Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский ядерный университет «МИФИ»

ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ

КАФЕДРА КОМПЬЮТЕРНЫХ СИСТЕМ И ТЕХНОЛОГИЙ

ОДОБРЕНО УМС ИФТЭБ

Протокол № 545-2/1

от 28.08.2024 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Направление подготовки (специальность) — [1] 10.05.04 Информационно-аналитические системы безопасности

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	5	180	30	15	15		66	0	Э
Итого	5	180	30	15	15	0	66	0	

АННОТАЦИЯ

Формирование принципов построения защищенных компьютерных систем, в том числе критически важных (ядерная энергетика, оборона, космос) компьютерных систем.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью освоения учебной дисциплины являются изучение принципов построения защищенных компьютерных систем, в том числе критически важных (ядерная энергетика, оборона, космос) компьютерных систем.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Для успешного освоения дисциплины Криптографические методы защиты информации необходимы компетенции, формируемые в результате освоения следующих дисциплин:

Информатика и основы программирования;

ЭВМ и периферийные устройства.

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
ОПК-1 [1] – Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	З-ОПК-1 [1] – знать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства У-ОПК-1 [1] – уметь определять роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства В-ОПК-1 [1] – владеть основными методами оценки информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства
ОПК-6 [1] – Способен при решении профессиональных задач проверять выполнение требований защиты информации ограниченного доступа в информационно-аналитических системах в соответствии с нормативными правовыми актами	З-ОПК-6 [1] – знать нормативные правовые акты, нормативные и методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю необходимые при решении задач профессиональной деятельности У-ОПК-6 [1] – уметь организовать защиту информации ограниченного доступа в автоматизированных системах в

и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю при решении задач профессиональной деятельности В-ОПК-6 [1] – владеть принципами организации защиты информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю при решении задач профессиональной деятельности
ОПК-7 [1] – Способен создавать программы на языках высокого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования	З-ОПК-7 [1] – знать языки программирования высокого и низкого уровня, инструментальные средства программирования для решения профессиональных задач У-ОПК-7 [1] – уметь создавать программы на языках высокого и низкого уровня, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ В-ОПК-7 [1] – владеть методами и инструментальными средствами программирования для решения профессиональных задач
ОПК-9 [1] – Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	З-ОПК-9 [1] – знать текущее состояние и тенденции развития методов криптографической защиты информации при решении задач профессиональной деятельности У-ОПК-9 [1] – уметь анализировать и учитывать текущее состояние и тенденции развития методов криптографической защиты информации при решении задач профессиональной деятельности В-ОПК-9 [1] – владеть методами анализа текущего состояния и тенденции развития методов криптографической защиты информации при решении задач профессиональной деятельности
ОПК-11 [1] – Способен осуществлять синтез технологий и основных компонентов функциональной и обеспечивающей частей создаваемых информационно-аналитических систем, в том числе выбор мероприятий по защите информации	З-ОПК-11 [1] – знать принципы построения информационно-аналитических систем, механизмы управления доступом в данных системах, основные виды безопасности информационно-аналитической системы, угрозы безопасности и механизмы их устранения У-ОПК-11 [1] – уметь осуществлять синтез технологий и основных компонентов функциональной и обеспечивающей частей создаваемых информационно-аналитических систем, в том числе выбор мероприятий по защите информации В-ОПК-11 [1] – владеть навыками проведения

	обследования подразделений организации (учреждения, предприятия), постановки новых задач автоматизации и информатизации информационно-аналитической системы, в том числе в контексте обеспечения функционирования данной системы и ее частей, защиты информации, содержащейся в ней

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**
эксплуатационно-технологический			
Решение информационно-аналитических задач в сфере профессиональной деятельности с использованием специальных ИАС; эксплуатация специальных ИАС и средств обеспечения их информационной безопасности.	Специальные ИАС, обеспечивающие поддержку принятия решений в процессе организационного управления; модели, методы и методики информационно-аналитической деятельности в процессе организационного управления; системы государственного финансового мониторинга; системы финансового мониторинга в кредитных организациях; системы финансового мониторинга в некредитных организациях; системы финансового мониторинга в субъектах первичного финансового мониторинга.	ПК-12 [1] - Способен выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах *Основание:* Профессиональный стандарт: 06.032	З-ПК-12[1] - знать виды основных угроз информационной безопасности и модели нарушителя в компьютерных системах ; У-ПК-12[1] - уметь выявлять основные угрозы безопасности информации, строить и исследовать модели нарушителя в компьютерных системах; В-ПК-12[1] - владеть принципами и методами выявления угроз безопасности информации, принципами и методами построения, исследования моделей нарушителей

4. ВОСПИТАТЕЛЬНЫЙ ПОТЕНЦИАЛ ДИСЦИПЛИНЫ

Направления/цели воспитания	Задачи воспитания (код)	Воспитательный потенциал дисциплин
Профессиональное воспитание	Создание условий, обеспечивающих, формирование культуры информационной безопасности (В23)	Использование воспитательного потенциала дисциплин профессионального модуля для формирование базовых навыков информационной безопасности через изучение последствий халатного отношения к работе с информационными системами, базами данных (включая персональные данные), приемах и методах злоумышленников, потенциальном уроне пользователям.

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	Классическая криптография	1-8	16/8/8		25	КИ-8	З-ОПК-1, У-ОПК-1, В-ОПК-1, З-ОПК-6, У-ОПК-6, В-ОПК-6, З-ОПК-7, У-ОПК-7, В-ОПК-7, З-ОПК-9, У-ОПК-9, В-ОПК-9, З-ОПК-11, У-ОПК-11, В-ОПК-11, З-ПК-12, У-ПК-12, В-ПК-12
2	Современная	9-15	14/7/7		25	КИ-15	З-ОПК-1,

	криптография						У-ОПК-1, В-ОПК-1, З-ОПК-6, У-ОПК-6, В-ОПК-6, З-ОПК-7, У-ОПК-7, В-ОПК-7, З-ОПК-9, У-ОПК-9, В-ОПК-9, З-ОПК-11, У-ОПК-11, В-ОПК-11, З-ПК-12, У-ПК-12, В-ПК-12
	Итого за 6 Семестр		30/15/15		50		
	Контрольные мероприятия за 6 Семестр				50	Э	З-ОПК-1, У-ОПК-1, В-ОПК-1, З-ОПК-6, У-ОПК-6, В-ОПК-6, З-ОПК-7, У-ОПК-7, В-ОПК-7, З-ОПК-9, У-ОПК-9, В-ОПК-9, З-ОПК-11, У-ОПК-11, В-ОПК-11, З-ПК-12, У-ПК-12, В-ПК-12

* – 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	30	15	15
1-8	**Классическая криптография**	16	8	8
1	**Причины трудоемкости решения задач защиты информации** Информационно-психологическая война. Информационно-техническая война. Главные угрозы кибербезопасности. Источники угроз кибербезопасности. Политика коммерческих IT-компаний. Уязвимые IT-технологии. Сложность современных информационных систем. Все большее отстранение пользователей от реальных процессов управления и обработки информации. Человеческий фактор.	Всего аудиторных часов 2 Онлайн 0	1 0	1 0
2 - 3	**Особенности криптографии как науки** Процессный подход к решению задач защиты информации. Стохастические методы защиты информации Особенности криптографии как науки. Задачи, решаемые криптографическими методами. Стандарты криптографической защиты. Шифр Ф. Бэкона. Основные термины и определения. Правило Керхгофса. Требования к качественному шифру. Классификация шифров. Простейшие шифры	Всего аудиторных часов 4 Онлайн 0	2 0	2 0
4 - 8	**Криптосистемы с секретным ключом** Модель криптосистемы с секретным ключом. Совершенно секретный шифр. Гаммирование. Свойства гаммирования. Генераторы псевдослучайных чисел (ГПСЧ). Требования к качественному ГПСЧ. Блочные и поточные шифры. SP-сеть. Сеть Фейстеля. Основы дифференциального криптоанализа Американский стандарт криптозащиты. Российский стандартр криптозащиты. Архитектура Квадрат. XSL-шифры. Идея криптоалгоритма Кузнечик. Режимы использования блочных шифров. Поточные шифры A5, PIKE и RC4.	Всего аудиторных часов 10 Онлайн 0	5 0	5 0
9-15	**Современная криптография**	14	7	7
9 - 11	**Криптосистемы с открытым ключом** Модель криптосистемы с открытым ключом. Односторонняя функция, односторонняя функция с секретом. Атака Man-in-the-Middle Криптосистема RSA. Пример работы криптосистемы RSA. Ранцевая криптосистема. Примеры работы ранцевой криптосистемы.	Всего аудиторных часов 6 Онлайн 0	3 0	3 0
12 - 14	**Криптографические протоколы** Протокол выработки общего секретного ключа Диффи-Хеллмана. Протокол классической электронной подписи. Протокол подбрасывания монеты. Протокол разделения секрета. Симметричные и асимметричные протоколы аутентификации удаленных абонентов. Схема Kerberos Цифровые деньги. Задачи защиты информации, требующие решения в электронных платежных системах (ЭПС) на основе цифровых денег. Слепая электронная	Всего аудиторных часов 6 Онлайн 0	3 0	3 0

	подпись RSA. Прикладные протоколы электронной платежной системы на основе цифровых денег.			
15	**Аппаратно-программные методы защиты информации** Поле Галуа GF(pn). Структура конечного поля. Примитивный элемент. Генератор ненулевых элементов поля. Примеры конечных полей. Расширение конечных полей	Всего аудиторных часов		
		2	1	1
		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
2	**Простейшие шифры** Простейшие шифры
4	**Построение дифференциального пути двухраундовой SP-сети** Построение дифференциального пути двухраундовой SP-сети
6	**Поточные режимы блочного шифрования** Поточные режимы блочного шифрования
8	**Поточный шифр RC4** Поточный шифр RC4
10	**Криптосистема RSA** Криптосистема RSA
12	**Ранцевая криптосистема** Ранцевая криптосистема
14	**Криптографические протоколы** Криптографические протоколы
16	**Криптографические протоколы** Криптографические протоколы

6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

При чтении лекционного материала используется электронное сопровождение курса: справочно-иллюстративный материал воспроизводится и озвучивается в аудитории с использованием проектора и переносного компьютера в реальном времени. Электронный материал доступен студентам для использования и самостоятельного изучения на сайте кафедры.

На сайте кафедры также находится методический и справочный материал, необходимый для проведения лабораторного практикума по курсу.

Лабораторный практикум проводится по расписанию в дисплейном классе одновременно для группы студентов, работающих в интерактивном режиме. Допустимо выполнение лабораторных работ в составе локальной сети кафедры или в удаленном режиме, используя Интернет.

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-1	З-ОПК-1	Э, КИ-8, КИ-15
	У-ОПК-1	Э, КИ-8, КИ-15
	В-ОПК-1	Э, КИ-8, КИ-15
ОПК-11	З-ОПК-11	Э, КИ-8, КИ-15
	У-ОПК-11	Э, КИ-8, КИ-15
	В-ОПК-11	Э, КИ-8, КИ-15
ОПК-6	З-ОПК-6	Э, КИ-8, КИ-15
	У-ОПК-6	Э, КИ-8, КИ-15
	В-ОПК-6	Э, КИ-8, КИ-15
ОПК-7	З-ОПК-7	Э, КИ-8, КИ-15
	У-ОПК-7	Э, КИ-8, КИ-15
	В-ОПК-7	Э, КИ-8, КИ-15
ОПК-9	З-ОПК-9	Э, КИ-8, КИ-15
	У-ОПК-9	Э, КИ-8, КИ-15
	В-ОПК-9	Э, КИ-8, КИ-15
ПК-12	З-ПК-12	Э, КИ-8, КИ-15
	У-ПК-12	Э, КИ-8, КИ-15
	В-ПК-12	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.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. ЭИ Г 55 Введение в теоретико-числовые методы криптографии : , Круглов И. А. [и др.], Санкт-Петербург: Лань, 2022

2. ЭИ И 20 Генераторы псевдослучайных чисел на регистрах сдвига с линейными и нелинейными обратными связями : Учебное пособие, Саликов Е.А., Иванов М.А., Москва: НИЯУ МИФИ, 2021

3. ЭИ И20 Криптографические методы защиты информации в компьютерных системах и сетях : учебное пособие для вузов, Иванов М.А., Чугунков И.В., Москва: НИЯУ МИФИ, 2012

4. ЭИ Р17 Разрушающие программные воздействия : учебно-методическое пособие для вузов, Шустова Л.И. [и др.], Москва: НИЯУ МИФИ, 2011

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

1. 519 С13 Введение в алгебраические коды : учебное пособие, Сагалович Ю.Л., Москва: ИППИ, 2010

2. 004 Ш76 Секреты и ложь : Безопасность данных в цифровом мире, Шнайер Б., М.и др.: Питер, 2003

3. 0 М24 Современная криптография : теория и практика, Мао В., Москва [и др.]: Вильямс, 2005

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

1. Указания для прослушивания лекций

Перед началом занятий ознакомиться с учебным планом и списком рекомендованной литературы.

Перед посещением очередной лекции освежить в памяти основные концепции пройденного ранее материала. Подготовить при необходимости вопросы преподавателю. На каждой лекции следует задавать вопросы как по материалу текущей лекции, так и по ранее прочитанным лекциям.

При изучении лекционного материала обязательно следует сопоставлять его с материалом семинарских и лабораторных занятий.

Для более подробного изучения курса следует работать с рекомендованными литературными источниками и материалами из сети Internet.

2. Указания для проведения лабораторного практикума.

Соблюдать требования техники безопасности, для чего прослушать необходимые разъяснения о правильности поведения в лаборатории.

Перед выполнением лабораторной работы провести самостоятельно подготовку к работе изучив основные теоретические положения, знание которых необходимо для осмысленного выполнения работы.

В процессе выполнения работы следует постоянно общаться с преподавателем, не допуская по возможности неправильных действий.

При сдаче зачета по работе подготовить отчет о проделанной работе, где должны быть отражены основные результаты и выводы.

3. Указания по выполнению самостоятельной работы

Получить у преподавателя задание и список рекомендованной литературы.

Изучение теоретических вопросов следует проводить по возможности самостоятельно, но при затруднениях обращаться к преподавателю.

При выполнении фронтальных заданий по усмотрению преподавателя работа может быть оценена без письменного отчета на основе ответов на контрольные вопросы, при условии активной самостоятельной работы.

11. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

1. Указания для проведения лекций

На первой вводной лекции сделать общий обзор содержания курса. Дать перечень рекомендованной основной литературы и вновь появившихся литературных источников.

Перед изложением текущего лекционного материала кратко напомнить об основных выводах по материалам предыдущей лекции.

Внимательно относиться к вопросам студентов и при необходимости давать дополнительные более подробные пояснения.

Периодически освещать на лекциях наиболее важные вопросы лабораторного практикума, вызывающие у студентов затруднения.

В середине семестра обязательно провести контроль знаний студентов по материалам всех прочитанных лекций.

Желательно использовать конспекты лекций, в которых используется принятая преподавателем система обозначений.

Давать рекомендации студентам для подготовки к очередным лабораторным работам.

На последней лекции уделить время для обзора наиболее важных положений, рассмотренных в курсе.

2. Указания для проведения лабораторного практикума

На первом занятии рассказать о лабораторном практикуме в целом, провести инструктаж по технике безопасности при работе в лаборатории.

Для выполнения каждой лабораторной работы студентам выдавать индивидуальные задания.

При принятии отчета по каждой лабораторной работе обязательно побеседовать с каждым студентом, задавая контрольные вопросы, направленные на понимание изучаемой в лабораторной работе проблемы.

По каждой работе фиксировать факт выполнения и ответа на контрольные вопросы.

Общий зачет по практикуму должен включать все зачеты по каждой лабораторной работе в отдельности.

Задания на каждую следующую лабораторную работу студенту выдавать по мере выполнения и сдачи предыдущих работ.

Автор(ы):

Иванов Михаил Александрович, д.т.н., профессор

Рецензент(ы):
Чугунков И.В.