

ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ
КАФЕДРА КОМПЬЮТЕРНЫХ СИСТЕМ И ТЕХНОЛОГИЙ

ОДОБРЕНО УМС ИФТЭБ

Протокол № 545-2

от 31.05.2023 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, экс./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

Дисциплина Защита информации относится к базовой части рабочего учебного плана.

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-8 [1] – Способен применять методы научных исследований при разработке информационно-аналитических систем безопасности	З-ОПК-8 [1] – знать методы научных исследований при разработке информационно-аналитических систем безопасности У-ОПК-8 [1] – уметь применять методы научных исследований при разработке информационно-аналитических систем безопасности В-ОПК-8 [1] – владеть методами научных исследований при разработке информационно-аналитических систем безопасности

4. ВОСПИТАТЕЛЬНЫЙ ПОТЕНЦИАЛ ДИСЦИПЛИНЫ

Направления/цели воспитания	Задачи воспитания (код)	Воспитательный потенциал дисциплин
-----------------------------	-------------------------	------------------------------------

5. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Разделы учебной дисциплины, их объем, сроки изучения и формы контроля:

№ п.п	Наименование раздела учебной дисциплины	Недели	Лекции/ Практик. (семинары)/ Лабораторные работы, час.	Обязат. текущий контроль (форма*, неделя)	Максимальный балл за раздел**	Аттестация раздела (форма*, неделя)	Индикаторы освоения компетенции
	<i>6 Семестр</i>						
1	Защита информации от умышленных деструктивных воздействий	1-8	16/8/8		25	КИ-8	З-ОПК-8, У-ОПК-8, В-ОПК-8
2	Защита информации от случайных деструктивных воздействий	9-15	14/7/7		25	КИ-15	З-ОПК-8, У-ОПК-8, В-ОПК-8
	<i>Итого за 6 Семестр</i>		30/15/15		50		
	Контрольные мероприятия за 6 Семестр				50	Э	З-ОПК-8, У-ОПК-8, В-ОПК-8

* – 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

Недел и	Темы занятий / Содержание	Лек., час.	Пр./сем. , час.	Лаб., час.
	<i>6 Семестр</i>	30	15	15
1-8	Защита информации от умышленных деструктивных воздействий	16	8	8
1	Компьютерные системы (КС) как объекты защиты информации. Методы и средства защиты информации от случайных и преднамеренных деструктивных воздействий. Требования к эффективной системе обеспечения безо Компьютерные системы (КС) как объекты защиты информации. Методы и средства защиты информации от случайных и преднамеренных деструктивных воздействий. Требования к эффективной системе обеспечения безопасности информации (ОБИ).	Всего аудиторных часов		
		2	1	1
		Онлайн		
		0	0	0
2	Введение в криптологию. Основные термины и определения. Криптографическое преобразование информации. Классификация шифров. Требования к качественному шифру. Требования к качественной хеш-функции. Введение в криптологию. Основные термины и определения. Криптографическое преобразование информации. Классификация шифров. Требования к качественному шифру. Требования к качественной хеш-функции.	Всего аудиторных часов		
		2	1	1
		Онлайн		
		0	0	0
3	Криптосистемы с секретным ключом. ГОСТ 28147-89. Американский стандарт криптозащиты AES-128. Поточные шифры A5, RC4. Криптосистемы с секретным ключом. ГОСТ 28147-89. Американский стандарт криптозащиты AES-128. Поточные шифры A5, RC4.	Всего аудиторных часов		
		2	1	1
		Онлайн		
		0	0	0
4 - 5	Криптосистемы с открытым ключом. Криптосистема RSA. Ранцевая криптосистема. Криптосистемы с открытым ключом. Криптосистема RSA. Ранцевая криптосистема.	Всего аудиторных часов		
		4	2	2
		Онлайн		
		0	0	0
6 - 8	Криптографические протоколы. Протокол выработки общего секретного ключа. Протоколы электронной цифровой подписи. Протоколы аутентификации удаленных абонентов. Протоколы доказательства с нулевым раз Криптографические протоколы. Протокол выработки общего секретного ключа. Протоколы электронной цифровой подписи. Протоколы аутентификации удаленных абонентов. Протоколы доказательства с нулевым разглашением знаний. Протоколы разделения секрета.	Всего аудиторных часов		
		6	3	3
		Онлайн		
		0	0	0
9-15	Защита информации от случайных деструктивных воздействий	14	7	7
9	Цифровые деньги. Структура централизованной платежной системы. Жизненный цикл цифровой купюры. Цифровые деньги. Структура централизованной платежной	Всего аудиторных часов		
		2	1	1
		Онлайн		
		0	0	0

	систе-мы. Жизненный цикл цифровой купюры.			
10 - 11	Стохастические методы защиты информации. Теория, применение и оценка качества генераторов псевдослучайных чисел (ГПСЧ). Внесение неопределенности в работу средств и объектов защиты. Функции ГПСЧ и хеш Стохастические методы защиты информации. Теория, применение и оценка качества генераторов псевдослучайных чисел (ГПСЧ). Внесение неопределенности в работу средств и объектов защиты. Функции ГПСЧ и хеш-генераторов в системах ОБИ.	Всего аудиторных часов		
		4	2	2
		Онлайн		
		0	0	0
12	Разрушающие программные воздействия (РПВ). Структура ком-плекса программных средств антивирусной защиты. Методы анти-вирусной защиты. Разрушающие программные воздействия (РПВ). Структура ком-плекса программных средств антивирусной защиты. Методы анти-вирусной защиты.	Всего аудиторных часов		
		2	1	1
		Онлайн		
		0	0	0
13	Контроль целостности информации. CRC-коды. Криптографиче-ские методы контроля целостности информации. Контроль целостности информации. CRC-коды. Криптографиче-ские методы контроля целостности информации.	Всего аудиторных часов		
		2	1	1
		Онлайн		
		0	0	0
14 - 15	Разграничение доступа. Организация парольных систем. Разграничение доступа. Организация парольных систем.	Всего аудиторных часов		
		4	2	2
		Онлайн		
		0	0	0

Сокращенные наименования онлайн опций:

Обозна- чение	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
	<i>6 Семестр</i>
4 - 5	Работа 1. Криптоанализ шифра "Усложненная перестановка по таблице". Работа 1. Криптоанализ шифра "Усложненная перестановка по таблице".
5 - 7	Работа 2. Протоколы электронной цифровой подписи.

	Работа 2. Протоколы электронной цифровой подписи.
8 - 9	Работа 3. Российский стандарт криптозащиты ГОСТ 28147-89. Работа 3. Российский стандарт криптозащиты ГОСТ 28147-89.
10 - 11	Работа 4. Американский стандарт криптозащиты AES. Работа 4. Американский стандарт криптозащиты AES.

ТЕМЫ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Недели	Темы занятий / Содержание
	<i>6 Семестр</i>
	Защита информации от умышленных деструктивных воздействий Защита информации от умышленных деструктивных воздействий
	Защита информации от случайных деструктивных воздействий Защита информации от случайных деструктивных воздействий

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>.

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-8	З-ОПК-8	Э, КИ-8, КИ-15
	У-ОПК-8	Э, КИ-8, КИ-15
	В-ОПК-8	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 – <i>«отлично»</i>	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 – <i>«хорошо»</i>	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 – <i>«удовлетворительно»</i>	E	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			
Ниже 60	2 – <i>«неудовлетворительно»</i>	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 В 60 Защита информации : Учебное пособие для вузов, Москва: Юрайт, 2021
2. ЭИ Щ 33 Защита информации: основы теории : учебник для вузов, Москва: Юрайт, 2022

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 Криптографические методы защиты информации в компьютерных системах и сетях : учебное пособие для вузов, М. А. Иванов, И. В. Чугунков ; ред. : М. А. Иванов, Москва: НИЯУ МИФИ, 2012
7. 004 И20 Теория, применение и оценка качества генераторов псевдослучайных последовательностей : , М.А. Иванов, И.В. Чугунков, Москва: Кудиц-образ, 2003
8. 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.