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

СИММЕТРИЧНЫЕ КРИПТОСИСТЕМЫ

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
1	4	144	32	0	32		44	0	Э
Итого	4	144	32	0	32	0	44	0	

Москва, 2020

АННОТАЦИЯ

Курс охватывает следующие темы – совершенная стойкость и поточные шифры, блочные шифры, обеспечение целостности сообщений, аутентифицированное шифрование. Для сдачи каждого раздела студенту необходимо сдача всех лабораторных работ данного раздела и защита домашней работы.

Особенностью лекционного материала является использование строгих математических моделей при описании криптографических примитивов, а также демонстрация принципов доказательства теоретической стойкости с использованием игровой модели Белларе – Рогавея.

Каждый раздел лекций построен по следующему принципу – математическое описание объекта криптосистемы, математическая модель нарушителя, понятие теоретической и практической стойкости модели, использование модели при построении примитивов, существующие криптографические примитивы, описываемые данной моделью.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Цель дисциплины – изучение современных подходов доказательной криптографии при анализе и построении криптографических схем.

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
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 методов	информационные ресурсы	ПК-1 [1] - Способен принимать участие в разработке систем обеспечения ИБ или информационно-аналитических систем безопасности *Основание:* Профессиональный стандарт: 06.032	З-ПК-1[1] - Знать: модели угроз нсд к сетям электросвязи; методики оценки уязвимостей сетей электросвязи с точки зрения возможности нсд к ним; нормативные правовые акты в области связи, информатизации и защиты информации; виды политик безопасности компьютерных систем и сетей; возможности используемых и планируемых к использованию средств защиты информации; особенности защиты информации в автоматизированных системах управления технологическими процессами; критерии оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем; основные характеристики технических средств защиты информации от утечек по техническим каналам; нормативные правовые акты, методические документы, национальные

			стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации; технические каналы утечки информации. ; У-ПК-1[1] - Уметь: выявлять и оценивать угрозы нсд к сетям электросвязи; анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия; классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; выбирать меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы; проводить анализ угроз безопасности информации на объекте информатизации; проводить предпроектное обследование объекта информатизации. ; В-ПК-1[1] - Владеть: основами проведения технических работ при аттестации сссэ с учетом требований по защите информации; определением угроз безопасности информации, реализация которых может привести к нарушению

			безопасности информации в компьютерной системе и сети; основами разработки модели угроз безопасности информации и модели нарушителя в автоматизированных системах; основами предпроектного обследования объекта информатизации; основами разработки аналитического обоснования необходимости создания системы защиты информации на объекте информатизации (модели угроз безопасности информации).
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
	1 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 1 Семестр		32/0/32		50		
	Контрольные мероприятия за 1 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
Э	Экзамен

КАЛЕНДАРНЫЙ ПЛАН

Недели	**Темы занятий / Содержание**	**Лек., час.**	**Пр./сем., час.**	**Лаб., час.**
	1 Семестр	32	0	32
1-8	**Первый раздел**	16		16
1 - 2	**Основные понятия доказательной криптографии** Введение, принципы современной криптографии, понятие стойкости, Шифр Шеннона, абсолютная стойкость, вычислимые шифры, семантическая стойкость, пренебрежимо малые величины, параметры стойкости и системные параметры, понятие игры, модель эффективного противника.	Всего аудиторных часов		
		4		4
		Онлайн		
3 - 4	**Псевдослучайные генераторы** Псевдослучайные генераторы – определение и формальная модель, шифрование с использованием псевдослучайных генераторов, ограничения псевдослучайных генераторов, композиция псевдослучайных генераторов.	Всего аудиторных часов		
		4		4
		Онлайн		
5 - 6	**Поточные шифры** Тест на определение следующего бита псевдослучайного генератора, псевдослучайный генератор Salsa и ChaCha, линейные генераторы, псевдослучайный генератор CSS, Способы генерации случайных последовательностей.	Всего аудиторных часов		
		4		4
		Онлайн		
7 - 8	**Блочные шифры** Блочные шифры – определение и формальная модель, блочные шифры DES, AES, Магма, Кузнечик, псевдослучайные функции – определение и формальная модель, псевдослучайные функции как модель блочных шифров, построение псевдослучайных функций на основе	Всего аудиторных часов		
		4		4
		Онлайн		

	псевдослучайных генераторов, стойкость при множественном использовании ключа, атаки по произвольному множеству открытых и шифрованных текстов – определение и формальная модель, построение схем стойких к атакам по произвольному множеству открытых и шифрованных текстов, режим CTR, режим CBC, дополнение в режиме CBC и возможные атаки на него.			
9-16	**Второй раздел**	16		16
9 - 12	**Коды аутентичности сообщений** Коды аутентичности сообщений – определение и формальная модель; Построение кодов аутентичности на основе псевдослучайных функций Коды аутентичности CBC MAC, CMAC, PMAC.	Всего аудиторных часов		
		4		4
		Онлайн		
13 - 14	**Хэш-функции** Коды аутентичности Картера – Вагмена, стойкие к коллизиям хэш-функции – определение и формальная модель, построение кодов аутентичности сообщений на основе хэш-функций, парадокс дней рождений, построение функций сжатия, функции сжатия Девиса – Мейера, хэш-функция SHA 256, стойкость функции сжатия Девиса – Мейера, губчатая конструкция, SHA3, деревья Меркла, формирование симметричных ключей, модель Случайного Оракула, стойкость при существовании коллизий.	Всего аудиторных часов		
		8		8
		Онлайн		
15 - 16	**Аутентифицированное шифрование** Аутентифицированное шифрование – определение и формальная модель, шифрование как абстрактный интерфейс, базовые конструкции аутентифицированного шифрования, режим шифрования GCM, Протокол TLS 1.3, атака на протокол SSH, атака на протокол WEP, протокол IPSec, оракулы дополнений и атаки по времени.	Всего аудиторных часов		
		4		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)**
ОПК-5	З-ОПК-5	Э, КИ-8, КИ-16
	У-ОПК-5	Э, КИ-8, КИ-16
	В-ОПК-5	Э, КИ-8, КИ-16
ПК-4.1	З-ПК-4.1	Э, КИ-8, КИ-16
	У-ПК-4.1	Э, КИ-8, КИ-16
	В-ПК-4.1	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 –		Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает
60-64		E	

			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.

Оценочные средства приведены в Приложении.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. ЭИ М 29 Алгебра и теория чисел для криптографии : учебное пособие, Санкт-Петербург: Лань, 2020

2. ЭИ Ф 76 Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : Учебник для вузов, Москва: Юрайт, 2021

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):

Когос Константин Григорьевич, к.т.н.