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

ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ

КАФЕДРА КРИПТОЛОГИИ И КИБЕРБЕЗОПАСНОСТИ

ОДОБРЕНО УМС ИИКС

Протокол № 8/1/2025

от 25.08.2025 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ

Направление подготовки (специальность) — [1] 10.03.01 Информационная безопасность

Семестр	Трудоемкость, кред.	Общий объем курса, час.	Лекции, час.	Практич. занятия, час.	Лаборат. работы, час.	В форме практической подготовки, час.	СРС, час.	КСР, час.	Форма(ы) контроля, экз./зач./КР/КП
7	2	72	0	32	0		40	0	З
Итого	2	72	0	32	0	0	40	0	

АННОТАЦИЯ

В курсе рассматриваются следующие темы:

- системная инженерия;
- защищенные автоматизированные системы;
- жизненный цикл системы;
- порядок выполнения работ по проектированию и созданию систем;
- техническая документация;
- основы оценки соответствия;
- критическая информационная инфраструктура.

Значительное место отведено методам оценки соответствия средств защиты информации, которым в современных технологиям уделяется повышенное внимание.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Цель дисциплины - изучение и освоение современных технологий построения защищенных автоматизированных систем на различных этапах их жизненного цикла, включая технические аспекты проектирования

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Полученные знания используются при изучении следующих дисциплин:

• Моделирование систем защиты информации;
• Аудит информационных технологий и систем обеспечения безопасности;
• Информационная безопасность открытых систем;
• Защита информации в банковских системах;
• Разработка и эксплуатация защищенных автоматизированных систем;
• Защищенный электронный документооборот в кредитно-финансовой сфере.

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 [1] – Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах	З-ОПК-1.1 [1] – знать способы разработки политик управления доступом и информационными потоками в компьютерных системах У-ОПК-1.1 [1] – разрабатывать политики управления доступом и информационными потоками в компьютерных системах В-ОПК-1.1 [1] – владеть принципами формирования политики управления доступом и информационными потоками в компьютерных системах

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**
эксплуатационный			
эксплуатация технических и программно-аппаратных средств защиты информации	программно-аппаратные средства защиты информации	ПК-4.3 [1] - способен проводить экспериментальное исследование компьютерных систем с целью выявления уязвимостей *Основание:* Профессиональный стандарт: 06.032	З-ПК-4.3[1] - знать способы проведения экспериментального исследования компьютерных систем с целью выявления уязвимостей; У-ПК-4.3[1] - уметь проводить экспериментальное исследование компьютерных систем с целью выявления уязвимостей; В-ПК-4.3[1] - владеть принципами проведения экспериментального исследования компьютерных систем с целью выявления уязвимостей
организационно-управленческий			
организация работы по эксплуатации системы защиты информации	системы защиты информации	ПК-1.1 [1] - способен участвовать в разработке политик управления доступом и информационными потоками в компьютерных системах *Основание:* Профессиональный стандарт: 06.032	З-ПК-1.1[1] - знать способы разработки политик управления доступом и информационными потоками в компьютерных системах; У-ПК-1.1[1] - уметь разрабатывать политики управления доступом и информационными потоками в компьютерных системах; В-ПК-1.1[1] - владеть принципами формирования

			политики управления доступом и информационными потоками в компьютерных системах
организация работы по эксплуатации системы защиты информации	системы защиты информации	ПК-1.1 [1] - способен планировать и организовывать процесс информационной безопасности в корпоративных и технологических сетях *Основание:* Профессиональный стандарт: 06.032	З-ПК-1.1[1] - знать требования российского законодательства и международных стандартов в области информационной безопасности (ФСТЭК России, ФСБ России, ЦБ РФ, ISO 27001 и т.д..), основные угрозы информационной безопасности (БДУ ФСТЭК, OWASP TOP10), принципы создания систем защиты информации (облачных инфраструктур, облачных платформ, ГИС, ИСПДн, КИИ и др.), фреймворки для описания архитектуры предприятия, принципы работы сканеров уязвимостей, методы оценки и приоритезации уязвимостей; У-ПК-1.1[1] - уметь составлять модель угроз информационной безопасности, проводить технический аудит информационных систем на соответствие требованиям информационной безопасности, проводить анализ информационной безопасности архитектуры

			информационных систем, сервисов, взаимодействовать с информационными технологиями в части уточнения требований и проектных ожиданий, согласовать технические решения, выстраивать процесс управления уязвимостями, устранять уязвимости и контролировать защищенность активов; В-ПК-1.1[1] - владеть методами определения угроз информационной безопасности, навыками работы с современными средствами защиты информации
проектно-технологический			
проектирование и разработка систем информационной безопасности	технологии обеспечения информационной безопасности компьютерных систем	ПК-1.2 [1] - способен разрабатывать и анализировать алгоритмы решения профессиональных задач, реализовывать их в современных программных комплексах *Основание:* Профессиональный стандарт: 06.032	З-ПК-1.2[1] - знать алгоритмы решения профессиональных задач; У-ПК-1.2[1] - уметь разрабатывать и анализировать алгоритмы решения профессиональных задач, реализовывать их в современных программных комплексах; В-ПК-1.2[1] - владеть принципами разработки и анализа алгоритмов решения профессиональных задач
проектирование и разработка защищенных программно-аппаратных комплексов и распределённых	программно-аппаратные комплексы и распределённые информационные системы	ПК-2 [1] - способен проектировать подсистемы безопасности информации с учетом действующих нормативных и	З-ПК-2[1] - знать действующие нормативные и методические документы по проектированию подсистемы

информационных систем		методических документов *Основание:* Профессиональный стандарт: 06.001, 06.032	безопасности информации ; У-ПК-2[1] - уметь проектировать подсистемы безопасности информации с учетом действующих нормативных и методических документов; В-ПК-2[1] - владеть принципами проектирования подсистемы безопасности информации

4. ВОСПИТАТЕЛЬНЫЙ ПОТЕНЦИАЛ ДИСЦИПЛИНЫ

Направления/цели воспитания	**Задачи воспитания (код)**
Профессиональное воспитание	Создание условий, обеспечивающих, формирование ответственности за профессиональный выбор, профессиональное развитие и профессиональные решения (В18)
Профессиональное воспитание	Создание условий, обеспечивающих, формирование научного мировоззрения, культуры поиска нестандартных научно-технических/практических решений, критического отношения к исследованиям лженаучного толка (В19)
Профессиональное воспитание	Создание условий, обеспечивающих, формирование профессионально значимых установок: не производить, не копировать и не использовать программные и технические средства, не приобретённые на законных основаниях; не нарушать признанные нормы авторского права; не нарушать тайны передачи сообщений, не практиковать вскрытие информационных систем и сетей передачи данных; соблюдать конфиденциальность доверенной информации (В40)

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	Первый раздел	1-8	0/16/0		25	КИ-8	З-ОПК-1.1, У-ОПК-1.1, В-ОПК-1.1, З-ПК-4.3, У-ПК-4.3, В-ПК-4.3, З-ПК-1.1, У-ПК-1.1, В-ПК-1.1, З-ПК-1.2, У-ПК-1.2, В-ПК-1.2, З-ПК-2, У-ПК-2, В-ПК-2
2	Второй раздел	9-16	0/16/0		25	КИ-16	З-ОПК-1.1, У-ОПК-1.1, В-ОПК-1.1, З-ПК-4.3, У-ПК-4.3, В-ПК-4.3, З-ПК-1.1, У-ПК-1.1, В-ПК-1.1, З-ПК-1.2, У-ПК-1.2, В-ПК-1.2, З-ПК-2, У-ПК-2, В-ПК-2
	Итого за 7 Семестр		0/32/0		50		
	Контрольные мероприятия за 7 Семестр				50	З	З-ОПК-1.1, У-ОПК-1.1, В-ОПК-1.1, З-ПК-4.3, У-ПК-4.3, В-ПК-4.3, З-ПК-1.1, У-ПК-1.1, В-ПК-1.1, З-ПК-1.2, У-ПК-1.2, В-ПК-1.2,

							З-ПК-1.1, У-ПК-1.1, В-ПК-1.1, З-ПК-2, У-ПК-2, В-ПК-2

* – 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.**
	7 Семестр	0	32	0
1-8	**Первый раздел**	0	16	0
1 - 2	**Введение. Доктрина информационной безопас-ности РФ. Системная инженерия.** Предназначение Доктрины информационной безопасности России. Информационная инфраструктура РФ. Основные информационные угрозы и состояние информационной безопасности. Основные направления обеспечения информационной безопасности. в различных сферах. Понятие сложной системы, ее элементы и подсистемы. Автоматизированная система. Информационная система. Клас-сификация объектов проектирования, основные стадии проектирования. Иерархия систем и проек-тов. Обеспечивающие системы.	Всего аудиторных часов		
		0	4	0
		Онлайн		
		0	0	0
3 - 4	**Защищенные автоматизированные системы** Основные характеристики защищенных автомати-зированных систем. Надежность и своевремен-ность предоставления информации. Полнота, без-ошибочность, корректность, конфиденциальность. Показатели безопасности функционирования си-стем, их защищенность от программно-технических воздействий и от несанкционирован-ного доступа.	Всего аудиторных часов		
		0	4	0
		Онлайн		
		0	0	0
5	**Жизненный цикл системы.** Жизненный цикл автоматизированных систем. Замысел, разработка, производство, эксплуатация, сопровождение, списание. Показатели эффективности системы на различных этапах жизненного цикла.	Всего аудиторных часов		
		0	2	0
		Онлайн		
		0	0	0
6	**Определение требований Заказчика, их анализ.** Общий и развернутый планы проектирования. Выбор архитектуры системы. Определение основных	Всего аудиторных часов		
		0	2	0
		Онлайн		

	компонентов системы. Разработка данных, средства их управления. Реализация проекта.	0	0	0
7 - 8	**Порядок проведения работ.** Основные стадии разработки защищенных автоматизированных систем. Комплексирование, верификация, передача системы Заказчику. Определение и виды НИР. Этапы НИР. Порядок выполнения НИР. Назначение и структура технического задания. Рациональное управление процессом проектирования, сбор исходных данных по проекту, их анализ и обобщение	Всего аудиторных часов		
		0	4	0
		Онлайн		
		0	0	0
9-16	**Второй раздел**	0	16	0
9 - 10	**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 восстанов-ления. Избыточность при создании ПО. Тестирование программ. Требования к документа-ции ПО.	Всего аудиторных часов		
		0	4	0
		Онлайн		
		0	0	0
11 - 12	**Техническая документация.** Роль технической документации при проектировании. Виды документов, их особенности. Комплектация проектной и сопровождающей документации. Структура от-чета о НИР.	Всего аудиторных часов		
		0	4	0
		Онлайн		
		0	0	0
13	**Критическая информационная инфраструкту-ра.** Объекты и субъекты инфраструктуры. Процедура категорирования. Категории значимости объ-ектов. Оценка безопасности объектов критической информационной инфраструктуры.	Всего аудиторных часов		
		0	2	0
		Онлайн		
		0	0	0
14 - 16	**Основы оценки соответствия.** Определение оценки соответствия. Виды процедур оценки соответствия технических систем. Сертификация средств защиты информации. Правила и участники сертификации средств защиты информации. Роль и задачи ФСТЭК. Методики испытаний автоматизи-рованных систем.	Всего аудиторных часов		
		0	6	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

Основными образовательными технологиями в освоении дисциплин профессионального цикла являются традиционные технологии в форме практических занятий. Интерактивные методики обеспечиваются решением индивидуальных задач студентами и коллективным обсуждением результатов и методов решения.

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-1.1	З-ОПК-1.1	З, КИ-8, КИ-16
	У-ОПК-1.1	З, КИ-8, КИ-16
	В-ОПК-1.1	З, КИ-8, КИ-16
ПК-2	З-ПК-2	З, КИ-8, КИ-16
	У-ПК-2	З, КИ-8, КИ-16
	В-ПК-2	З, КИ-8, КИ-16
ПК-4.3	З-ПК-4.3	З, КИ-8, КИ-16
	У-ПК-4.3	З, КИ-8, КИ-16
	В-ПК-4.3	З, КИ-8, КИ-16
ПК-1.1	З-ПК-1.1	З, КИ-8, КИ-16
	У-ПК-1.1	З, КИ-8, КИ-16
	В-ПК-1.1	З, КИ-8, КИ-16
ПК-1.2	З-ПК-1.2	З, КИ-8, КИ-16
	У-ПК-1.2	З, КИ-8, КИ-16
	В-ПК-1.2	З, КИ-8, КИ-16
ПК-1.1	З-ПК-1.1	З
	У-ПК-1.1	З
	В-ПК-1.1	З

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-х балльной шкале**	**Отметка о зачете**	**Оценка ECTS**
90-100	5 – *«отлично»*	*«зачтено»*	A
85-89	4 – «*хорошо*»		B
75-84			C
70-74			D
65-69	3 – «*удовлетворительно*»		

60-64			E
ниже 60	2 – «*неудовлетворительно*»	*«не зачтено»*	F

Оценка «отлично» соответствует глубокому и прочному освоению материала программы обучающимся, который последовательно, четко и логически стройно излагает свои ответы, умеет тесно увязывать теорию с практикой, использует в ответах материалы монографической литературы.

Оценка «хорошо» соответствует твердым знаниям материала обучающимся, который грамотно и, по существу, излагает свои ответы, не допуская существенных неточностей.

Оценка «удовлетворительно» соответствует базовому уровню освоения материала обучающимся, при котором освоен основной материал, но не усвоены его детали, в ответах присутствуют неточности, недостаточно правильные формулировки, нарушения логической последовательности.

Отметка «зачтено» соответствует, как минимум, базовому уровню освоения материала программы, при котором обучающийся владеет необходимыми знаниями, умениями и навыками, умеет применять теоретические положения для решения типовых практических задач.

Оценку «неудовлетворительно» / отметку «не зачтено» получает обучающийся, который не знает значительной части материала программы, допускает в ответах существенные ошибки, не выполнил все обязательные задания, предусмотренные программой. Как правило, такие обучающиеся не могут продолжить обучение без дополнительных занятий.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. 004 М 21 Глобальная культура кибербезопасности : , Малюк А.А., Москва: Горячая линия - Телеком, 2018

2. 004 Т 76 Интеллектуальные автоматизированные системы управления технологическими объектами : учебно-практ. пособие, Кулаков С.М., Трофимов В.Б., Москва: Инфра-Инженерия, 2017

3. 005 М 48 Исследование систем управления : учебник для академического бакалавриата, Мельников В.П., Схиртладзе А.Г., Москва: Юрайт, 2016

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

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

Студенты должны своевременно спланировать учебное время для поэтапного и системного изучения данной учебной дисциплины в соответствии с планом занятий, графиком контроля знаний.

Успешное освоение дисциплины требует от студентов посещения и активной работы во время занятий, выполнения всех домашних заданий, ознакомления с базовыми учебниками, основной и дополнительной литературой, а также предполагает творческое участие студента путем планомерной, повседневной работы.

Изучение дисциплины следует начинать с проработки учебной программы, особое внимание, уделяя целям и задачам, структуре и содержанию курса.

Во время занятий рекомендуется писать конспект., что является одной из форм активной самостоятельной работы студентов, требующей навыков и умения кратко, схематично, последовательно и логично фиксировать основные положения, выводы, обобщения, формулировки.

В процессе изучения учебной дисциплины необходимо обратить внимание на самоконтроль. Требуется регулярно отводить время для повторения пройденного материала, проверяя свои знания, умения и навыки по контрольным вопросам, а также для выполнения домашних заданий, которые выдаются после каждого занятия.

Систематическая индивидуальная работа, постоянная активность на занятиях, готовность ставить и обсуждать актуальные проблемы курса – залог успешной работы и положительной оценки.

11. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

Учебный курс строится на интегративной основе и включает в себя как теоретические знания, так и практические навыки, получаемые студентами.

Данная дисциплина выполняет функции теоретической и практической подготовки студентов.

Содержание учебного курса, его объем и характер обусловливают необходимость оптимизации учебного процесса в плане отбора материала обучения и методики его организации, а также контроля текущей учебной работы. В связи с этим возрастает значимость и изменяется статус внеаудиторной (самостоятельной) работы, которая становится полноценным и обязательным видом учебно-познавательной деятельности студентов. При изучении курса самостоятельная работа включает:

самостоятельное ознакомление студентов с теоретическим материалом, представленным в отечественных и зарубежных научно-практических публикациях;

самостоятельное изучение тем учебной программы, достаточно хорошо обеспеченных литературой и сравнительно несложных для понимания;

подготовку к практическим занятиям по тем разделам, которые предполагают самостоятельную проработку материала учебных пособий.

Со стороны преподавателя должен быть установлен контакт со студентами, и они должны быть информированы о порядке прохождения курса, его особенностях, учебно-методическом обеспечении по данной дисциплине. Преподаватель дает методические рекомендации обучаемым по самостоятельному изучению проблем, характеризуя пути и средства достижения поставленных перед ними задач, высказывает советы и рекомендации по изучению учебной литературы, самостоятельной работе и работе на семинарских занятиях.

Автор(ы):

Финошин Михаил Александрович