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

ТЕХНОЛОГИЯ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

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**
6	2	72	30	0	15		27	0	З
Итого	2	72	30	0	15	0	27	0	

Москва, 2020

АННОТАЦИЯ

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.

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.

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.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Полученные знания используются при изучении следующих дисциплин:

• Моделирование систем защиты информации;

• Аудит информационных технологий и систем обеспечения безопасности;
• Информационная безопасность открытых систем;
• Защита информации в банковских системах;
• Разработка и эксплуатация защищенных автоматизированных систем;
• Защищенный электронный документооборот в кредитно-финансовой сфере.

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**
проектно-технологический			
проектирование и разработка систем информационной безопасности	технологии обеспечения информационной безопасности компьютерных систем	ПК-1.2 [1] - способен разрабатывать и анализировать алгоритмы решения профессиональных задач, реализовывать их в современных программных комплексах *Основание:* Профессиональный стандарт: 06.032	З-ПК-1.2[1] - знать алгоритмы решения 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	З-ПК-2[1] - знать действующие нормативные и методические документы по проектированию

		нормативных и методических документов *Основание:* Профессиональный стандарт: 06.032	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 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 воспитание	Создание условий, обеспечивающих, формирование научного мировоззрения, культуры поиска нестандартных научно-технических/практических решений, критического отношения к исследованиям лженаучного толка (В19)	1.Использование воспитательного 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.

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

	6 Семестр						
1	Первый раздел	1-8			25	КИ-8	
2	Второй раздел	9-15			25	КИ-16	
	Итого за 6 Семестр		30/0/15		50		
	Контрольные мероприятия за 6 Семестр				50		

* – 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.**
	6 Семестр	30	0	15
1-8	**Первый раздел**	16		8
	Раздел 1 Алгоритмы решения задачи о рюкзаке; алгоритмы разложения целых чисел на множители, основанные на использование метода решета квадратичного поля	Всего аудиторных часов		
		Онлайн		
1 - 4	**Алгоритмы решения задачи о рюкзаке.** Метод прямого перебора, проблема равномерной вычислительной нагрузки. Обход дерева укладок, линеаризация дерева укладок. Метод динамического программирования. Сравнение. Слияние списков, переход к параллельному алгоритму.	Всего аудиторных часов		
		8		4
		Онлайн		
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		
9-15	**Второй раздел**	14		7
	Раздел 2 Алгоритмы метода эллиптических кривых; алгоритмы больших чисел: возведения в степень, вычисления НОД и поиска обратного элемента	Всего аудиторных часов		
		Онлайн		

9 - 12	**Алгоритмы метода эллиптических кривых;** Базовый алгоритм метода эллиптических кривых. Оптимизации алгоритма ECM. Доказательство простоты при помощи эллиптических кривых.	Всего аудиторных часов		
		8		4
		Онлайн		
13 - 15	**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		
		6		3
		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**

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 формулировки, нарушения логической последовательности в изложении программного материала.</td></tr>
<tr><td>60-64</td><td>E</td></tr>
<tr><td>Ниже 60</td><td>2 – «неудовлетворительно»</td><td>F</td><td>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.</td></tr>
</table>

Оценочные средства приведены в Приложении.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. 004 М 21 Глобальная культура кибербезопасности : , Москва: Горячая линия -Телеком, 2018

2. 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/

Автор(ы):

Смирнов Павел Владимирович, к.т.н.