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 ИФТЭБ Протокол №545-2/1 от 28.08.2024 г.
УМС ИИКС Протокол №8/1/2025 от 25.08.2025 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Направление подготовки (специальность)
[1] 10.03.01 Информационная безопасность
[2] 09.03.01 Информатика и вычислительная техника

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	4-5	144-180	60	0	15		15-60	0	Э
Итого	4-5	144-180	60	0	15	0	15-60	0	

АННОТАЦИЯ

Цель дисциплины – формирование у студентов знаний о современных криптографических методах защиты и особенностях их применения при комплексной защите объектов информатизации.

В курсе рассматриваются следующие темы:

- основные понятия и задачи криптологии;
- основные типы криптографических алгоритмов с секретным и открытым ключом;
- основные методы построения и оценки качества протоколов на основе криптосистем с секретным и открытым ключом.
- типовые методы криптографического анализа и оценивания криптографической стойкости;
- проблемы и методы управления ключевым материалом криптосистем;
- принятые отечественные, зарубежные и международные стандарты для средств криптографической защиты информации и рекомендации по их использованию;
- тенденции развития и основных направлений исследований в области криптологии;
- вопросы лицензирования и сертификации средств криптографической защиты информации;
- параметры безопасности для основных используемых на практике типов криптосистем;

Знания и практические навыки, полученные в курсе, используются при изучении других дисциплин профессионального цикла, а также при выполнении курсовых и дипломных работ.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Цель дисциплины – формирование у студентов знаний о современных криптографических методах защиты и особенностях их применения при комплексной защите объектов информатизации.

В курсе рассматриваются следующие темы:

- основные понятия и задачи криптологии;
- основные типы криптографических алгоритмов с секретным и открытым ключом;
- основные методы построения и оценки качества протоколов на основе криптосистем с секретным и открытым ключом.
- типовые методы криптографического анализа и оценивания криптографической стойкости;
- проблемы и методы управления ключевым материалом криптосистем;
- принятые отечественные, зарубежные и международные стандарты для средств криптографической защиты информации и рекомендации по их использованию;
- тенденции развития и основных направлений исследований в области криптологии;
- вопросы лицензирования и сертификации средств криптографической защиты информации;
- параметры безопасности для основных используемых на практике типов криптосистем;

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Знания и практические навыки, полученные в курсе, используются при изучении других дисциплин профессионального цикла, а также при выполнении курсовых и дипломных работ.

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
ОПК-2 [1] – Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	З-ОПК-2 [1] – знать программные средства системного и прикладного назначения, информационно-коммуникационные технологии для решения профессиональных задач У-ОПК-2 [1] – уметь применять программные средства системного и прикладного назначения, информационно-коммуникационные технологии для решения профессиональных задач В-ОПК-2 [1] – владеть принципами работы программных средств системного и прикладного назначения, информационно-коммуникационных технологий для решения профессиональных задач
ОПК-4 [1] – Способен применять необходимые физические законы и модели для решения задач профессиональной деятельности	З-ОПК-4 [1] – знать основные черты современной естественнонаучной картины мира и физические основы функционирования средств защиты информации У-ОПК-4 [1] – уметь объяснять физические принципы функционирования средств защиты информации В-ОПК-4 [1] – владеть основными принципами функционирования средств защиты информации
ОПК-7 [2] – Способен участвовать в настройке и наладке программно-аппаратных комплексов	З-ОПК-7 [2] – Знать: методы настройки, наладки программно-аппаратных комплексов, методы и средства проверки работоспособности компьютерного программного обеспечения, государственные стандарты испытания автоматизированных систем, руководящие документы по стандартизации требований к документам автоматизированных систем. У-ОПК-7 [2] – Уметь: анализировать техническую документацию, производить настройку, наладку и тестирование программно-аппаратных комплексов, применять методы и средства проверки работоспособности компьютерного программного обеспечения, интерпретировать диагностические данные проверки работоспособности компьютерного программного обеспечения, анализировать значения полученных характеристик компьютерного программного обеспечения. В-ОПК-7 [2] – Владеть: навыками проверки работоспособности программно-аппаратных комплексов

ОПК-9 [1] – Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	З-ОПК-9 [1] – знать характеристики и особенности основных средств криптографической и технической защиты информации, применяемых для решения задач профессиональной деятельности У-ОПК-9 [1] – уметь применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности В-ОПК-9 [1] – владеть методиками применения средств криптографической и технической защиты информации
ОПК-9 [2] – Способен осваивать методики использования программных средств для решения практических задач	З-ОПК-9 [2] – Знать: классификацию программных средств и возможности их применения для решения практических задач У-ОПК-9 [2] – Уметь: находить и анализировать техническую документацию по использованию программного средства, выбирать и использовать необходимые функции программных средств для решения конкретной задачи В-ОПК-9 [2] – Владеть: способами описания методики использования программного средства для решения конкретной задачи в виде документа, презентации или видеоролика
ОПК-10 [1] – Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	З-ОПК-10 [1] – знать способы создания политики информационной безопасности организации и комплекс мер по обеспечению информационной безопасности У-ОПК-10 [1] – уметь формировать политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты В-ОПК-10 [1] – владеть принципами формирования политики информационной безопасности организации

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	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

	информационных систем и сетей передачи данных; соблюдать конфиденциальность доверенной информации (В40)	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	30/0/8		25	КИ-8	З-ОПК-2, У-ОПК-2, В-ОПК-2
2	Второй раздел	9-15	30/0/7		25	КИ-15	З-ОПК-9, У-ОПК-9, В-ОПК-9, З-ОПК-10, У-ОПК-10, В-ОПК-10
	Итого за 6 Семестр		60/0/15		50		
	Контрольные мероприятия за 6 Семестр				50	Э	З-ОПК-2, У-ОПК-2, В-ОПК-2, З-ОПК-4, У-ОПК-4, В-ОПК-4, З-ОПК-7, У-ОПК-7, В-ОПК-7, З-ОПК-9, У-ОПК-9, В-ОПК-9, З-ОПК-9, У-ОПК-9, В-ОПК-9, З-ОПК-10, У-ОПК-10, В-ОПК-10

* – 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.
	6 Семестр	60	0	15
1-8	**Первый раздел**	30	0	8
1 - 8	**Раздел 1** Введение. Основные понятия и определения. Примитивы и протоколы. Регулирование. Обеспечение секретности. Понятие о шифрах. Теория информации и криптография. Совершенная стойкость. Криптографические генераторы случайных и псевдослучайных последовательностей. Поточные шифры. Симметричные блочные шифры.	Всего аудиторных часов		
		30	0	8
		Онлайн		
		0	0	0
9-15	**Второй раздел**	30	0	7
9 - 15	**Раздел 2** Основные понятия криптографии с открытым ключом. Основные понятия управления ключами Вопросы стандартизации и патентования.	Всего аудиторных часов		
		30	0	7
		Онлайн		
		0	0	0

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
	6 Семестр
	Л/Р 1 Совершенная стойкость шифров по Шеннону
	Л/Р 2 Управление ключами криптосистем
	Л/Р 3

	Криптографические свойства S- блоков
	Л/Р 4 Разделение секрета

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**	**Аттестационное мероприятие (КП 1)**
ОПК-10	З-ОПК-10	Э, КИ-15
	У-ОПК-10	Э, КИ-15
	В-ОПК-10	Э, КИ-15
ОПК-2	З-ОПК-2	Э, КИ-8
	У-ОПК-2	Э, КИ-8
	В-ОПК-2	Э, КИ-8
ОПК-4	З-ОПК-4	Э
	У-ОПК-4	Э
	В-ОПК-4	Э
ОПК-9	З-ОПК-9	Э, КИ-15
	У-ОПК-9	Э, КИ-15
	В-ОПК-9	Э, КИ-15
ОПК-7	З-ОПК-7	Э
	У-ОПК-7	Э
	В-ОПК-7	Э
ОПК-9	З-ОПК-9	Э
	У-ОПК-9	Э
	В-ОПК-9	Э

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.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. ЭИ Н 62 Методы защиты информации. Шифрование данных : учебное пособие, Никифоров С. Н., Санкт-Петербург: Лань, 2022

2. ЭИ Н 56 Основы информационной безопасности : учебное пособие, Нестеров С. А., Санкт-Петербург: Лань, 2021

3. ЭИ А 28 Основы классической криптологии: секреты шифров и кодов : , Адаменко М. В., Москва: ДМК Пресс, 2016

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

1. 004 П 30 Основы практической защиты информации : учеб. пособие, Петраков А.В., Москва: РадиоСофт, 2018

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

Специальное программное обеспечение не требуется

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

https://online.mephi.ru/

http://library.mephi.ru/

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Специальное материально-техническое обеспечение не требуется

10. 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.

11. 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):

Варфоломеев Александр Алексеевич, к.ф.-м.н., с.н.с.