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

ПРИКЛАДНАЯ КРИПТОГРАФИЯ

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	3	108	30	0	60		18	0	З
3	3	108	32	0	32		8	0	Э
Итого	6	216	62	0	92	0	26	0	

АННОТАЦИЯ

Цель дисциплины – изучение наиболее важных классов криптографических протоколов для решения прикладных задач обеспечения безопасности информации.

В курсе рассматриваются следующие темы:

- основы теории и практики конструирования криптографических протоколов,
- основы интерактивных и неинтерактивных вероятностных доказательств, доказательств с нулевым разглашением,
- протоколы аутентификации,
- основы управления ключами и протоколы распределения ключей,
- протоколы образования защищенных каналов передачи данных.

В рамках лабораторного практикума студенты получают навыки программирования криптографических протоколов с использованием специализированных библиотек криптографических функций.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Цель дисциплины – изучение наиболее важных классов криптографических протоколов для решения прикладных задач обеспечения безопасности информации.

В курсе рассматриваются следующие темы:

- основы теории и практики конструирования криптографических протоколов,
- основы интерактивных и неинтерактивных вероятностных доказательств, доказательств с нулевым разглашением,
- протоколы аутентификации,
- основы управления ключами и протоколы распределения ключей,
- протоколы образования защищенных каналов передачи данных.

В рамках лабораторного практикума студенты получают навыки программирования криптографических протоколов с использованием специализированных библиотек криптографических функций.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Учебная дисциплина является обязательной

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**
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
научно-исследовательский			
выполнение научно-исследовательских работ по развитию физических, математических или технических методов обеспечения безопасности данных	методы обеспечения безопасности данных	ПК-3 [1] - Способен 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	З-ПК-3[1] - Знать: 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.

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	16/0/30		25	КИ-8	З-ПК-4.1, У-ПК-4.1, В-ПК-4.1, З-ПК-3,

							У-ПК-3, В-ПК-3
2	Второй раздел	9-15	14/0/30		25	КИ-15	З-ПК-4.1, У-ПК-4.1, В-ПК-4.1, З-ПК-3, У-ПК-3, В-ПК-3
	Итого за 2 Семестр		30/0/60		50		
	Контрольные мероприятия за 2 Семестр				50	З	З-ПК-4.1, З-ПК-3, У-ПК-3, В-ПК-3, 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-3, У-ПК-3, В-ПК-3
2	Второй раздел	9-16	16/0/16		25	КИ-15	З-ПК-4.1, У-ПК-4.1, В-ПК-4.1, З-ПК-3, У-ПК-3, В-ПК-3
	Итого за 3 Семестр		32/0/32		50		
	Контрольные мероприятия за 3 Семестр				50	Э	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
Э	Экзамен

КАЛЕНДАРНЫЙ ПЛАН

Недели	**Темы занятий / Содержание**	**Лек., час.**	**Пр./сем., час.**	**Лаб., час.**

	2 Семестр	30	0	60
1-8	**Первый раздел**	16	0	30
1 - 3	**Введение. Теоретические и методические основы создания криптографических протоколов.** Понятие криптографического протокола. Свойства протоколов. Виды атак на протоколы. Принципы оценки стойкости протоколов. Криптографические примитивы и вычислительно сложные задачи.	Всего аудиторных часов		
		6	0	10
		Онлайн		
		0	0	0
4 - 6	**Вероятностные доказательства.** Классификация вероятностных доказательств. Интерактивные и неинтерактивные доказательства. Доказательства с нулевым разглашением. zk-SNARKs. Примеры систем доказательства. Основные сферы применения вероятностных доказательств.	Всего аудиторных часов		
		6	0	10
		Онлайн		
		0	0	0
7 - 8	**Протоколы аутентификации.** Задача аутентификации. Классификация протоколов аутентификации. Протоколы с фиксированными и одноразовыми паролями. Протоколы типа «запрос – ответ». Протоколы на основе доказательств с нулевым разглашением.	Всего аудиторных часов		
		4	0	10
		Онлайн		
		0	0	0
9-15	**Второй раздел**	14	0	30
	Защищенные каналы передачи данных. Постановка задачи. Способы обеспечения конфиденциальности и аутентичности информации в каналах связи. Требования к протоколам образования защищенных каналов передачи данных. Протокол TLS 1.3. Асинхронные протоколы. Механизм храповика, двойного храповика (double ratcheting). Протоколы Signal.	Всего аудиторных часов		
		5	0	10
		Онлайн		
		0	0	0
	Многосторонние криптографические протоколы. Протоколы распределения ключей конференц-связи. Схемы разделения секрета. Безопасные многосторонние вычисления	Всего аудиторных часов		
		4	0	10
		Онлайн		
		0	0	0
9 - 15	**Управление ключами. Протоколы распределения ключей.** Понятие жизненного цикла криптографических ключей. Стандарт ISO/IEC 11770. Принципы построения ключевых систем. Инфраструктура управления ключами (PKI/KMI). Типология протоколов распределения ключей (ПРК), их свойства. ПРК, основанные на симметричных криптосистемах. Централизованные и децентрализованные протоколы. ПРК, основанные на асимметричных криптосистемах. Протоколы обмена	Всего аудиторных часов		
		5	0	10
		Онлайн		
		0	0	0

	ключами.			
	3 Семестр	32	0	32
1-8	**Первый раздел**	16	0	16
1 - 3	**Доказательства с нулевым разглашением.** Программная реализация протоколов доказательства с нулевым разглашением Фиата – Шамира, Гиллу – Кискатра, Шнорра на языке высокого уровня с использованием функций библиотек.	Всего аудиторных часов		
		6	0	6
		Онлайн		
		0	0	0
4 - 6	**Протоколы удаленной аутентификации.** Программная реализация протоколов аутентификации PAP, CHAP, S/KEY на языке высокого уровня с использованием функций библиотек.	Всего аудиторных часов		
		6	0	6
		Онлайн		
		0	0	0
7 - 8	**Протоколы транспортировки ключей** Программная реализация одного протоколов транспортировки ключей Needham – Schroeder, Otway – Rees, Kerberos на языке высокого уровня с использованием функций библиотек.	Всего аудиторных часов		
		4	0	4
		Онлайн		
		0	0	0
9-16	**Второй раздел**	16	0	16
	Схемы разделения секрета. Программная реализация схем разделения секрета Шамира и Миньотта, схем проверяемого разделения секрета Фельдмана и Педерсена на языке высокого уровня с использованием функций библиотек.	Всего аудиторных часов		
		0	0	0
		Онлайн		
		0	0	0
	Исследование гомоморфных свойств криптографических схем. Программная реализация схем открытого шифрования, обладающих свойством гомоморфизма по одной из алгебраических операций: схемы Эль-Гамаля, схемы RSA, схемы Пайе. Наблюдение явлений гомоморфизма при шифровании текстов.	Всего аудиторных часов		
		0	0	0
		Онлайн		
		0	0	0
	Гибридное шифрование. Гибридное шифрование. Аутентифицированное шифрование. Реализация схем гибридного шифрования с использованием блочных шифров в режимах CBC, OFB, CFB и в режимах аутентифицированного шифрования CCM, OCB, GCM.	Всего аудиторных часов		
		0	0	0
		Онлайн		
		0	0	0
9 - 16	**Протоколы обмена ключами.** Программная реализация протоколов X3DH, MTI, STS на языке высокого уровня с использованием функций	Всего аудиторных часов		
		16	0	16
		Онлайн		
		0	0	0

	библиотек.			

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 Вероятностные доказательства.
	Л/Р 2 Протоколы аутентификации.
	Л/Р 3 Защищенные каналы передачи данных.
	Л/Р 4 Многосторонние криптографические протоколы.
	3 Семестр
	Л/Р 1 Протоколы удаленной аутентификации.
	Л/Р 2 Протоколы транспортировки ключей
	Л/Р 3 Схемы разделения секрета.
	Л/Р 4 Гибридное шифрование.

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, работа с компьютерными программами.

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-3	З-ПК-3	З, КИ-8, КИ-15	Э, КИ-8, КИ-15
	У-ПК-3	З, КИ-8, КИ-15	Э, КИ-8, КИ-15
	В-ПК-3	З, КИ-8, КИ-15	Э, КИ-8, КИ-15
ПК-4.1	З-ПК-4.1	З, КИ-8, КИ-15	Э, КИ-8, КИ-15
	У-ПК-4.1	З, КИ-8, КИ-15	Э, КИ-8, КИ-15
	В-ПК-4.1	З, КИ-8, КИ-15	Э, КИ-8, КИ-15

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.

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):

Запечников Сергей Владимирович, д.т.н., доцент