

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

ИНСТИТУТ ФИНАНСОВЫХ ТЕХНОЛОГИЙ И ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ
КАФЕДРА ФИНАНСОВОГО МОНИТОРИНГА

ОДОБРЕНО УМС ИФТЭБ

Протокол № 545-1

от 30.08.2021 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ

Направление подготовки [1] 10.04.01 Информационная безопасность
(специальность)

Семестр	Трудоемкость, кред.	Общий объем курса, час.	Лекции, час.	Практич. занятия, час.	Лаборат. работы, час.	В форме практической подготовки/В СРС, час.	KCP, час.	Форма(ы) контроля, экз./зач./КР/КП
3	4	144	32	0	16		60	0
Итого	4	144	32	0	16	0	60	0

АННОТАЦИЯ

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции ОПК-1 [1] – Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	Код и наименование индикатора достижения компетенции 3-ОПК-1 [1] – Знать: основы стандартов в области обеспечения информационной безопасности; элементы компьютерного моделирования сложных систем, проектирования информационных, автоматизированных и автоматических систем У-ОПК-1 [1] – Уметь: проектировать информационные системы; обосновывать и планировать состав и архитектуру моделируемых и проектируемых информационных, автоматизированных и автоматических систем; разрабатывать и обосновывать критерии оценки эффективности проектируемой системы обеспечения информационной безопасности. В-ОПК-1 [1] – Владеть: навыками участия в разработке системы обеспечения информационной безопасности объекта; навыками проектирования автоматизированных информационных систем и систем обеспечения информационной безопасности
ОПК-2 [1] – Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	3-ОПК-2 [1] – Знать: методы проектирования технологий обеспечения информационной безопасности; принципы построения и функционирования современных информационных систем; требования к системам комплексной защиты информации У-ОПК-2 [1] – Уметь: обосновывать применяемые методы решения задач защиты информации, проектировать подсистемы безопасности информационных систем с учетом действующих нормативных и методических документов, разрабатывать модели угроз и нарушителей информационной безопасности В-ОПК-2 [1] – Владеть: навыками проектирования систем информационной безопасности

--	--

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
<p>Системный анализ прикладной области, выявление угроз и оценка уязвимости информационных систем, разработка требований и критерии оценки информационной безопасности, согласованных со стратегией развития информационных систем; обоснование выбора принципов организации и функциональной структуры программного, программно-аппаратного и технического обеспечения систем и средств обеспечения информационной безопасности объектов защиты на основе отечественных и международных стандартов; проектирование и разработка систем, комплексов, средств и технологий обеспечения информационной безопасности; разработка программ и методик испытаний программных, программноаппаратных</p>	<p>проектный</p> <p>Система обеспечения информационной безопасности и информационно-аналитического обеспечения финансового мониторинга</p>	<p>ПК-1 [1] - Способен принимать участие в разработке систем обеспечения ИБ или информационно-аналитических систем безопасности</p> <p><i>Основание:</i> Профессиональный стандарт: 06.033</p>	<p>З-ПК-1[1] - Знать: модели угроз НСД к сетям электросвязи; методики оценки уязвимостей сетей электросвязи с точки зрения возможности НСД к ним; нормативные правовые акты в области связи, информатизации и защиты информации; виды политик безопасности компьютерных систем и сетей; возможности используемых и планируемых к использованию средств защиты информации; особенности защиты информации в автоматизированных системах управления технологическими процессами; критерии оценки эффективности и надежности средств защиты информации программного обеспечения автоматизированных систем; основные характеристики технических средств защиты информации от утечек по техническим каналам; нормативные правовые акты, методические документы,</p>

<p>и технических средств и систем обеспечения информационной безопасности; разработка и применение автоматизированных технологий обработки больших информационных потоков (массивов) финансовой и/или экономической информации в режиме реального времени.</p>			<p>национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации; технические каналы утечки информации. ; У-ПК-1[1] - Уметь: выявлять и оценивать угрозы нсд к сетям электросвязи; анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия; классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; выбирать меры защиты информации, подлежащие реализации в системе защиты информации автоматизированной системы; проводить анализ угроз безопасности информации на объекте информатизации; проводить предпроектное обследование объекта информатизации. ; В-ПК-1[1] - Владеть: основами проведения технических работ при аттестации сссэ с учетом требований по защите информации; определением угроз безопасности информации, реализация которых может привести к</p>
--	--	--	--

			нарушению безопасности информации в компьютерной системе и сети; основами разработки модели угроз безопасности информации и модели нарушителя в автоматизированных системах; основами предпроектного обследования объекта информатизации; основами разработки аналитического обоснования необходимости создания системы защиты информации на объекте информатизации (модели угроз безопасности информации).
Системный анализ прикладной области, выявление угроз и оценка уязвимости информационных систем, разработка требований и критериев оценки информационной безопасности, согласованных со стратегией развития информационных систем; обоснование выбора принципов организации и функциональной структуры программного, программно-аппаратного и технического обеспечения систем и средств обеспечения информационной безопасности объектов защиты на основе отечественных и	Система обеспечения информационной безопасности и информационно-аналитического обеспечения финансового мониторинга	ПК-2 [1] - Способен разрабатывать технические задания на проектирование систем обеспечения ИБ или информационно-аналитических систем безопасности <i>Основание:</i> Профессиональный стандарт: 06.033	З-ПК-2[1] - Знать: формальные модели безопасности компьютерных систем и сетей; способы обнаружения и нейтрализации последствий вторжений в компьютерные системы; основные угрозы безопасности информации и модели нарушителя; в автоматизированных системах основные меры по защите информации; в автоматизированных системах; основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации; в автоматизированных системах; технические средства контроля эффективности мер

<p>международных стандартов; проектирование и разработка систем, комплексов, средств и технологий обеспечения информационной безопасности; разработка программ и методик испытаний программных, програмноаппаратных и технических средств и систем обеспечения информационной безопасности; разработка и применение автоматизированных технологий обработки больших информационных потоков (массивов) финансовой и/или экономической информации в режиме реального времени.</p>			<p>защиты информации; современные информационные технологии (операционные системы, базы данных, вычислительные сети); методы контроля защищенности информации от несанкционированного доступа и специальных действий; средства контроля защищенности информации от несанкционированного доступа. ; У-ПК-2[1] - Уметь: применять инструментальные средства проведения мониторинга защищенности компьютерных систем; анализировать основные характеристики и возможности телекоммуникационных систем по передаче информации, основные узлы и устройства современных автоматизированных систем; разрабатывать программы и методики испытаний программно-технического средства защиты информации от несанкционированного доступа и специальных действий на нее; проводить испытания программно-технического средства защиты информации от несанкционированного доступа и специальных действий на нее. ; В-ПК-2[1] - Владеть: основами выполнения анализа защищенности</p>
---	--	--	---

компьютерных систем с использованием сканеров безопасности; основами составлением методик тестирования систем защиты информации автоматизированных систем; основами подбора инструментальных средств тестирования систем защиты информации автоматизированных систем; основами разработки технического задания на создание программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее; основами разработки программ и методик испытаний программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее; основами испытаний программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее.

4. 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
	3 Семестр						

1	Первый раздел	1-8			25	КИ-8	
2	Второй раздел	9-16			25	КИ-16	
	<i>Итого за 3 Семестр</i>		32/0/16		50		
	Контрольные мероприятия за 3 Семестр				50		

* – 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:

Обозна чение	Полное наименование
КИ	Контроль по итогам
Э	Экзамен
КП	Курсовой проект

КАЛЕНДАРНЫЙ ПЛАН

Недел и	Темы занятий / Содержание	Лек., час.	Пр./сем. , час.	Лаб., час.
--------------------	----------------------------------	-----------------------	----------------------------	-----------------------

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

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
-------------	---------------------

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 иочно 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	
75-84		C	
70-74	4 – «хорошо»	D	Оценка «хорошо» выставляется студенту, если он твёрдо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.
65-69			
60-64	3 – «удовлетворительно»	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.
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.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

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