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 ИИКС

Протокол № 4/1/2023

от 25.04.2023 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ЗАЩИТА ИНФОРМАЦИИ

Направление подготовки (специальность) — [1] 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
5	4	144	32	0	0		76	0	Э
Итого	4	144	32	0	0	0	76	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 Защита информации необходимы компетенции, формируемые в результате освоения следующих дисциплин:

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-2 [1] – Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности	З-ОПК-2 [1] – Знать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, используемых при решении задач профессиональной деятельности У-ОПК-2 [1] – Уметь выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности В-ОПК-2 [1] – Владеть навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности
ОПК-3 [1] – Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	З-ОПК-3 [1] – Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности У-ОПК-3 [1] – Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных

	технологий и с учетом основных требований информационной безопасности В-ОПК-3 [1] – Владеть: навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности
ОПК-8 [1] – Способен разрабатывать алгоритмы и программы, пригодные для практического применения	З-ОПК-8 [1] – Знать: алгоритмические языки программирования, операционные системы и оболочки, современные среды разработки программного обеспечения У-ОПК-8 [1] – Уметь: составлять алгоритмы, писать и отлаживать коды на языке программирования, тестировать работоспособность программы, интегрировать программные модули В-ОПК-8 [1] – Владеть: языком программирования; навыками отладки и тестирования работоспособности программы
ОПК-9 [1] – Способен осваивать методики использования программных средств для решения практических задач	З-ОПК-9 [1] – Знать: классификацию программных средств и возможности их применения для решения практических задач У-ОПК-9 [1] – Уметь: находить и анализировать техническую документацию по использованию программного средства, выбирать и использовать необходимые функции программных средств для решения конкретной задачи В-ОПК-9 [1] – Владеть: способами описания методики использования программного средства для решения конкретной задачи в виде документа, презентации или видеоролика

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**
научно-исследовательский и инновационный			
Изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования. Математическое	Вычислительные машины, комплексы, системы и сети; автоматизированные системы обработки информации и управления; системы автоматизированного	ПК-1 [1] - Способен обосновывать принимаемые проектные решения, осуществлять постановку и выполнять эксперименты по	З-ПК-1[1] - Знать: основы верификации и аттестации аппаратного и программного обеспечения, стандарты качества и процессов его

моделирование процессов и объектов на базе стандартных пакетов автоматизированного проектирования и исследований. Проведение экспериментов по заданной методике и анализ результатов. Проведение измерений и наблюдений, составление описания проводимых исследований, подготовка данных для составления обзоров, отчетов и научных публикаций. Составление отчета по выполненному заданию, участие во внедрении результатов исследований и разработок. Участие в составе коллектива исполнителей во внедрении результатов научно-технических исследований в высокотехнологичных сферах экономики и коммерциализации разработок.	проектирования и информационной поддержки жизненного цикла промышленных изделий; программное обеспечение средств вычислительной техники и автоматизированных систем (программы, программные комплексы и системы); математическое, информационное, техническое, лингвистическое, программное, эргономическое, организационное и правовое обеспечение перечисленных систем.	проверке их корректности и эффективности *Основание:* Профессиональный стандарт: 06.001	обеспечения, способы оптимизации, принципы и виды отладки, методы оценки качества, методики постановки экспериментов; У-ПК-1[1] - Уметь: разрабатывать и специфицировать требования, осуществлять составление описания проводимых исследований, подготовку данных для составления обзоров и отчетов, обосновывать принимаемые проектные решения, выполнять эксперименты по проверке корректности решений; В-ПК-1[1] - Владеть: навыками построения моделей объектов профессиональной деятельности с использованием инструментальных средств, навыками тестирования, отладки и верификации

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
	5 Семестр						
1	Причины трудоемкости решения задач защиты информации. Основы криптографии	1-8	16/0/0	к.р-8 (25)	25	КИ-8	З-ОПК-2, У-ОПК-2, В-ОПК-2, З-ОПК-3, У-ОПК-3, В-ОПК-3, З-ОПК-8, У-ОПК-8, В-ОПК-8, З-ОПК-

							9, У-ОПК-9, В-ОПК-9, З-ПК-1, У-ПК-1, В-ПК-1
2	Разрушающие программные воздействия. Аппаратно-программные методы защиты информации	9-16	16/0/0	Т-16 (25)	25	КИ-16	З-ОПК-2, У-ОПК-2, В-ОПК-2, З-ОПК-3, У-ОПК-3, В-ОПК-3, З-ОПК-8, У-ОПК-8, В-ОПК-8, З-ОПК-9, У-ОПК-9, В-ОПК-9, З-ПК-1, У-

							ПК-1, В-ПК-1
	Итого за 5 Семестр		32/0/0		50		
	Контрольные мероприятия за 5 Семестр				50	Э	З-ОПК-2, У-ОПК-2, В-ОПК-2, З-ОПК-3, У-ОПК-3, В-ОПК-3, З-ОПК-8, У-ОПК-8, В-ОПК-8, З-ОПК-9, У-ОПК-9, В-ОПК-9, З-ПК-1, У-ПК-1, В-ПК-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
Т	Тестирование
КИ	Контроль по итогам
к.р	Контрольная работа
Э	Экзамен

КАЛЕНДАРНЫЙ ПЛАН

Недели	Темы занятий / Содержание	Лек., час.	Пр./сем., час.	Лаб., час.
	5 Семестр	32	0	0
1-8	**Причины трудоемкости решения задач защиты информации. Основы криптографии**	16	0	0
1	**Информационно-психологическая война. Информационно-техническая война. Главные угрозы кибербезопасности** 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	0 0	0 0
2	**Процессный подход к решению задач защиты информации** 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.	Всего аудиторных часов 2 Онлайн 0	0 0	0 0
3	**Основные термины и определения. Правило Кергофса** Основные термины и определения. Правило Кергофса. Требования к качественному шифру. Классификация шифров.	Всего аудиторных часов 2 Онлайн 0	0 0	0 0
4 - 5	**Модель криптосистемы с секретным ключом. Блочные и поточные шифры** Модель криптосистемы с секретным ключом. Блочные и поточные шифры. SP-сеть. Сеть Фейстеля. Архитектура Квадрат. XSL-шифры. Генераторы псевдослучайных чисел (ГПСЧ). Требования к качественному ГПСЧ. Хеш-функции. Требования к качественной хеш-функции.	Всего аудиторных часов 4 Онлайн 0	0 0	0 0
6 - 8	**Модель криптосистемы с открытым ключом. Односторонняя функция, Односторонняя функция с секретом** Модель криптосистемы с открытым ключом. Односторонняя функция, Односторонняя функция с секретом. Криптосистема RSA. Криптографические протоколы. Протокол выработки общего секретного ключа.	Всего аудиторных часов 6 Онлайн 0	0 0	0 0

	Протокол классической электронной подписи. Протоколы аутентификации удаленных абонентов. Протокол разделения секрета. Протоколы доказательства с нулевым разглашением знаний.			
9-16	**Разрушающие программные воздействия. Аппаратно-программные методы защиты информации**	16	0	0
9 - 10	**Типы РПВ. Компьютерные вирусы (КВ), применяющие специальные приемы, затрудняющие их обнаружение** Типы РПВ. Компьютерные вирусы (КВ), применяющие специальные приемы, затрудняющие их обнаружение. Сверхживучие КВ. Сетевые черви. Троянские программы. Бэкдоры. Эксплойты. Дропперы. Хакерские утилиты	Всего аудиторных часов		
		4	0	0
		Онлайн		
		0	0	0
11	**Методы антивирусной защиты (АВЗ)** Методы антивирусной защиты (АВЗ). Комплекс программных средств АВЗ.	Всего аудиторных часов		
		2	0	0
		Онлайн		
		0	0	0
12 - 13	**Самотестирование СБИС. Контролепригодное проектирование** Самотестирование СБИС. Контролепригодное проектирование. Контроль хода выполнения программ. Сторожевой процессор. Помехоустойчивое кодирование. Кодек (7, 4)-кода Хэмминга.	Всего аудиторных часов		
		4	0	0
		Онлайн		
		0	0	0
14 - 16	**Генераторы псевдослучайных чисел на регистрах сдвига с линейными и нелинейными обратными связями** Генераторы псевдослучайных чисел на регистрах сдвига с линейными и нелинейными обратными связями. Генераторы М-последовательностей. Генераторы (М - 1)-последовательностей. Генераторы (М + 1)-последовательностей.	Всего аудиторных часов		
		6	0	0
		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

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-2	З-ОПК-2	Э, КИ-8, КИ-16, к.р-8, Т-16
	У-ОПК-2	Э, КИ-8, КИ-16, к.р-8, Т-16
	В-ОПК-2	Э, КИ-8, КИ-16, к.р-8, Т-16
ОПК-3	З-ОПК-3	Э, КИ-8, КИ-16, к.р-8, Т-16
	У-ОПК-3	Э, КИ-8, КИ-16, к.р-8, Т-16
	В-ОПК-3	Э, КИ-8, КИ-16, к.р-8, Т-16
ОПК-8	З-ОПК-8	Э, КИ-8, КИ-16, к.р-8, Т-16
	У-ОПК-8	Э, КИ-8, КИ-16, к.р-8, Т-16
	В-ОПК-8	Э, КИ-8, КИ-16, к.р-8, Т-16
ОПК-9	З-ОПК-9	Э, КИ-8, КИ-16, к.р-8, Т-16
	У-ОПК-9	Э, КИ-8, КИ-16, к.р-8, Т-16
	В-ОПК-9	Э, КИ-8, КИ-16, к.р-8, Т-16
ПК-1	З-ПК-1	Э, КИ-8, КИ-16, к.р-8, Т-16
	У-ПК-1	Э, КИ-8, КИ-16, к.р-8, Т-16
	В-ПК-1	Э, КИ-8, КИ-16, к.р-8, Т-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 – «*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 : , Санкт-Петербург: Лань, 2022

2. ЭИ В 60 Защита информации : Учебное пособие для вузов, Москва: Юрайт, 2021

3. ЭИ И20 Криптографические методы защиты информации в компьютерных системах и сетях : учебное пособие для вузов, Москва: НИЯУ МИФИ, 2012

4. ЭИ Ч-45 Применение искусственных нейронных сетей и системы остаточных классов в криптографии : учебное пособие, Москва: Физматлит, 2012

5. ЭИ Р17 Разрушающие программные воздействия : учебно-методическое пособие для вузов, ред. М. А. Иванов, Москва: НИЯУ МИФИ, 2011

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

1. 004 Р17 Разрушающие программные воздействия : учебно-методическое пособие для вузов, А. Б. Вавренюк [и др.], Москва: НИЯУ МИФИ, 2011

2. 004 П64 Поточные шифры : , А.В.Асосков [и др.], М.: Кудиц-образ, 2003

3. 004 Ш76 Секреты и ложь : Безопасность данных в цифровом мире, Б. Шнайер, М.и др.: Питер, 2003

4. 004 Г82 Цифровая стеганография : , В. Г. Грибунин, И. Н. Оков, И. В. Туринцев, М.: Солон-Пресс, 2002

5. 0 М24 Современная криптография : теория и практика, В. Мао, Москва [и др.]: Вильямс, 2005

6. 004 И20 Теория, применение и оценка качества генераторов псевдослучайных последовательностей : , М.А. Иванов, И.В. Чугунков, Москва: Кудиц-образ, 2003

7. 519 С13 Введение в алгебраические коды : учебное пособие, Ю. Л. Сагалович, Москва: ИППИ, 2010

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 (ориентировочно после 8-й лекции) 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 (о целях практикума, инструментальных средствах для выполнения лабораторных работ, о порядке отчета по лабораторным работам), 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.