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

ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ

КАФЕДРА СТРАТЕГИЧЕСКИХ ИНФОРМАЦИОННЫХ ИССЛЕДОВАНИЙ

ОДОБРЕНО УМС ИИКС

Протокол № 8/1/2024

от 28.08.2024 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ЗАЩИЩЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ (PROTECTED INFORMATION SYSTEMS)

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, экз./зач./КР/КП
2	4	144	30	15	15		48	0	Э
Итого	4	144	30	15	15	0	48	0	

АННОТАЦИЯ

Дисциплина «Защищённые информационные системы (Protected Information Systems)» обеспечивает приобретение знаний и умений в соответствии с федеральным государственным образовательным стандартом, содействует формированию научного мировоззрения и системного мышления; посвящена изучению современных международных и российских стандартов обеспечения информационной безопасности, программно-аппаратных методов и средств защиты информации, критериев оценки обеспечения безопасности информационно-технологических систем и сетей.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью освоения учебной дисциплины (модуля) является изучение программно-аппаратных методов и средств защиты информации, современных руководящих документов и стандартов обеспечения информационной безопасности, критериев оценки обеспечения безопасности информационно-технологических систем и сетей.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Требования к «входным» знаниям, умениям и готовностям студента, необходимым при освоении данной дисциплины и приобретенным в результате освоения предшествующих дисциплин (модулей):

знание математических и физических основ защиты информации;

знание технических и экономических основ защиты информации;

знание иностранного языка в объеме, позволяющем читать оригинальные материалы по специальности;

знание основных принципов и особенностей функционирования автоматизированных систем обработки информации.

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 обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	З-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	З-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
УК-2 [1] – Способен управлять проектом на всех этапах его жизненного цикла	З-УК-2 [1] – Знать: этапы жизненного цикла проекта; этапы разработки и реализации проекта; методы разработки и управления проектами У-УК-2 [1] – Уметь: разрабатывать проект с учетом анализа альтернативных вариантов его реализации, определять целевые этапы, основные направления работ; объяснить цели и сформулировать задачи, связанные с подготовкой и реализацией проекта; управлять проектом на всех этапах его жизненного цикла В-УК-2 [1] – Владеть: методиками разработки и управления проектом; методами оценки потребности в ресурсах и эффективности проекта
УК-6 [1] – Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	З-УК-6 [1] – Знать: методики самооценки, самоконтроля и саморазвития с использованием подходов здоровьесбережения У-УК-6 [1] – Уметь: решать задачи собственного личностного и профессионального развития, определять и реализовывать приоритеты совершенствования собственной деятельности; применять методики самооценки и самоконтроля; применять методики, позволяющие улучшить и сохранить здоровье в процессе жизнедеятельности В-УК-6 [1] – Владеть: технологиями и навыками управления своей познавательной деятельностью и ее совершенствования на основе самооценки, самоконтроля и принципов самообразования в течение всей жизни, в том числе с использованием здоровьесберегающих подходов и методик

Профессиональные компетенции в соотвествии 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**
проектный			
Проектирование систем обеспечения информационной безопасности (СОИБ) конкретных объектов на стадиях разработки, эксплуатации и модернизации	Средства и технологии обеспечения безопасности значимых объектов критической информационной инфраструктуры	ПК-1 [1] - Способен принимать участие в разработке систем обеспечения ИБ или информационно-аналитических систем безопасности *Основание:* Профессиональный стандарт: 06.030, 06.032, 06.033, 06.034	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, 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 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).
Проектирование систем обеспечения информационной безопасности (СОИБ) конкретных объектов на стадиях разработки, эксплуатации и модернизации	Средства и технологии обеспечения безопасности значимых объектов критической информационной инфраструктуры	ПК-2 [1] - Способен разрабатывать технические задания на проектирование систем обеспечения ИБ или информационно-аналитических систем безопасности *Основание:* Профессиональный стандарт: 06.032, 06.033, 06.034	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 защиты информации; современные информационные технологии

			(операционные системы, базы данных, вычислительные сети); методы контроля защищенности информации от несанкционированного доступа и специальных программных воздействий; 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 воздействий на нее; проводить испытания программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее.; В-ПК-2[1] - Владеть: основами выполнения анализа защищенности 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 средств защиты информации от несанкционированного доступа и специальных воздействий на нее.
педагогический			
Выполнение учебной и методической работы в образовательных организациях среднего профессионального образования, высшего образования и дополнительного профессионального образования (ДПО) по дополнительным профессиональным	Методы и средства проектирования, моделирования и экспериментальной отработки систем, средств и технологий обеспечения информационной безопасности значимых объектов критической информационной инфраструктуры; Образовательный процесс в области	ПК-6 [1] - Способен методически грамотно строить планы лекционных и практических занятий по разделам учебных дисциплин и публично излагать теоретические и практические разделы учебных дисциплин в соответствии с утвержденными учебно-методическими пособиями	З-ПК-6[1] - Знать: особенности организации образовательного процесса по программам бакалавриата и дпп; современные образовательные технологии профессионального образования; основы законодательства российской федерации об образовании и локальные нормативные акты,

программам (ДПП) в должностях преподавателя и ассистента по дисциплинам направления	обеспечения безопасности значимых объектов критической информационной инфраструктуры.	*Основание:* Профессиональный стандарт: 01.002	регламентирующие организацию образовательного процесса, проведение промежуточной и итоговой (итоговой государственной) аттестации обучающихся по программам бакалавриата и (или) дпп, ведение и порядок доступа к учебной и иной документации, в том числе документации, содержащей персональные данные. ; У-ПК-6[1] - Уметь: использовать педагогически обоснованные формы, методы и приемы организации деятельности обучающихся, применять современные технические средства обучения и образовательные технологии, в том числе при необходимости осуществлять электронное обучение, использовать дистанционные образовательные технологии, информационно-коммуникационные технологии, электронные образовательные и информационные ресурсы; контролировать соблюдение обучающимися на занятиях требований охраны труда; анализировать и устранять возможные риски жизни и здоровью обучающихся в учебном кабинете (лаборатории,

			ином учебном помещении); соблюдать требования охраны труда; использовать педагогически обоснованные формы, методы, способы и приемы организации контроля и оценки освоения учебного курса, дисциплины (модуля), образовательной программы, применять современные оценочные средства, обеспечивать объективность оценки, охрану жизни и здоровья обучающихся в процессе публичного представления результатов оценивания: -соблюдать предусмотренную процедуру контроля и методику оценки; - соблюдать нормы педагогической этики, устанавливать педагогически целесообразные взаимоотношения с обучающимися для обеспечения. ; В-ПК-6[1] - Владеть: проведением учебных занятий по программам бакалавриата и (или) дпп; организацией самостоятельной работы обучающихся по программам бакалавриата и дпп.

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
	2 Семестр						
1	Первый раздел	1-8	15/8/8		25	КИ-8	З-ОПК-1, У-ОПК-1, В-ОПК-1, З-ОПК-2, У-ОПК-2, В-ОПК-2, З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-2, У-ПК-2, В-ПК-2, З-ПК-6, У-ПК-6, В-ПК-6, З-УК-2, У-УК-2, В-УК-2, З-УК-6, У-УК-6, В-УК-6
2	Второй раздел	9-15	15/7/7		25	КИ-15	З-ОПК-1, У-ОПК-1, В-ОПК-1, З-ОПК-2, У-ОПК-2, В-ОПК-2, З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-2, У-ПК-2, В-ПК-2, З-ПК-6, У-ПК-6, В-ПК-6, З-УК-2, У-УК-2, В-УК-2, З-УК-6, У-УК-6, В-УК-6
	Итого за 2 Семестр		30/15/15		50		

	Контрольные мероприятия за 2 Семестр				50	Э	З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-2, У-ПК-2, В-ПК-2, З-ПК-6, У-ПК-6, В-ПК-6, З-УК-2, У-УК-2, В-УК-2, З-УК-6, У-УК-6, В-УК-6, З-ОПК-1, У-ОПК-1, В-ОПК-1, З-ОПК-2, У-ОПК-2, В-ОПК-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
Э	Экзамен

КАЛЕНДАРНЫЙ ПЛАН

Недели	**Темы занятий / Содержание**	**Лек., час.**	**Пр./сем., час.**	**Лаб., час.**
	2 Семестр	30	15	15
1-8	**Первый раздел**	15	8	8
1 - 2	**Основные угрозы информационной безопасности. Понятие архитектуры безопасности. Архитектура безопасности ЭМВОС.** Почему необходимо защищаться? Источники и последствия реализации угроз информационной безопасности. Функция, способы и средства обеспечения ИБ. Архитектура безопасности ЭМВОС.	Всего аудиторных часов		
		4	2	2
		Онлайн		
		0	0	0
3 - 4	**Стандарты и концептуальные основы обеспечения безопасности открытых ИТС.** Концепции обеспечения безопасности открытых ИТС: вспомогательная информация, политики, способы, схемы и средства обеспечения безопасности, участники и роли процедур обеспечения безопасности. Аутентификация.	Всего аудиторных часов		
		4	2	2
		Онлайн		
		0	0	0

	Управление доступом. Неотказуемость. Конфиденциальность. Целостность. Аудит ИБ и системы оповещения об опасности. Обеспечение ключами.			
5 - 6	**Основы аутентификации.** Основные понятия. Информация, необходимая для аутентификации. Политики аутентификации. Участники и роли в процедурах аутентификации. Способы и схемы аутентификации. Средства аутентификации.	Всего аудиторных часов		
		4	2	2
		Онлайн		
		0	0	0
7 - 8	**Основы управления доступом.** Основные понятия. Информация, необходимая для УД. Политики УД. Участники и роли в процедурах УД. Способы и схемы УД. Средства УД.	Всего аудиторных часов		
		3	2	2
		Онлайн		
		0	0	0
9-15	**Второй раздел**	15	7	7
9	**Основы обеспечения неотказуемости.** Основные понятия. Информация, необходимая для обеспечения неотказуемости. Политики обеспечения неотказуемости. Участники и роли в процедурах обеспечения неотказуемости. Способы обеспечения неотказуемости. Средства обеспечения неотказуемости.	Всего аудиторных часов		
		4	2	2
		Онлайн		
		0	0	0
10 - 11	**Основы обеспечения конфиденциальности.** Основные понятия. Информация, необходимая для обеспечения конфиденциальности. Политики обеспечения конфиденциальности. Участники и роли в процедурах обеспечения конфиденциальности. Способы обеспечения конфиденциальности. Средства обеспечения конфиденциальности.	Всего аудиторных часов		
		4	2	2
		Онлайн		
		0	0	0
11 - 12	**Основы обеспечения целостности.** Основные понятия. Информация, необходимая для обеспечения целостности. Политики обеспечения целостности. Участники и роли в процедурах обеспечения целостности. Способы обеспечения целостности. Средства обеспечения целостности.	Всего аудиторных часов		
		2	2	2
		Онлайн		
		0	0	0
13	**Основы аудита ИБ и систем оповещения об опасности.** Основные понятия. Информация, необходимая для аудита ИБ. Политики проведения аудита ИБ. Участники и роли в процедурах аудита ИБ. Способы и схемы проведения аудита ИБ. Средства проведения аудита ИБ и оповещения об опасности. Системы оповещения об опасности.	Всего аудиторных часов		
		2	1	1
		Онлайн		
		0	0	0
14 - 15	**Основы обеспечения ключами.** Основные понятия. Общая модель, на основе которой строятся способы обеспечения ключами. Основные концепций обеспечения ключами. Характеристик служб по обеспечению ключами. Единые принципы обеспечения ключевой информацией в течение её жизненного цикла. Концептуальная модель распределения ключей. Сертификаты открытых ключей.	Всего аудиторных часов		
		3	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

ТЕМЫ ЛАБОРАТОРНЫХ РАБОТ

Недели	**Темы занятий / Содержание**
	2 Семестр
	1. Основные угрозы информационной безопасности. Понятие архитектуры безопасности. Архитектура безопасности ЭМВОС. Функция, способы и средства обеспечения ИБ. Архитектура безопасности ЭМВОС.
	2. Стандарты и концептуальные основы обеспечения безопасности открытых ИТС. Концепции обеспечения безопасности открытых ИТС: вспомогательная информация, политики, способы, схемы и средства обеспечения безопасности, участники и роли процедур обеспечения безопасности.
	3. Основы аутентификации. Способы и схемы аутентификации. Средства аутентификации.
	4. Основы управления доступом. Способы и схемы УД. Средства УД.
	5. Основы обеспечения неотказуемости. Способы обеспечения неотказуемости.
	6. Основы обеспечения конфиденциальности. Способы обеспечения конфиденциальности. Средства обеспечения конфиденциальности.
	7. Основы обеспечения целостности. Способы обеспечения целостности. Средства обеспечения целостности.
	8. Основы аудита ИБ и систем оповещения об опасности. Способы и схемы проведения аудита ИБ. Средства проведения аудита ИБ и оповещения об опасности. Системы оповещения об опасности.
	9. Основы обеспечения ключами. Концептуальная модель распределения ключей. Сертификаты открытых ключей.

ТЕМЫ СЕМИНАРОВ

Недели	**Темы занятий / Содержание**
	2 Семестр
1 - 8	**Темы 1-6** 1. Основные угрозы информационной безопасности. Понятие архитектуры безопасности. Архитектура безопасности ЭМВОС. Вопросы: Почему необходимо защищаться? Источники и последствия реализации угроз информационной безопасности. Функция, способы и средства обеспечения ИБ. Архитектура безопасности ЭМВОС. 2. Стандарты и концептуальные основы обеспечения безопасности открытых ИТС. Вопросы: Концепции обеспечения безопасности открытых ИТС: вспомогательная информация,

	политики, способы, схемы и средства обеспечения безопасности, участники и роли процедур обеспечения безопасности. Аутентификация. Управление доступом. Неотказуемость. Конфиденциальность. Целостность. Аудит ИБ и системы оповещения об опасности. Обеспечение ключами. 3. Основы аутентификации. Вопросы: Основные понятия. Информация, необходимая для аутентификации. Политики аутентификации. Участники и роли в процедурах аутентификации. Способы и схемы аутентификации. Средства аутентификации. 4. Основы управления доступом. Вопросы: Основные понятия. Информация, необходимая для УД. Политики УД. Участники и роли в процедурах УД. Способы и схемы УД. Средства УД. 5. Основы обеспечения неотказуемости. Вопросы: Основные понятия. Информация, необходимая для обеспечения неотказуемости. Политики обеспечения неотказуемости. Участники и роли в процедурах обеспечения неотказуемости. Способы обеспечения неотказуемости. Средства обеспечения неотказуемости. 6. Основы обеспечения конфиденциальности. Вопросы: Основные понятия. Информация, необходимая для обеспечения конфиденциальности. Политики обеспечения конфиденциальности. Участники и роли в процедурах обеспечения конфиденциальности. Способы обеспечения конфиденциальности. Средства обеспечения конфиденциальности.
9 - 15	**Темы 7-9** 7. Основы обеспечения целостности. Вопросы: Основные понятия. Информация, необходимая для обеспечения целостности. Политики обеспечения целостности. Участники и роли в процедурах обеспечения целостности. Способы обеспечения целостности. Средства обеспечения целостности. 8. Основы аудита ИБ и систем оповещения об опасности. Вопросы: Основные понятия. Информация, необходимая для аудита ИБ. Политики проведения аудита ИБ. Участники и роли в процедурах аудита ИБ. Способы и схемы проведения аудита ИБ. Средства проведения аудита ИБ и оповещения об опасности. Системы оповещения об опасности. 9. Основы обеспечения ключами. Вопросы: Основные понятия. Общая модель, на основе которой строятся способы обеспечения ключами. Основные концепций обеспечения ключами. Характеристик служб по обеспечению ключами. Единые принципы обеспечения ключевой информацией в течение её жизненного цикла. Концептуальная модель распределения ключей. Сертификаты открытых ключей.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Лекции (с визуализацией) по выбраному направлению, семинарские занятия, раздаточные материалы, лабораторные работы.

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)**
ОПК-1	З-ОПК-1	Э, КИ-8, КИ-15
	У-ОПК-1	Э, КИ-8, КИ-15
	В-ОПК-1	Э, КИ-8, КИ-15
ОПК-2	З-ОПК-2	Э, КИ-8, КИ-15
	У-ОПК-2	Э, КИ-8, КИ-15
	В-ОПК-2	Э, КИ-8, КИ-15
ПК-1	З-ПК-1	Э, КИ-8, КИ-15
	У-ПК-1	Э, КИ-8, КИ-15
	В-ПК-1	Э, КИ-8, КИ-15
ПК-2	З-ПК-2	Э, КИ-8, КИ-15
	У-ПК-2	Э, КИ-8, КИ-15
	В-ПК-2	Э, КИ-8, КИ-15
ПК-6	З-ПК-6	Э, КИ-8, КИ-15
	У-ПК-6	Э, КИ-8, КИ-15
	В-ПК-6	Э, КИ-8, КИ-15
УК-2	З-УК-2	Э, КИ-8, КИ-15
	У-УК-2	Э, КИ-8, КИ-15
	В-УК-2	Э, КИ-8, КИ-15
УК-6	З-УК-6	Э, КИ-8, КИ-15
	У-УК-6	Э, КИ-8, КИ-15
	В-УК-6	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 – *«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.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. 004 М48 Информационная безопасность открытых систем : учебник, Мельников Д.А., Москва: Флинта, 2013

2. 004 И74 Информационная безопасность открытых систем Т.1 Угрозы, уязвимости, атаки и подходы к защите, , : Горячая линия - Телеком, 2006

3. 004 И74 Информационная безопасность открытых систем Т.2 Средства защиты в сетях, , Москва: Горячая линия-Телеком, 2008

4. ЭИ Ф 76 Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов, Фомичёв В. М., Москва: Юрайт, 2022

5. ЭИ Ф 76 Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для вузов, Фомичёв В. М., Москва: Юрайт, 2022

6. 0 Ф 76 Криптографические методы защиты информации Ч.1. Математические аспекты , Фомичев В.М., Москва: Юрайт, 2019

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

Дисциплина имеет интегративный характер и включает в себя знания и умения, получаемые студентами в ходе реализации учебных программ раздела Государственного образовательного стандарта высшего профессионального образования.

Данная дисциплина направлена на теоретико-практическую подготовку студентов к работе в качестве специалиста по защите информации. Преподавание дисциплины предполагает проведение лекций и лабораторных занятий. Лекции проводятся в основном посредством метода устного изложения с элементами проблемного подхода и беседы (на основе обсуждения практических ситуаций из реального процесса профессионального обучения). В лекционном курсе главное место отводится общетеоретическим проблемам, выяснению особенностей применения принципов применительно к изучению различных проблем защиты информации.

Вузовская лекция – главное звено дидактического цикла обучения. Её цель – формирование у студентов ориентировочной основы для последующего усвоения материала методом самостоятельной работы. Содержание лекции должно отвечать следующим дидактическим требованиям:

изложение материала от простого к сложному, от известного к неизвестному;

логичность, четкость и ясность в изложении материала;

возможность проблемного изложения, дискуссии, диалога с целью активизации деятельности студентов;

опора смысловой части лекции на подлинные факты, события, явления, статистические данные;

тесная связь теоретических положений и выводов с практикой и будущей профессиональной деятельностью студентов.

Перед началом чтения дисциплины приводится график учебного процесса и самостоятельной работы и обоснование сроков выполнения всех видов аудиторных занятий и самостоятельной работы.

Преподаватель, читающий лекционные курсы в вузе, должен знать существующие в педагогической науке и используемые на практике варианты лекций, их дидактические и воспитывающие возможности, а также их методическое место в структуре процесса обучения.

При изложении материала важно помнить, что почти половина информации на лекции передается через интонацию. Учитывать тот факт, что первый кризис внимания студентов наступает на 15-20-й минутах, второй – на 30-35-й минутах. В профессиональном общении

исходить из того, что восприятие лекций студентами младших и старших курсов существенно отличается по готовности и умению.

Задания по самостоятельной работе включают:

конспектирование лекций, первоисточников и другой учебной литературы;

проработку учебного материала (по конспектам лекций, учебной и научной литературе);

работу с нормативными документами;

выполнение домашнего задания.

Домашнее задание является видом самостоятельной работы студентов, выдается после изложения теоретического материала на лекциях.

При выдаче заданий для самостоятельной работы определяются предельные сроки их выполнения и сдачи.

Проверка качества усвоения знаний в течение семестра осуществляется в устной форме, путем обсуждения проблем и письменной, путем выполнения студентами домашнего задания и лабораторных заданий, связанных с практическим освоением содержания дисциплины.

Студенты демонстрируют в рамках проверки умение анализировать значимость и выявлять специфику содержания дисциплины и ее компонентов, работу с учебной и методической литературой. Текущая проверка знаний и умений студентов также осуществляется через организацию фронтального письменного опроса по пройденному материалу на основе тестов. Предусмотрено и осуществляется обязательное тестирование студентов после освоения ими половины объема и полного объема материала дисциплины (в середине и в конце семестра).

Итоговая аттестация по дисциплине предполагает зачет, на котором проверяется: усвоение теоретического материала дисциплины, усвоение базовых понятий дисциплины, умение использовать полученные знания для решения практических задач на лабораторных занятиях. При проведении аттестации студентов важно всегда помнить, что систематичность, объективность, аргументированность –главные принципы, на которых основаны контроль и оценка знаний студентов. Проверка, контроль и оценка знаний студента, требуют учета его индивидуального стиля в осуществлении учебной деятельности. В качестве критериев оценки знаний используются результаты промежуточного контроля по тестам, выполнения домашнего задания, посещаемости занятий, выполнения лабораторных и сдачи зачета.

Оценка работы студентов осуществляется в ходе разбора конкретных ситуаций воздействия вредоносного программного обеспечения на основе компьютерных симуляций и контроля выполнения лабораторных работ. Итоговый контроль разделов проводится по тестам и опросу по вопросам.

Аттестация по разделам:

К8, КИ16 - максим.балл-25, мин. балл – 15. Раздел считается аттестованным при получении оценки не ниже минимальной по каждой контрольной работе и выполнении всех лабораторных работ раздела.

При не аттестации хотя бы по одному из разделов, студент не допускается к экзамену.

Студент:

1. Предоставляет конспекты или доклады по темам, которые были пропущены;

2. Отвечают на один вопрос из списка вопросов к экзамену.

Оценка не зачтено ставится, если студент не смог продемонстрировать ключевые знания и навыки по данной дисциплине.

Оценка зачтено ставится:

если студент продемонстрировал ключевые знания и навыки, но не смог продемонстрировать углубленное понимание взаимосвязей между основными понятиями по данной дисциплине, что может выражаться в неуверенном ответе на вопросы преподавателя;

если студент продемонстрировал ключевые знания и навыки, продемонстрировал углубленное понимание взаимосвязей между основными понятиями дисциплины, что может выражаться в уверенном ответе на вопросы преподавателя, но не смог сразу разъяснить особенности взаимосвязи между изучаемыми в данной дисциплине;

если студент продемонстрировал ключевые знания и навыки, продемонстрировал углубленное понимание взаимосвязей между основными понятиями и смог разъяснить особенности взаимосвязи между изучаемыми в данной дисциплине законами и моделями переноса нейтронов, что может выражаться в уверенных ответах на дополнительные вопросы преподавателя.

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

Средства обеспечения освоения учебного курса

При изучении дисциплины рекомендуется использовать следующие средства обучения:

программу учебного курса:

рекомендуемую основную и дополнительную литературу;

методические указания, пособия и учебники (в бумажном виде);

задания для самостоятельной работы для закрепления теоретического материала;

план практических занятий;

методическое обеспечение текущего и итогового контроля знаний.

Со стороны преподавателя должен быть установлен контакт со студентами, и они должны быть информированы о порядке прохождения курса, его особенностях, учебно-методическом обеспечение 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 и самостоятельной работе.

Основные формы изучения дисциплины

Курс читается во втором семестре.

Принципы отбора содержания и организации учебного материала дисциплины

Учебный курс строится на интегративной основе и включает в себя как теоретические знания, так и практические навыки, получаемые студентами во время практических занятий и самостоятельной работы.

В данной дисциплине заложен деятельностный компонент, наиболее ярко проявляющийся при выполнении небольших заданий на каждом из занятий (во время чтения лекций), а также в рамках самостоятельной работы (домашних заданий), выдаваемых преподавателем каждому студенту.

Содержание дисциплины распределяется между лекционной и практической частями на основе принципа дополняемости: практические занятия, как правило, не дублируют лекции и носят ярко выраженный творческий характер.

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 основной литературе;

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

подготовку к практическим занятиям по тем разделам, которые не дублируют темы лекционной части, а потому предполагают самостоятельную проработку материала учебных пособий.

Преподавание дисциплины предполагает проведение ряда лекционных и практических занятий. Лекции проводятся в основном посредством метода устного изложения с элементами проблемного подхода и беседы (на основе обсуждения практических ситуаций из реального процесса управления защитой информации). Практические занятия проводятся для студентов в 8 семестре в форме круглого стола, выбираемые темы корректируются преподавателем в зависимости от интересов студентов и изменяющейся направленности деятельности в условиях формирования информационного общества.

Подготовка преподавателя к лекциям

При подготовке к конкретным занятиям преподавателю следует помнить, что вузовская лекция – главное звено дидактического цикла обучения. Её цель – формирование у студентов ориентировочной основы для последующего усвоения материала методом самостоятельной работы. Содержание лекции должно отвечать следующим дидактическим требованиям:

изложение материала от простого к сложному, от известного к неизвестному;

логичность, четкость и ясность в изложении материала;

возможность проблемного изложения, дискуссии, диалога с целью активизации деятельности студентов;

опора смысловой части лекции на подлинные факты, события, явления, статистические данные;

тесная связь теоретических положений и выводов с практикой и будущей профессиональной деятельностью студентов.

При изложении материала преподавателю важно помнить, что почти половина информации на лекции передается через интонацию. Учитывать тот факт, что первый кризис внимания студентов наступает на 15-20-й минутах, второй – на 30-35-й минутах. В профессиональном общении исходить из того, что восприятие лекций студентами младших и старших курсов существенно отличается по готовности и умению.

Преподаватель, читающий лекционные курсы, должен знать существующие в педагогической науке и используемые на практике варианты лекций, их дидактические и воспитывающие

Автор(ы):

Евсеев Владимир Леонович, к.т.н., доцент

Рецензент(ы):
Горбатов