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

РЕШЁТОЧНЫЕ И РЮКЗАЧНЫЕ АЛГОРИТМЫ В ПОСТ-КВАНТОВОЙ КРИПТОГРАФИИ

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
2	2	72	30	0	15		27	0	З
3	3	108	32	0	16		24	0	Э
Итого	5	180	62	0	31	0	51	0	

Москва, 2020

АННОТАЦИЯ

Решёточные и рюкзачные алгоритмы в пост-квантовой криптографии

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Решёточные и рюкзачные алгоритмы в пост-квантовой криптографии

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Решёточные и рюкзачные алгоритмы в пост-квантовой криптографии

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
ОПК-5 [1] – Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи	З-ОПК-5 [1] – Знать: теоретические и эмпирические методы научных исследований, порядок проведения научных исследований У-ОПК-5 [1] – Уметь: применять методы научных исследований в научной деятельности, обобщать полученные экспериментальные данные, анализировать и делать выводы В-ОПК-5 [1] – Владеть: теоретическими и эмпирическими методами научного исследования при выполнении научно-исследовательских работ, методикой оформления отчетов по научно-исследовательским работам, статей и тезисов докладов

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**
проектный			
разработка проектных решений по обеспечению безопасности данных с применением криптографических	информационные ресурсы	ПК-4.1 [1] - Способен разрабатывать проектные решения по обеспечению безопасности данных с применением	З-ПК-4.1[1] - Знать: методы обеспечения безопасности данных с применением криптографических методов;

методов		криптографических методов *Основание:* Профессиональный стандарт: 06.032	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
	2 Семестр						
1	Первый раздел	1-8	15/0/8		25	КИ-8	З-ОПК-5, У-ОПК-5, В-ОПК-5, З-ПК-4.1, У-ПК-4.1, В-ПК-4.1
2	Второй раздел	9-15	15/0/7		25	КИ-15	З-ОПК-5, У-ОПК-5,

							В-ОПК-5, З-ПК-4.1, У-ПК-4.1, В-ПК-4.1
	Итого за 2 Семестр		30/0/15		50		
	Контрольные мероприятия за 2 Семестр				50	З	З-ОПК-5, У-ОПК-5, В-ОПК-5, З-ПК-4.1, У-ПК-4.1, В-ПК-4.1
	3 Семестр						
1	Первый раздел	1-8			25	КИ-8	З-ОПК-5, У-ОПК-5, В-ОПК-5, З-ПК-4.1, У-ПК-4.1, В-ПК-4.1
2	Второй раздел	9-16			25	КИ-16	З-ОПК-5, У-ОПК-

							5, В-ОПК-5, З-ПК-4.1, У-ПК-4.1, В-ПК-4.1
	Итого за 3 Семестр		32/0/16		50		
	Контрольные мероприятия за 3 Семестр				50	Э	З-ОПК-5, У-ОПК-5, В-ОПК-5, 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
Э	Экзамен

КАЛЕНДАРНЫЙ ПЛАН

Недели	**Темы занятий / Содержание**	**Лек., час.**	**Пр./сем., час.**	**Лаб., час.**
	2 Семестр	30	0	15
1-8	**Первый раздел**	15	0	8
	1	Всего аудиторных часов		
	1	15		8

		Онлайн		
9-15	**Второй раздел**	15	0	7
	2 2	Всего аудиторных часов		
		15		7
		Онлайн		
	3 Семестр	32	0	16
1-8	**Первый раздел**	16		8
1 - 8	**1** 1	Всего аудиторных часов		
		16		8
		Онлайн		
9-16	**Второй раздел**	16		8
9 - 15	**2** 2	Всего аудиторных часов		
		16		8
		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

Решёточные и рюкзачные алгоритмы в пост-квантовой криптографии

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)**	**Аттестационное мероприятие (КП 2)**
ОПК-5	З-ОПК-5	З, КИ-8, КИ-15	Э, КИ-8, КИ-16
	У-ОПК-5	З, КИ-8, КИ-15	Э, КИ-8, КИ-16

	В-ОПК-5	З, КИ-8, КИ-15	Э, КИ-8, КИ-16
ПК-4.1	З-ПК-4.1	З, КИ-8, КИ-15	Э, КИ-8, КИ-16
	У-ПК-4.1	З, КИ-8, КИ-15	Э, КИ-8, КИ-16
	В-ПК-4.1	З, КИ-8, КИ-15	Э, 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. 004 М 21 Комментарии к Доктрине информационной безопасности Российской Федерации. : , 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/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Специальное материально-техническое обеспечение не требуется

9. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ

Решёточные и рюкзачные алгоритмы в пост-квантовой криптографии

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

приложены

Автор(ы):

Куприяшин Михаил Андреевич