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 ТФ НИЯУ МИФИ

Протокол № 6

от 23.12.2022 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ЗАЩИТА ИНФОРМАЦИИ

Направление подготовки (специальность) [1] 14.03.01 Ядерная энергетика и теплофизика

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**
7	1	36	24	0	0		12	0	З
Итого	1	36	24	0	0	0	12	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

Дисциплина "Защита информации" относится к вариативной части образовательной программы.

Для успешного освоения дисциплины "Защита информации" необходимы компетенции, формируемые в результате освоения следующих дисциплин:

"Информатика".

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 использовать базовые знания естественнонаучных дисциплин в профессиональной деятельности, применять методы математического анализа и моделирования, теоретического и экспериментального исследования	З-ОПК-1 [1] – Знать базовые законы естественнонаучных дисциплин; основные математические законы; основные физические явления, процессы, законы и границы их применимости; сущность основных химических законов и явлений; методы математического моделирования, теоретического и экспериментального исследования У-ОПК-1 [1] – Уметь выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности, привлекать для их решения соответствующий физико-математический аппарат В-ОПК-1 [1] – Владеть математическим аппаратом для разработки моделей процессов и явлений, решения практических задач профессиональной деятельности; навыками использования основных общефизических законов и принципов
ОПК-2 [1] – Способен понимать принципы работы информационных технологий; осуществлять поиск, хранение, обработку и анализ информации из	З-ОПК-2 [1] – Знать средства и методы поиска, анализа, обработки и хранения информации, в том числе виды источников информации, поисковые системы и системы хранения информации. У-ОПК-2 [1] – Уметь осуществлять поиск, хранение,

различных источников и баз данных, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий	анализ и обработку информации, представлять ее в требуемом формате; применять компьютерные и сетевые технологии. В-ОПК-2 [1] – Владеть навыком поиска, хранения, обработки и анализа информации из различных источников и баз данных, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий.
ОПК-4 [1] – Способен использовать в профессиональной деятельности современные информационные системы, анализировать возникающие при этом опасности и угрозы, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны	З-ОПК-4 [1] – Знать системы хранения информации, требования информационной безопасности, включая защиту государственной тайны У-ОПК-4 [1] – Уметь использовать информационные системы и анализировать возникающие при этом опасности и угрозы. В-ОПК-4 [1] – Владеть навыками соблюдения основных требований информационной безопасности, в том числе защиты государственной тайны
УКЦ-1 [1] – Способен в цифровой среде использовать различные цифровые средства, позволяющие во взаимодействии с другими людьми достигать поставленных целей	З-УКЦ-1 [1] – Знать: современные информационные технологии и цифровые средства коммуникации, в том числе отечественного производства, а также основные приемы и нормы социального взаимодействия и технологии межличностной и групповой коммуникации с использованием дистанционных технологий У-УКЦ-1 [1] – Уметь: выбирать современные информационные технологии и цифровые средства коммуникации, в том числе отечественного производства, а также устанавливать и поддерживать контакты, обеспечивающие успешную работу в коллективе и применять основные методы и нормы социального взаимодействия для реализации своей роли и взаимодействия внутри команды с использованием дистанционных технологий В-УКЦ-1 [1] – Владеть: навыками применения современных информационных технологий и цифровых средств коммуникации, в том числе отечественного производства, а также методами и приемами социального взаимодействия и работы в команде с использованием дистанционных технологий

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
	7 Семестр						
1	Защита информации от умышленных деструктивных воздействий	1-6	12/0/0		25	СК-8	З-ОПК-1, У-ОПК-1, В-ОПК-1, З-ОПК-2, У-ОПК-2, В-ОПК-2, З-ОПК-4, У-ОПК-4, В-ОПК-4, З-

							УКЦ-1, У-УКЦ-1, В-УКЦ-1
2	Разрушающие программные воздействия	7-12	12/0/0		25	КИ-16	З-ОПК-1, У-ОПК-1, В-ОПК-1, З-ОПК-2, У-ОПК-2, В-ОПК-2, З-ОПК-4, У-ОПК-4, В-ОПК-4, З-УКЦ-1, У-УКЦ-1, В-УКЦ-1
	Итого за 7 Семестр		24/0/0		50		
	Контрольные мероприятия за 7 Семестр				50	З	З-ОПК-1, У-ОПК-1, В-

							ОПК-1, З-ОПК-2, У-ОПК-2, В-ОПК-2, В-ОПК-4, З-УКЦ-1, У-УКЦ-1, В-УКЦ-1, З-ОПК-4, У-ОПК-4

* – 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**
СК	Семестровый контроль
КИ	Контроль по итогам
З	Зачет

КАЛЕНДАРНЫЙ ПЛАН

Недели	**Темы занятий / Содержание**	**Лек., час.**	**Пр./сем., час.**	**Лаб., час.**
	7 Семестр	24	0	0
1-6	**Защита информации от умышленных деструктивных воздействий**	12	0	0
1	**Компьютерные системы (КС) как объекты защиты информации**	Всего аудиторных часов		
		2	0	0

	Компьютерные системы (КС) как объекты защиты информации. Методы и средства защиты информации от случайных и преднаме-ренных деструктивных воздействий. Требования к эффективной системе обеспечения безопасности информации (ОБИ).	Онлайн		
		0	0	0
2	**Введение в криптологию** Введение в криптологию. Основные термины и определения. Криптографическое преобразование информации. Классификация шифров. Требования к качественному шифру. Требования к каче-ственной хеш-функции.	Всего аудиторных часов		
		2	0	0
		Онлайн		
		0	0	0
3	**Криптосистемы с секретным ключом** Криптосистемы с секретным ключом. ГОСТ 28147-89. Американ-ский стандарт криптозащиты AES-128. Поточные шифры A5, RC4.	Всего аудиторных часов		
		2	0	0
		Онлайн		
		0	0	0
4	**Криптосистемы с открытым ключом** Криптосистемы с открытым ключом. Криптосистема RSA. Ранце-вая криптосистема.	Всего аудиторных часов		
		2	0	0
		Онлайн		
		0	0	0
5 - 6	**Криптографические протоколы** Криптографические протоколы. Протокол выработки общего сек-ретного ключа. Протоколы электронной цифровой подписи. Про-токолы аутентификации удаленных абонентов. Протоколы доказа-тельства с нулевым разглашением знаний. Протоколы разделения секрета.	Всего аудиторных часов		
		4	0	0
		Онлайн		
		0	0	0
7-12	**Разрушающие программные воздействия**	12	0	0
7 - 8	**Стохастические методы защиты информации** Теория, применение и оценка качества генераторов псевдослучайных чисел (ГПСЧ). Внесение неопредленности в работу средств и объектов защиты. Функции ГПСЧ и хеш-генераторов в системах ОБИ.	Всего аудиторных часов		
		4	0	0
		Онлайн		
		0	0	0
9 - 10	**Разрушающие программные воздействия (РПВ)** Разрушающие программные воздействия (РПВ). Структура ком-плекса программных средств антивирусной защиты. Методы анти-вирусной защиты.	Всего аудиторных часов		
		4	0	0
		Онлайн		
		0	0	0
11	**Контроль целостности информации** Контроль целостности информации. CRC-коды. Криптографиче-ские методы контроля целостности информации.	Всего аудиторных часов		
		2	0	0
		Онлайн		
		0	0	0
12	**Разграничение доступа** Организация парольных систем	Всего аудиторных часов		
		2	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 по адресу http://dozen.mephi.ru.

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	З, СК-8, КИ-16
	У-ОПК-1	З, СК-8, КИ-16
	В-ОПК-1	З, СК-8, КИ-16
ОПК-2	З-ОПК-2	З, СК-8, КИ-16
	У-ОПК-2	З, СК-8, КИ-16
	В-ОПК-2	З, СК-8, КИ-16
ОПК-4	З-ОПК-4	З, СК-8, КИ-16
	У-ОПК-4	З, СК-8, КИ-16
	В-ОПК-4	З, СК-8, КИ-16
УКЦ-1	З-УКЦ-1	З, СК-8, КИ-16
	У-УКЦ-1	З, СК-8, КИ-16
	В-УКЦ-1	З, СК-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:

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.

Оценочные средства приведены в Приложении.

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

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 (при его наличии)

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.

4. 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 (при его наличии)

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.