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 № УМС-575/01-1

от 30.08.2021 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ЗАЩИТА ИНФОРМАЦИОННЫХ ПРОЦЕССОВ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

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**
1	3	108	8	0	24		40	0	Э
Итого	3	108	8	0	24	2	40	0	

АННОТАЦИЯ

Изучение дисциплины «Защита информационных процессов в компьютерных системах» предполагает изучение основных понятий, принципов и особенностей технологий обеспечения информационной безопасности объектов.

Дисциплина «Защита информационных процессов в компьютерных системах» реализует требования Федерального государственного образовательного стандарта (ФГОС3++) по специальности 10.04.01 «Информационная безопасность» (квалификация (степень) выпускника «Магистр») и содействует формированию у студентов профессиональных компетенций, необходимых для решения задач, относящихся к определенному виду профессиональной деятельности.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Курс занимает важное место в общей системе профильной подготовки выпускника, являясь своего рода мостом, связывающим общенаучные и общеобразовательные дисциплины с профильными для будущего специалиста курсами.

В свою очередь дисциплина обеспечивает необходимую подготовку студентов для выполнения проектирования.

Целью освоения учебной дисциплины «Защита информационных процессов в компьютерных системах»» является формирование общих представлений и знаний в области построения систем информационной безопасности с использованием технических средст, освоение дисциплинарных компетенций, связанных с раскрытием базовых и расширенных технологий информационной безопасности сложных технических объектов и систем.

Задачи изучения дисциплины:

- изучение основных положений, понятий и категорий, относящихся к базовым и расширенным технологиям информационной безопасности сложных технических объектов и систем;

– изучение основы правовых, организационно-распорядительных, нормативных и информационных документов в области информационных технологий, средств защиты информации и безопасности;

- изучение принципов организации, комплексного подхода к выбору средств и технологий обеспечения информационной безопасности объектов защиты;

- изучение принципов работы технических средств и определение критериев защищенности охраняемого объекта;

- освоение механизмов защиты объектов;

- формирование правильного подхода к проблемам информационной безопасности объектов.

Таким образом, дисциплина «Защита информационных процессов в компьютерных системах» является неотъемлемой составной частью профессиональной подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность». Вместе с другими дисциплинами общенаучного и профессионального циклов дисциплин 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

Данная учебная дисциплина входит в базовую часть профессионального модуля ООП «Обеспечение безопасности значимых объектов критической информационной инфраструктуры» ОС НИЯУ МИФИ 10.04.01 «Информационная безопасность».

В процессе изучения дисциплины студенты получают возможность последовательно рассмотреть технологии и систему построения защищенных автоматизированных систем и её основные элементы и др. От студентов требуется знание основ защиты информации. Дисциплина «Защита информационных процессов в компьютерных системах» относится к числу дисциплин специализации «Обеспечение безопасности значимых объектов критической информационной инфраструктуры».

Для усвоения учебной дисциплины «Защита информационных процессов в компьютерных системах» студенты должны знать следующие дисциплины: «Общая алгебра»; «Математический анализ»; «Линейная алгебра»; «Теория вероятностей и математическая статистика»; «Дискретная математика»; «Информатика»; «Теория информации».

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
УК-4 [1] – Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	З-УК-4 [1] – Знать: правила и закономерности личной и деловой устной и письменной коммуникации; современные коммуникативные технологии на русском и иностранном языках; существующие профессиональные сообщества для профессионального взаимодействия В-УК-4 [1] – Владеть: методикой межличностного делового общения на русском и иностранном языках, с применением профессиональных языковых форм, средств и современных коммуникативных технологий У-УК-4 [1] – Уметь: применять на практике коммуникативные технологии, методы и способы делового общения для академического и профессионального взаимодействия

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;**	**Код и наименование индикатора достижения профессиональной**

		Основание (профессиональный стандарт-ПС, анализ опыта)	**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 иди 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.

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
	1 Семестр						
1	Информационные процессы в компьютерных системах	1-8	4/0/12		25	КИ-8	З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-2, У-ПК-2, В-

							ПК-2, З-УК-4, У-УК-4, В-УК-4
2	Методы и средства защиты информационных процессов в компьютерных системах	9-16	4/0/12		25	КИ-16	З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-2, У-ПК-2, В-ПК-2, З-УК-4, У-УК-4, В-УК-4
	Итого за 1 Семестр		8/0/24		50		
	Контрольные мероприятия за 1 Семестр				50	Э	З-ПК-1, У-ПК-1, В-ПК-1, З-ПК-2, У-ПК-2, В-ПК-2, З-УК-4, У-УК-4, В-УК-4

* – 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.
	1 Семестр	8	0	24
1-8	**Информационные процессы в компьютерных системах**	4	0	12
1	**Тема 1. Общие вопросы построения и безопасности информационных систем** Введение. О современных проблемах информационной безопасности. Пример построения онтологии в области защиты информации. Основные положения теории информационно-психологического воздействия. Использование теории графов для проектирования стратегических задач виртуального предприятия. Основы технологий поисковой оптимизации сайта для обеспечения его продвижения и защиты информации. Вопросы безопасности в Интернете вещей. Построение сетей связи специального назначения на основе технологий программно-конфигурируемых сетей.	Всего аудиторных часов 1 Онлайн 0	 0 0	 0 0
1	**Тема 2. Правовые основы защиты информации и информационных процессов в компьютерных системах** Структура государственной системы правового регулирования информационной безопасности (ИБ) в Российской Федерации (РФ). Правовые и нормативные акты, квалифицирующие информационные компьютерные преступления. Понятие информационной безопасности. Понятие и свойства информации. Законодательство об информационных правонарушениях в РФ. Классификация компьютерных систем. Объекты защиты в персональных компьютерах и компьютерных системах.	Всего аудиторных часов 1 Онлайн 0	 0 0	 0 0
2	**Тема 3. Анализ потенциальных угроз безопасности информационных (УИБ) процессов в компьютерных системах** Постановка задачи анализа потенциальных угроз. Случайные угрозы. Преднамеренные угрозы. Анализ электромагнитных излучений и наводок в компьютерных системах. Характеристики излучения протоколов обмена. Анализ спектра излучения протоколов обмена. Анализ спектра излучений наводок оборудованием компьютерной системы.	Всего аудиторных часов 1 Онлайн 0	 0 0	 0 0
2	**Тема 4. Анализ и оценка прочности защиты информации и информационнных процессов в компьютерных** Основы теории защиты информационнных процессов от несанкционирован-ного доступа (НСД). Модель поведения потенциального нарушителя. Модель защиты информационнного процесса. Концептуальные основы построения защиты информационнных процессов от НСД.	Всего аудиторных часов 1 Онлайн 0	 0 0	 0 0

	Оценка эффективности автоматизированных средств управления защитой информации в компьютерных система.			
3 - 4	**Лабораторная работа №1** Исследование уязвимости обхода взаимной аутентификации в компьютерных сетях	Всего аудиторных часов		
		0	0	4
		Онлайн		
		0	0	0
5 - 6	**Лабораторная работа №2** Исследование уязвимостей баз	Всего аудиторных часов		
		0	0	4
		Онлайн		
		0	0	0
7 - 8	**Лабораторная работа №3** Исследование веб-уязвимостей	Всего аудиторных часов		
		0	0	4
		Онлайн		
		0	0	0
9-16	**Методы и средства защиты информационных процессов в компьютерных системах**	4	0	12
9	**Тема 5. Оценка эффективности систем защиты информации и анализ рисков информационной безопасности** Метод категорирования информационных активов по требованиям безопасности информации (анализ иерархий и класстерный анализ). Модели управления информационными рисками в системах условного доступа. Оценка рисков безопасности локальной сети с применением технологий нечеткого моделирования. Оценка эффективности комплексной системы защиты информации и инфраструктуры защиты информации.	Всего аудиторных часов		
		1	0	0
		Онлайн		
		0	0	0
9	**Тема 6. Методы защиты информационных процессов в компьютерных системах** Инженерно-технические методы защиты информационнных процессов. Пассивные методы инженерно-технические защиты информационнных процессов. Активные методы инженерно-технические защиты информационнных процессов. Программно-аппаратные методы защиты информационнных процессов.	Всего аудиторных часов		
		1	0	0
		Онлайн		
		0	0	0
10	**Основные способы защиты информации и информационных процессов в КС** Защита информации от утечки. Защита информации от несанкционированного воздействия. Защита информации от непреднамеренного воздействия. Защита информации от разглашения. Защита информации от несанкционированного доступа. Защита информации от преднамеренного воздействия. Защита информации от [иностранной] разведки.	Всего аудиторных часов		
		1	0	0
		Онлайн		
		0	0	0
10	**Тема 8. Средства защиты информации и информационных процессов в компьютерных системах** Распределение средств защиты информации и информационных процессов в компьютерных сетях. Распределение средств защиты в модели взаимосвязи открытых систем. Программно-аппаратные средства защиты информации и информационных процессов.	Всего аудиторных часов		
		1	0	0
		Онлайн		
		0	0	0

	Основы построения программно-аппаратных средств защиты информации. Технические средства программно-аппаратной защиты информационных процессов.			
11 - 12	**Лабораторная работа №4** Изучение программ для тестирования безопасности веб-приложений	Всего аудиторных часов		
		0	0	4
		Онлайн		
		0	0	0
12 - 13	**Лабораторная работа №5** Изучение встроенных инструментов для исследования сетевых инфраструктур и мониторинга ИБ в компьютерных сетях	Всего аудиторных часов		
		0	0	4
		Онлайн		
		0	0	0
14 - 15	**Лабораторная работа №6** Основы проектирования структуры баз данных	Всего аудиторных часов		
		0	0	4
		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**
	1 Семестр
3 - 4	**Лабораторная работа №1** Исследование уязвимости обхода взаимной аутентификации в компьютерных сетях
5 - 6	**Лабораторная работа №2** Исследование уязвимостей баз
7 - 8	**Лабораторная работа №3** Исследование веб-уязвимостей
11 - 12	**Лабораторная работа №4** Изучение программ для тестирования безопасности веб-приложений
13 - 14	**Лабораторная работа №5** Изучение встроенных инструментов для исследования
15 - 16	**Лабораторная работа №6** Основы проектирования структуры баз данных

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Цель обучения достигается сочетанием применения традиционных и инновационных педагогических технологий, направленных на развитие познавательной активности, творческой самостоятельности студентов.

В соответствии с целью формирования и развития профессиональных навыков студентов и требованиями ОС ВО по направлению подготовки реализация компетентностного подхода предусматривает в учебном процессе широкое использование активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой.

Цель обучения достигается сочетанием применения традиционных и инновационных педагогических технологий, направленных на развитие познавательной активности, творческой самостоятельности студентов. Последовательное и целенаправленное выдвижение перед студентом познавательных задач, решая которые студенты активно усваивают знания. Поисковые методы; постановка познавательных задач. С целью формирования и развития профессиональных навыков студентов в дисциплине используются активные и интерактивные формы проведения занятий: лабораторные работы и доклады и презентации с их обсуждением в сочетании с внеаудиторной работой. В соответствии со спецификой ВУЗа в процессе преподавания дисциплины методически целесообразно в каждом разделе выделить наиболее важные темы и акцентировать на них внимание обучаемых. В рамках дисциплины предусмотрены встречи с представителями государственных и общественных организаций, мастер-классы экспертов и специалистов в области технологий обеспечения ИБ, а также российских и зарубежных компаний – разработчиками средств обеспечения ИБ.

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-1	З-ПК-1	Э, КИ-8, КИ-16
	В-ПК-1	Э, КИ-8, КИ-16
	У-ПК-1	Э, КИ-8, КИ-16
ПК-2	З-ПК-2	Э, КИ-8, КИ-16
	У-ПК-2	Э, КИ-8, КИ-16
	В-ПК-2	Э, КИ-8, КИ-16
УК-4	З-УК-4	Э, КИ-8, КИ-16
	В-УК-4	Э, КИ-8, КИ-16
	У-УК-4	Э, 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:

<table>
<tr><th>Сумма баллов</th><th>Оценка по 4-ех балльной шкале</th><th>Оценка ECTS</th><th>Требования к уровню освоению учебной дисциплины</th></tr>
<tr><td>90-100</td><td>5 – «отлично»</td><td>A</td><td>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.</td></tr>
<tr><td>85-89</td><td rowspan="3">4 – «хорошо»</td><td>B</td><td rowspan="3">Оценка «хорошо» выставляется студенту, если он твёрдо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.</td></tr>
<tr><td>75-84</td><td>C</td></tr>
<tr><td>70-74</td><td rowspan="2">D</td></tr>
<tr><td>65-69</td><td rowspan="2">3 – «удовлетворительно»</td><td rowspan="2">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.</td></tr>
<tr><td>60-64</td><td>E</td></tr>
<tr><td>Ниже 60</td><td>2 – «неудовлетворительно»</td><td>F</td><td>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.</td></tr>
</table>

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОСНОВНАЯ ЛИТЕРАТУРА:

1. 004 М 60 Управление инцидентами информационной безопасности и непрерывностью бизнеса Кн.3 , Москва: Горячая линия - Телеком, 2017

2. 004 М 60 Управление рисками информационной безопасности Кн.2 , Москва: Горячая линия - Телеком, 2017

3. 004 Ц 75 Цифровые технологии в системе управления "Умными городами" : Научно-аналитический сборник, Москва: Научный консультант, 2022

4. 004 И74 Информационная безопасность открытых систем Т.2 Средства защиты в сетях, , Москва: Горячая линия-Телеком, 2008

5. 004 М21 Основы теории защиты информации : конспект лекций, А. А. Малюк, Москва: МИФИ, 2004

6. 004 В24 Введение в информационную безопасность : учебное пособие для вузов, А. А. Малюк [и др.], Москва: Горячая линия - Телеком, 2013

7. 004 М21 Введение в защиту информации в автоматизированных системах : учебное пособие для вузов, А. А. Малюк, С. В. Пазизин, Н. С. Погожин, Москва: Горячая линия-Телеком, 2011

8. 004 М21 Информационная безопасность: концептуальные и методологические основы защиты информации : учеб. пособие для вузов, А.А. Малюк, Москва: Горячая линия - Телеком, 2004

9. 004 Г37 Основы защиты информации : Учебник для вузов, В. А. Герасименко, А. А. Малюк, М.: МИФИ, 1997

10. 004 О-75 Основы информационной безопасности автоматизированных банковских систем : Учеб. пособие, Курило А.П., Милославская Н.Г., Михайлов С.Ф., Толстой А.И., М.: МИФИ, 2001

11. 004 М60 Уязвимость и методы защиты в глобальной сети Internet : , Милославская Н.Г.,Тимофеев Ю.А.,Толстой А.И., М.: МИФИ, 1997

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

Специальное программное обеспечение не требуется

LMS И ИНТЕРНЕТ-РЕСУРСЫ:

1. Вузовские электронно-библиотечные системы учебной литературы ()

2. База научно-технической информации (например, ВИНИТИ РАН) ()

3. www.fstec.ru; www.gost.ru; www.fsb.ru. ()

4. http://www.scinet.cc ()

5. https://bit.spels.ru/index.php/bit ()

6. http://library.mephi.ru/ ()

https://online.mephi.ru/

http://library.mephi.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

1. специализированная учебная лаборатория: «Контроль защищенности ЛВС от НСД» ()

2. Специализированная учебная лаборатория: «Контроль защищенности ЛВС от НСД» ()

9. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ

Методические рекомендации студентам по изучению дисциплины «Защита информационных процессов в компьютерных системах»

Методические рекомендации по организации работы студента на лекциях

На лекционные занятия выносятся вопросы, усвоение которых требуется на уровне получения знаний. Во время лекции по дисциплине «Защита информационных процессов в компьютерных системах» студент должен уметь сконцентрировать внимание на рассматриваемых проблемах и включить в работу все виды памяти: словесную, образную и моторно-двигательную. Для этого ему необходимо конспектировать материал, излагаемый преподавателем. Во время конспектирования в работу включается моторно-двигательная память, позволяющая эффективно усвоить лекционный материал. Весь иллюстративный материал, представляемый на лекции (на слайдах, на доске, в раздаточном материале) также должен быть зафиксирован в конспекте лекций. Каждому студенту необходимо помнить о том, что конспектирование лекции – это не диктант. Студент должен уметь (или учиться уметь) выделять главное и фиксировать основные моменты «своими словами». Это гораздо более эффективно, чем запись «под диктовку».

На лекциях по дисциплине «Защита информационных процессов в компьютерных системах» периодически проводится письменный опрос (тестирование) студентов по материалам лекций. Подборка вопросов осуществляется на основе изученного теоретического материала. Такой подход позволяет не только контролировать уровень усвоения теоретического материала, но и организовать эффективный контроль посещаемости занятий на потоковых лекциях.

Методические рекомендации по организации работы студента в ходе лабораторных работ

На лабораторные работы выносятся вопросы, усвоение которых требуется на уровне навыков и умений. Цикл лабораторных работ по отработке практических навыков использования математических методов и программных средств криптографической защиты информации. Результаты, полученные в ходе лабораторных работ, используются студентами в качестве исходных данных при отработке итоговых пакетов документов.

В конце занятия преподаватель подводит его итоги, даёт оценку активности студентов и уровня их знаний полученных на лекциях и уровня их умений и навыков полученных в ходе подготовки, выполнения и защиты лабораторных работ.

Методические рекомендации по организации самостоятельной работы студента

Для эффективного достижения указанных выше целей обучения по дисциплине «Защита информационных процессов в компьютерных системах» процесс изучения материала курса предполагает достаточно интенсивную работу не только на лекциях и семинарах, но и с различными текстами и информационными ресурсами в ходе самостоятельной работы.

Самостоятельная работа по дисциплине «Защита информационных процессов в компьютерных системах» делится на аудиторную и внеаудиторную. Вопросы организации самостоятельной работы в ходе аудиторных занятий рассмотрены в предыдущих разделах предлагаемых методических рекомендаций. Поэтому рассмотрим процесс организации самостоятельной внеаудиторной работы студентов. Весь материал темы или отдельных ее вопросов, выносимых на самостоятельное изучение, разбивается на небольшие части. В конце каждой части приводятся вопросы для самоконтроля, отвечая на которые студент может проверить степень усвоения им изучаемого материала. Внеаудиторная самостоятельная работа включает также выполнение индивидуальных контрольных заданий. По результатам работы студента на всех занятиях и по результатам самостоятельной работы проставляется оценка в ведомость текущего контроля успеваемости и посещаемости студентов, а также передаются сведения в автоматизированную систему контроля самостоятельной и аудиторной работы студентов в Учебный Департамент НИЯУ «МИФИ».

Подготовка к экзамену и порядок его проведения

Итоговой формой контроля знаний студентов в семестре по дисциплине «Защита информационных процессов в компьютерных системах» является экзамен. Перед его проведением студенту необходимо восстановить в памяти теоретический материал по всем темам курса и не только. Для этого следует обратиться к соответствующим конспекту лекций, главам учебника и другим источникам.

Студент считается аттестванным (допущенным к экзамену, если по каждому из двух разделов набрал количество баллов не менее (зачетного минимума) 15 баллов и выполнил и защитил все лабораторные работы получив за каждую из них зачетный минимум (не менее 60 баллов).

Экзамен по курсу «Защита информационных процессов в компьютерных системах» может быть проведен в традиционной устной форме, но с обязательной записью основных формулировок по каждому вопросу в экзаменационном листе. Данный лист может служить документом при возникновении спорных ситуаций, и подаче студентом аппеляции. В качестве методической помощи студентам при подготовке к зачету рекомендуется перечень вопросов для подготовки к экзамену. Экзамен по курсу может быть проведен также в письменной форме: в форме письменных ответов на вопросы (на усмотрение преподавателя). Вопросы должны в обязательном порядке охватывать все дидактические единицы дисциплины «Защита информационных процессов в компьютерных системах». Форма проведения экзамена сообщается студентам на последних занятиях.

Итоговая оценка по дисциплине определяется суммарно из результата сдачи экзамена (не более 50 баллов) и суммы баллов, полученных по аттестации разделов (не более 50 баллов за все разделы).

Так итоговая оценка по дисциплине проставляется если студент в сумме набрал от 60-100 баллов. Неудовлетворительно - ниже 60 баллов.

Сумма баллов Оценка (ECTS) Градация

90 - 100 A отлично

85 - 89 B очень хорошо

75 - 84 C хорошо

70 - 74 D хорошо

65 - 69 D удовлетворительно

60 - 64 E удовлетворительно

Ниже 60 F неудовлетворительно

В основу разработки данной бально-рейтинговой системы положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется постоянно в процессе его обучения в университете. Настоящая система оценки успеваемости студентов основана на использовании совокупности контрольных точек, оптимально расположенных на всем временном интервале изучения дисциплины. При этом предполагается разделение всего курса на ряд более или менее самостоятельных, логически завершенных блоков и модулей и проведение по ним промежуточного контроля.

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

Методические рекомендации для преподавателя по организации изучения дисциплины «Защита информационных процессов в компьютерных системах»

Целью методических рекомендаций являются формирование теоретико-методологических знаний и закрепление профессиональных навыков в области построения, проектирования и создания защищенных автоматизированных систем, а также навыков и умения в применении знаний для конкретных условий.

Методологические подходы к изучению дисциплины «Защита информационных процессов в компьютерных системах»

- Направленность обучения на получение студентами качественных знаний, которые являются средством развития мышления и культуры, основой воспитания и поведения, будующего практического применения в различных сферах профессиональной деятельности.

- Реализация возможностей студентов в процессе выявления дискуссионных вопросов и комплексных проблем, определения взаимосвязей, анализа разнообразной информации.

- Развитие самостоятельности и способности принятия эффективных решений, определения выбора тех или иных действий с точки зрения их результативности.

Средства обеспечения освоения дисциплины «Защита информационных процессов в компьютерных системах»

Общий подход к реализации всего программного комплекса предполагает широкое использование активных методических форм преподавания материала.

Необходимо также обратить внимание на сочетание различных форм и методов обучения, включая лекционную форму подачи наиболее фундаментальных положений, изложение доступного материала в виде непрерывного диалога, проведение контроля, закрепляющих полученные теоретические знания посредством конкретных расчетов и принятия решений.

При изучении курса рекомендуется широко использовать наглядные пособия, презентации, фрагменты учебных кинофильмов по отдельным разделам дисциплины и обучающие программы.

Формы проведения учебных занятий:

• Практикумы (теоретические и практические задания в ходе проведения лекционных занятий).

• Ситуационные (творческие) задачи, вопросы для обсуждения (закрепление представлений учащихся об понятиях и принципах обеспечения безопасности (защищенности), навыков формирования конструктивных и конкретных вопросов).

• Тестовые задания (тестирование).

Педагогические функции преподавания дисциплины реализуются через совокупность педагогических приемов. В качестве основных можно выделить следующие:

- Дидактические (способность к передаче знаний в краткой и интересной форме, т. е. умение делать учебный материал доступным для студентов, опираясь на взаимосвязь теории и практики, учебного материала и реальной действительности).

- Рефлексивно-гностические (способность понимать студентов, базирующаяся на интересе к ним и личной наблюдательности; самостоятельный и творческий склад мышления; находчивость или быстрая и точная ориентировка).

- Интерактивно-коммуникативные (педагогически волевое влияние на студентов, требовательность, педагогический такт, организаторские способности, необходимые как для обеспечения работы самого преподавателя, так и для создания хорошего психологического климата в учебной группе).

- Речевые (содержательность, яркость, образность и убедительность речи преподавателя; способность ясно и четко выражать свои мысли и чувства с помощью речи, а также мимики и жестов).

Материально-техническое обеспечение дисциплины «Защита информационных процессов в компьютерных системах»

При выполнении заданий, самостоятельных работ и подготовке учебно-методических комплексов предусматривается обязательное применение ПК и обращение к сети Интернет.

Методические рекомендации по организации изучения дисциплины «Защита информационных процессов в компьютерных системах»

Методически обосновано изучать дисциплину в аудитории на лекциях, практических занятиях и в ходе проведения лабораторных работ.

Целесообразно для увеличения времени проработки важных тем предусмотреть рассмотрение отдельных вопросов в форме дискуссий и диспутов, на конференциях. Кроме того, необходимо предусмотреть дополнительные консультации по сложным темам.

В качестве форм промежуточного контроля полученных знаний (раздел 1 и 2) используются: контрольная работа и тестирование. Для повышения результатов контроля студентами (по их желанию) могут быть выполнены и использованы письменные работы (рефераты). В процессе итогового контроля также могут использоваться результаты, полученные студентами при выполнении самостоятельной подготовки.

Студент считается аттестванным (допущенным к экзамену, если по каждому из двух разделов набрал количество баллов не менее (зачетного минимума) 15 баллов и выполнил и защитил все лабораторные работы получив за каждую из них зачетный минимум (не менее 60 баллов).

Автор(ы):

Гавдан Григорий Петрович

Рецензент(ы):

Дураковский А.П.