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.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

РАЗРАБОТКА И АНАЛИЗ АЛГОРИТМОВ ДЛЯ КРИПТОГРАФИЧЕСКИХ ПРИЛОЖЕНИЙ

Направление подготовки (специальность) [1] 10.04.01 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**
3	2	72	0	32	16		24	0	З
Итого	2	72	0	32	16	0	24	0	

Москва, 2020

АННОТАЦИЯ

Ключевой задачей при разработке и применении криптографических систем защиты информации является определение надежности (стойкости) алгоритмов шифрования. Из-за отсутствия нижних оценок временной сложности решения теоретико-числовых задач, на которых основываются криптографические алгоритмы, единственным способом проверки их надежности является их экспериментальная проверка. Реализация подобных проверок основывается на разработке специальных параллельных алгоритмов и на использование современных технологий параллельного программирования.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Цель дисциплины – изучение принципов, методов и средств разработки алгоритмов, используемых при реализации криптографических приложений и при определении надежности алгоритмов шифрования.

В курсе рассматриваются следующие темы:

- алгоритмы решения задачи о рюкзаке;
- алгоритмы разложения целых чисел на множители, основанные на использование метода решета квадратичного поля;
- алгоритмы метода эллиптических кривых;
- алгоритмы больших чисел: возведения в степень, вычисления НОД и поиска обратного элемента.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Полученные в результате освоения учебной дисциплины знания, умения, навыки используются в процессе дипломного проектирования.

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; Основание (профессиональный стандарт-ПС, анализ опыта)**	**Код и наименование индикатора достижения профессиональной компетенции**
научно- исследовательский			
выполнение научно-	методы	ПК-3 [1] - Способен	З-ПК-3[1] - Знать:

исследовательских работ по развитию физических, математических или технических методов обеспечения безопасности данных	обеспечения безопасности данных	самостоятельно ставить конкретные задачи научных исследований в области ИБ или информационно-аналитических систем безопасности и решать их с использованием новейшего отечественного и зарубежного опыта *Основание:* Профессиональный стандарт: 06.032	руководящие и методические документы уполномоченных федеральных органов исполнительной власти, устанавливающие требования к организации и проведению аттестации и сертификационных испытаний средств и систем защиты сссэ от нсд, зткс; основные средства и способы обеспечения информационной безопасности, принципы построения средств и систем защиты сссэ от нсд, зткс; национальные, межгосударственные и международные стандарты, устанавливающие требования по защите информации, анализу защищенности сетей электросвязи и оценки рисков нарушения их информационной безопасности. ; У-ПК-3[1] - Уметь: организовывать сбор, обработку, анализ и систематизацию научно-технической информации, отечественного и зарубежного опыта по проблемам информационной безопасности сетей электросвязи.; В-ПК-3[1] - Владеть: организацией подготовки научно-технических отчетов, обзоров, публикаций

			по результатам выполненных исследований.
проектный			
разработка проектных решений по обеспечению безопасности данных с применением криптографических методов	информационные ресурсы	ПК-4.1 [1] - Способен разрабатывать проектные решения по обеспечению безопасности данных с применением криптографических методов *Основание:* Профессиональный стандарт: 06.032	З-ПК-4.1[1] - Знать: методы обеспечения безопасности данных с применением криптографических методов; У-ПК-4.1[1] - Уметь: разрабатывать проектные решения по обеспечению безопасности данных с применением криптографических методов; В-ПК-4.1[1] - Владеть: навыками разработки проектных решений по обеспечению безопасности данных с применением криптографических методов

4. 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
	3 Семестр						
1	Первый раздел	1-8			25	КИ-8	З-ПК-3, У-ПК-3, В-ПК-3, З-ПК-4.1, У-ПК-4.1, В-ПК-

							4.1
2	Второй раздел	9-16			25	КИ-16	З-ПК-3, У-ПК-3, В-ПК-3, З-ПК-4.1, У-ПК-4.1, В-ПК-4.1
	Итого за 3 Семестр		0/32/16		50		
	Контрольные мероприятия за 3 Семестр				50	З	З-ПК-3, У-ПК-3, В-ПК-3, З-ПК-4.1, У-ПК-4.1, В-ПК-4.1

* – 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.**
	3 Семестр	0	32	16
1-8	**Первый раздел**		16	8
1 - 4	**Алгоритмы решения задачи о рюкзаке.** Метод прямого перебора, проблема равномерной вычислительной нагрузки. Обход дерева укладок,	Всего аудиторных часов		
			8	4
		Онлайн		

	линеаризация дерева укладок. Метод динамического программирования. Сравнение. Слияние списков, переход к параллельному алгоритму.			
5 - 7	**Субэкспоненциальные алгоритмы разложения на множители.** Разложения с помощью метода решета квадратичного поля. Базовый алгоритм. Быстрые матричные методы. Вариация больших простых чисел. Использование нескольких полиномов. Автоматическая инициализация	Всего аудиторных часов		
			6	3
		Онлайн		
8	**Арифметика эллиптических кривых.** Арифметика эллиптических кривых.	Всего аудиторных часов		
			2	1
		Онлайн		
9-16	**Второй раздел**		16	8
9 - 12	**Алгоритмы метода эллиптических кривых; алгоритмы больших чисел: возведения в степень, вычисления НОД и поиска обратного элемента** Базовый алгоритм метода эллиптических кривых. Оптимизации алгоритма ECM. Доказательство простоты при помощи эллиптических кривых.	Всего аудиторных часов		
			8	4
		Онлайн		
13 - 16	**Большие числа.** Возведение в степень. Простые двоичные схемы. Улучшения схем возведения в степень. Вычисление НОД и ПОИСК обратного элемента. Двоичные алгоритмы вычисления НОД. Особые алгоритмы обращения. Рекурсивные алгоритмы для НОД в случае очень больших операндов	Всего аудиторных часов		
			8	4
		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

5. 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.

6. 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-3	З-ПК-3	З, КИ-8, КИ-16
	У-ПК-3	З, КИ-8, КИ-16
	В-ПК-3	З, КИ-8, КИ-16
ПК-4.1	З-ПК-4.1	З, КИ-8, КИ-16
	У-ПК-4.1	З, КИ-8, КИ-16
	В-ПК-4.1	З, КИ-8, КИ-16

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	3 – «*удовлетворительно*»		Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала.
60-64		E	
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.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. ЭИ П 16 Булевы функции в криптографии : учебное пособие, Санкт-Петербург: Лань, 2019

2. 004 М 21 Глобальная культура кибербезопасности : , Москва: Горячая линия -Телеком, 2018

3. ЭИ А 18 Дискретная математика. Модулярная алгебра, криптография, кодирование : , Москва: ДМК Пресс, 2017

4. 004 М 21 Основы политики безопасности критических систем информационной инфраструктуры. Курс лекций. : учеб. пособие для вузов., Москва: Горячая линия -Телеком, 2018

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

Специальное программное обеспечение не требуется

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

https://online.mephi.ru/

http://library.mephi.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Специальное материально-техническое обеспечение не требуется

9. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ

приложены

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

приложены

Автор(ы):

Борзунов Георгий Иванович, д.т.н., профессор