спланировать учебное время для поэтапного и системного изучения данной учебной дисциплины в соответствии с планом лекций и семинарских занятий, графиком контроля знаний.

Успешное освоение дисциплины требует от студентов посещения лекций, активной работы во время семинарских занятий, выполнения всех домашних заданий, ознакомления с базовыми учебниками, основной и дополнительной литературой, а также предполагает творческое участие студента путем планомерной, повседневной работы.

Изучение дисциплины следует начинать с проработки учебной программы, особое внимание, уделяя целям и задачам, структуре и содержанию курса.

Во время лекций рекомендуется писать конспект. Запись лекции – одна из форм активной самостоятельной работы студентов, требующая навыков и умения кратко, схематично, последовательно и логично фиксировать основные положения, выводы, обобщения, формулировки.

При необходимости в конце лекции преподаватель оставляет время для того, чтобы студенты имели возможность задать вопросы по изучаемому материалу.

Лекции нацелены на освещение основополагающих положений теории алгоритмов и теории функций алгебры логики, наиболее трудных вопросов, как правило, связанных с доказательством необходимых утверждений и теорем, призваны способствовать формированию навыков работы с научной литературой. Предполагается также, что студенты приходят на лекции, предварительно проработав соответствующий учебный материал по источникам, рекомендуемым программой.

Конспект лекций для закрепления полученных знаний необходимо просмотреть сразу после занятий. Хорошо отметить материал конспекта лекций, который вызывает затруднения для понимания. Можно попытаться найти ответы на затруднительные вопросы, используя рекомендуемую литературу. Если самостоятельно не удалось разобраться в материале, рекомендуется сформулировать вопросы и обратиться за помощью к преподавателю на консультации или ближайшей лекции.

В процессе изучения учебной дисциплины необходимо обратить внимание на самоконтроль. Требуется регулярно отводить время для повторения пройденного материала, проверяя свои знания, умения и навыки по контрольным вопросам, а также для выполнения домашних заданий, которые выдаются после каждого семинара.

Систематическая индивидуальная работа, постоянная активность на занятиях, готовность ставить и обсуждать актуальные проблемы курса – залог успешной работы и положительной оценки.

11. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

Учебный курс строится на интегративной основе и включает в себя как теоретические знания, так и практические навыки, получаемые студентами в ходе лекций, аудиторных практических занятий, лабораторных и самостоятельных занятий.

Данная дисциплина выполняет функции теоретической и практической подготовки студентов. Содержание дисциплины распределяется между лекционной и практической частями на основе принципа дополняемости: практические занятия, как правило, не дублируют лекции и посвящены рассмотрению практических примеров и конкретизации материала, введенного на лекции. В лекционном курсе главное место отводится общетеоретическим проблемам.

Содержание учебного курса, его объем и характер обусловливают необходимость оптимизации учебного процесса в плане отбора материала обучения и методики его организации, а также контроля текущей учебной работы. В связи с этим возрастает значимость и изменяется статус внеаудиторной (самостоятельной) работы, которая становится полноценным и обязательным видом учебно-познавательной деятельности студентов. При изучении курса самостоятельная работа включает:

самостоятельное ознакомление студентов с теоретическим материалом, представленным в отечественных и зарубежных научно-практических публикациях;

самостоятельное изучение тем учебной программы, достаточно хорошо обеспеченных литературой и сравнительно несложных для понимания;

подготовку к практическим занятиям по тем разделам, которые не дублируют темы лекционной части, а потому предполагают самостоятельную проработку материала учебных пособий.

Со стороны преподавателя должен быть установлен контакт со студентами, и они должны быть информированы о порядке прохождения курса, его особенностях, учебно-методическом обеспечении по данной дисциплине. Преподаватель дает методические рекомендации обучаемым по самостоятельному изучению проблем, характеризуя пути и средства достижения поставленных перед ними задач, высказывает советы и рекомендации по изучению учебной литературы, самостоятельной работе и работе на семинарских занятиях.

Автор(ы):

Епишкина Анна Васильевна, к.т.н.