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 № 8/1/2024

от 28.08.2024 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	30		12	0	З
3	3	108	32	0	32		8	0	Э
Итого	5	180	62	0	62	0	20	0	

АННОТАЦИЯ

Дисциплина призвана дать представление слушателям об основных задачах, решаемых с использованием криптографии, актуальных методах синтеза и анализа криптографических механизмов, среди которых алгоритмы блочного шифрования, функции хэширования, схемы подписи и протоколы выработки общего ключа. Представлены перспективные методы синтеза криптографических механизмов, стойких к атакам с использованием квантового компьютера (постквантовых криптографических механизмов), среди которых теория решеток, коды исправляющие ошибки, многочлены от многих переменных, итеративное использование функций хэширования. Знание основных принципов лежащих в основе синтеза и анализа как классических, так и постквантовых криптографических механизмов является ключевым элементом при разработке квантовых вычислителей предназначенных для решения задач криптографического анализа.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Дисциплина призвана дать представление слушателям об основных задачах, решаемых с использованием криптографии, актуальных методах синтеза и анализа криптографических механизмов, среди которых алгоритмы блочного шифрования, функции хэширования, схемы подписи и протоколы выработки общего ключа. Представлены перспективные методы синтеза криптографических механизмов, стойких к атакам с использованием квантового компьютера (постквантовых криптографических механизмов), среди которых теория решеток, коды исправляющие ошибки, многочлены от многих переменных, итеративное использование функций хэширования. Знание основных принципов лежащих в основе синтеза и анализа как классических, так и постквантовых криптографических механизмов является ключевым элементом при разработке квантовых вычислителей предназначенных для решения задач криптографического анализа.

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; Основание (профессиональный**	**Код и наименование индикатора достижения профессиональной компетенции**

		стандарт-ПС, анализ опыта)	
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
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).

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	15/0/15		25	КИ-8	З-ПК-4.1, У-ПК-4.1, В-ПК-4.1, З-ПК-1, У-ПК-1, В-ПК-1
2	Второй раздел	9-15	15/0/15		25	КИ-15	З-ПК-4.1, У-ПК-4.1, В-ПК-4.1, З-ПК-1, У-ПК-1, В-ПК-1
	Итого за 2 Семестр		30/0/30		50		
	Контрольные мероприятия за 2 Семестр				50	З	З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-4.1, У-ПК-4.1, В-ПК-4.1
	3 Семестр						
1	Первый раздел	1-8	16/0/16		25	КИ-8	З-ПК-4.1, У-ПК-4.1, В-ПК-4.1, З-ПК-1, У-ПК-1, В-ПК-1
2	Второй раздел	9-16	16/0/16		25	КИ-16	З-ПК-4.1, У-ПК-4.1, В-ПК-4.1, З-ПК-1, У-ПК-1, В-ПК-1
	Итого за 3 Семестр		32/0/32		50		
	Контрольные мероприятия за 3 Семестр				50	Э	З-ПК-1, У-ПК-1, В-ПК-1, 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	30
1-8	**Первый раздел**	15	0	15
	Основные синтезные принципы криптографических механизмов Блочные шифры. Методы синтеза раундовых преобразований блочных шифров. Сети Фейстеля, SPсети, XSL схемы. Режимы работы блочных шифров, их криптографические и эксплуатационно-технические свойства. Бесключевые и ключевые функции хэширования. Итеративные способы построения хэш-функций. Криптография с открытым ключом. Связь асимметричных систем с математическими проблемами (факторизация, дискретное логарифмирование). Схемы цифровой подписи RSA, Эль-Гамаля, Шнорра. Протоколы открытого распределения ключей	Всего аудиторных часов 15 Онлайн 0	0 0	15 0
9-15	**Второй раздел**	15	0	15
	Общие методы анализа криптографических механизмов Методы анализа блочных шифров. S-блоки и их свойства. Криптографический анализ режимов работы шифра. Режимы работы блочных шифров их криптографические и эксплуатационно-технические свойства. Общие методы анализа функции хэширования. Анализ схемы цифровой подписи и протоколов открытого распределения ключей. Методы анализа, основанные на поиске коллизий для используемых функций хэшировани и на решении базовых теоретикосложностных задач.	Всего аудиторных часов 15 Онлайн 0	0 0	15 0
	3 Семестр	32	0	32
1-8	**Первый раздел**	16	0	16
	Подходы к использованию квантового компьютера при построении методов анализа Особенности применения квантового компьютера при анализе криптографических механизмов Алгоритм Гровера. Применение алгоритма при анализе блочных шифров и функций хэширования. Алгоритм Саймона. Применение протокола при анализе функций хэширования. Алгоритм Шора. Применение алгоритма и его модификаций при анализе схем цифровой подписи	Всего аудиторных часов 16 Онлайн 0	0 0	16 0
9-16	**Второй раздел**	16	0	16
	Подходы к построению постквантовых криптографических механизмов О возможности использования методов классической криптографии при построении посквантовых криптографических механизмов. Методы, основанные на использовании теории решеток. Методы, основанные на использовании многочленов от	Всего аудиторных часов 16 Онлайн 0	0 0	16 0

	многих переменных. Методы, основанные на использовании теории кодов. Методы, основанные на итеративном использовании функций хэширования			

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

ТЕМЫ ЛАБОРАТОРНЫХ РАБОТ

Недели	**Темы занятий / Содержание**
	2 Семестр
	Л/Р 1 Итеративные способы построения хэш-функций
	Л/Р 2 Протоколы открытого распределения ключей
	Л/Р 2 Режимы работы блочных шифров их криптографические и эксплуатационно-технические свойства
	Л/Р 4 Общие методы анализа функции хэширования
	3 Семестр
	Л/Р 1 Алгоритм Гровера
	Л/Р 2 Алгоритм Шора
	Л/Р 3 Методы, основанные на использовании теории решеток
	Л/Р 4 Методы, основанные на использовании теории кодов

5. 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.

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)**
ПК-1	З-ПК-1	З, КИ-8, КИ-15	Э, КИ-8, КИ-16
	У-ПК-1	З, КИ-8, КИ-15	Э, КИ-8, КИ-16
	В-ПК-1	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:

<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 –</td><td>F</td><td>Оценка «неудовлетворительно»</td></tr>
</table>

	«*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.

7. 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/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Специальное материально-техническое обеспечение не требуется

9. 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.

10. 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):

Куприяшин Михаил Андреевич