

ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ
КАФЕДРА КРИПТОЛОГИИ И ДИСКРЕТНОЙ МАТЕМАТИКИ

ОДОБРЕНО УМС ИИКС

Протокол № УМС-575/01-1

от 30.08.2021 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ИССЛЕДОВАНИЕ И РАЗРАБОТКА ДЕЦЕНТРАЛИЗОВАННЫХ СИСТЕМ

Направление подготовки
(специальность)

[1] 10.04.01 Информационная безопасность

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
3	2	72	0	32	16	24	0	3
Итого	2	72	0	32	16	0	24	0

АННОТАЦИЯ

Дисциплина реализует требования образовательного стандарта НИЯУ МИФИ.

Рабочая программа учебной дисциплины содержит описание целей освоения дисциплины, ее место в структуре ООП, ВПО, формируемые в результате освоения дисциплины компетенции студента, структуру и содержание дисциплины, используемые во время освоения дисциплины образовательные технологии, оценочные средства для контроля успеваемости, учебно-методическое, информационное и материально-техническое обеспечение дисциплины.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью освоения учебной дисциплины является изучение современных технологий построения защищенных децентрализованных систем, включая технические аспекты их проектирования.

Задачами дисциплины являются:

- привитие обучаемым основ комплексного подхода к обеспечению информацион-ной безопасности объекта защиты;
- формирование у обучаемых понимания сущности этапов жизненного цикла;
- ознакомление обучаемых с порядком оформления рабочей технической докумен-тации и с учетом действующих нормативных и методических документов;
- обучение различным подходам и методам проектирования подсистем и средств обеспечения информационной безопасности.

Вместе с другими дисциплинами общенаучного и профессионального циклов дис-циplin изучение данной дисциплины призвано формировать специалиста, и в частности, вырабатывать у него такие качества, как

- строгость в суждениях,
- творческое мышление,
- организованность и работоспособность,
- дисциплинированность,
- самостоятельность и ответственность.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина является неотъемлемой составной частью профессиональной подготовки магистров по направлению подготовки 10.04.03 «Информационная безопасность».

Дисциплина относится к числу дисциплин по выбору профессионального модуля.

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыки, сформированные в процессе:

- изучения программы общеобразовательной школы;
- освоения программы подготовки бакалавров или программ подготовки специалистов по родственным направлениям высшего профессионального образования;
- изучения дисциплин «Основы информационной безопасности», «Теоретические основы кибернетики».

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
--------------------------------	--

Профессиональные компетенции в соответствии 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			
выполнение научно-исследовательских работ по развитию физических, математических или технических методов обеспечения безопасности данных	методы обеспечения безопасности данных	ПК-3 [1] - Способен самостоятельно ставить конкретные задачи научных исследований в области ИБ или информационно-аналитических систем безопасности и решать их с использованием новейшего отечественного и зарубежного опыта <i>Основание:</i> Профессиональный стандарт: 06.032	З-ПК-3[1] - Знать: руководящие и методические документы уполномоченных федеральных органов исполнительной власти, устанавливающие требования к организации и проведению аттестации и сертификационных испытаний средств и систем защиты сссэ от нсд, зткс; основные средства и способы обеспечения информационной безопасности, принципы построения средств и систем защиты сссэ от нсд, зткс; национальные, межгосударственные и международные стандарты, устанавливающие требования по защите информации, анализу

			защищенности сетей электросвязи и оценки рисков нарушения их информационной безопасности. ; У-ПК-3[1] - Уметь: организовывать сбор, обработку, анализ и систематизацию научно-технической информации, отечественного и зарубежного опыта по проблемам информационной безопасности сетей электросвязи.; В-ПК-3[1] - Владеть: организацией подготовки научно-технических отчетов, обзоров, публикаций по результатам выполненных исследований.
	проектный		
разработка проектных решений по обеспечению безопасности данных с применением криптографических методов	информационные ресурсы	ПК-4.1 [1] - Способен разрабатывать проектные решения по обеспечению безопасности данных с применением криптографических методов <i>Основание:</i> Профессиональный стандарт: 06.032	3-ПК-4.1[1] - Знать: методы обеспечения безопасности данных с применением криптографических методов; У-ПК-4.1[1] - Уметь: разрабатывать проектные решения по обеспечению безопасности данных с применением криптографических методов; В-ПК-4.1[1] - Владеть: навыками разработки проектных решений по обеспечению безопасности данных с применением криптографических методов

4. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

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

№ п.п	Наименование раздела учебной дисциплины	Недели	Лекции/ Практи. (семинары)/ Лабораторные работы, час.	Обязат. текущий контроль (форма*, неделя)	Максимальный балл за раздел**	Аттестация раздела (форма*, неделя)	Индикаторы освоения компетенции
	<i>3 Семестр</i>						
1	Первый раздел	1-8			25	КИ-8	3-ПК-3, У-ПК-3, В-ПК-3, 3-ПК-4.1, У-ПК-4.1, В-ПК-4.1
2	Второй раздел	9-16			25	КИ-16	3-ПК-3, У-ПК-3, В-ПК-3, 3-ПК-4.1, У-ПК-4.1, В-ПК-4.1
	<i>Итого за 3 Семестр</i>		0/32/16		50		
	Контрольные мероприятия за 3 Семестр				50	3	3-ПК-3, У-ПК-3, В-ПК-3, 3-ПК-4.1, У-ПК-4.1, В-ПК-4.1

* – 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
КИ	Контроль по итогам
З	Зачет

КАЛЕНДАРНЫЙ ПЛАН

Недели	Темы занятий / Содержание	Лек., час.	Пр./сем., час.	Лаб., час.
	<i>3 Семестр</i>	0	32	16
1-8	Первый раздел		16	8
1	Тема № 1. Введение. Системная инженерия. Понятие сложной системы, ее элементы и подсистемы. Автоматизированная система. Информационная система. Классификация объектов проектирования, основные стадии проектирования. Иерархия систем и проектов. Обеспечивающие системы.	Всего аудиторных часов		
			2	1
		Онлайн		
2 - 3	Тема № 2. Защищенные автоматизированные системы. Основные характеристики защищенных децентрализованных систем. Надежность и своевременность предоставления информации. Полнота, безошибочность, корректность, конфиденциальность. Показатели безопасности функционирования систем, их защищенность от программно-технических воздействий и от несанкционированного доступа.	Всего аудиторных часов		
			4	2
		Онлайн		
4	Тема № 3. Жизненный цикл системы. Жизненный цикл децентрализованных систем. Замысел, разработка, производство, эксплуатация, сопровождение, списание. Показатели эффективности системы на различных этапах жизненного цикла.	Всего аудиторных часов		
			2	1
		Онлайн		
5 - 6	Тема № 4. Определение требований Заказчика, их анализ. Общий развернутый планы проектирования. Выбор архитектуры системы. Определение основных компонентов системы. Разработка данных, средства их управления. Реализация проекта.	Всего аудиторных часов		
			4	2
		Онлайн		
7 - 8	Тема № 5. Порядок проведения работ. Основные стадии разработки защищенных децентрализованных систем. Комплексирование, верификация, передача системы Заказчику. Рациональное управление процессом проектирования, сбор исходных данных по проекту, их анализ и обобщение. Выбор рационального варианта, максимизирующего или минимизирующего значение целевой функции системы.	Всего аудиторных часов		
			4	2
		Онлайн		

9-16	Второй раздел		16	8
9 - 10	Тема № 6. Обеспечение качества программных средств. Основные режимы функционирования программ. Жизненный цикл программного обеспечения (ПО). Особенности отказов в ПО. Последствия искажений в программах. Корректная и надежная программы. Методы программного восстановления. Избыточность при создании ПО. Тестирование программ. Требования к программной документации.	Всего аудиторных часов		
			4	2
		Онлайн		
11	Тема № 7. Техническая документация. Роль технической до-кументации при проектировании. Виды документов, их особенности. Комплектация проектной и сопровождающей документации. Структура отчета о НИР.	Всего аудиторных часов		
			2	1
		Онлайн		
12 - 13	Тема № 8. Человеческий фактор при построении систем. Понятие человеческого фактора., его роль при проектирова-нии децентрализованных систем. Анализ ошибок при контроле. Корректность выполнения обработки информации. Анализ комплексного функционирования системы.	Всего аудиторных часов		
			4	2
		Онлайн		
14 - 16	Тема № 9. Риски при построении систем. Факторы неопределенности при проектировании, их учет. Риски в жизнен-ном цикле систем и при их проектировании. Определение рисков, их анализ, учет и контроль. Стратегии управления рисками при проектировании и эксплуатации защищенных децентрализованных систем.	Всего аудиторных часов		
			6	3
		Онлайн		

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

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Дисциплина сформирована как курс лекций, при чтении которых используются современные мультимедийные средства. Для самостоятельной работы студентов используются специально подготовленный конспект лекций и другая рекомендуемая преподавателем учебная литература.

С целью формирования и развития профессиональных навыков студентов в дисциплине используются активные и интерактивные формы проведения занятий: доклады и презентации с их обсуждением, ролевые игры с дискуссиями и разбором конкретных ситуаций в сочетании с внеаудиторной работой.

В процессе преподавания дисциплины в каждом разделе выделяются наиболее важные темы и внимание обучаемых особо акцентируется на них.

В рамках дисциплины предусмотрены встречи с представителями государственных и общественных организаций, мастер-классы экспертов и специалистов в области сетевой безопасности, а также российских и зарубежных компаний – разработчиками систем защиты информации для сетей.

6. 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)
ПК-3	З-ПК-3	З, КИ-8, КИ-16
	У-ПК-3	З, КИ-8, КИ-16
	В-ПК-3	З, КИ-8, КИ-16
ПК-4.1	З-ПК-4.1	З, КИ-8, КИ-16
	У-ПК-4.1	З, КИ-8, КИ-16
	В-ПК-4.1	З, КИ-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		B	Оценка «хорошо» выставляется

75-84		С	студенту, если он твёрдо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.
70-74		Д	
65-69	3 – «удовлетворительно»	Е	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 – «неудовлетворительно»	Ф	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.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. 004 М 21 Глобальная культура кибербезопасности : , Москва: Горячая линия -Телеком, 2018
2. 004 М 21 Основы политики безопасности критических систем информационной инфраструктуры. Курс лекций. : учеб. пособие для вузов., Москва: Горячая линия -Телеком, 2018

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

Специальное программное обеспечение не требуется

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

<https://online.mephi.ru/>

<http://library.mephi.ru/>

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Специальное материально-техническое обеспечение не требуется

9. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ

приложены

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

приложены

Автор(ы):

Епишкина Анна Васильевна, к.т.н.