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

ОСНОВЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

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	2	72	16	16	0		40	0	3
Итого	2	72	16	16	0	12	40	0	

АННОТАЦИЯ

Изучение дисциплины «Основы технической защиты конфиденциальной информации» предполагает изучение основных понятий, принципов и особенностей технической защиты конфиденциальной информации и основ противодействию создания каналов утечки информации.

Дисциплина «Основы технической защиты конфиденциальной информации» обеспечивает приобретение знаний и умений в соответствии с федеральным государственным образовательным стандартом (ФГОС3++), содействует формированию научного мировоззрения и системного мышления; посвящена изучению основных разделов физики, участвующих в процессе переноса информации с помощью технических средств и методам противодействия созданию каналов утечки информации.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целью освоения учебной дисциплины «Основы технической защиты конфиденциальной информации»» является формирование общих представлений о методах технической защиты конфиденциальной информации, лежащих в основе обеспечения информационной безопасности и особенностей каналов утечки информации.

Задачи дисциплины – дать основы правовых, организационно-распорядительных, нормативных и информационных документов в области технической защиты конфиденциальной информации (ТЗКИ); порядка выявления утечки информации по техническим каналам; практической отработки методик проведения специальных исследований основных технических систем и средств информации (ОТСС) в соответствии с методологией исследований защищенности средств и систем на соответствие требованиям по безопасности информации.

В результате обучения студенты должны ознакомиться с:

- с разновидностями технических каналов утечки информации и методах противодействия созданию каналов утечки информации;
- физическими явлениями, обуславливающими возможные технические каналы утечки информации;
- устройствами и принципами функционирования защищенных АС и СЗИ;
- критериями и методами оценки защищенности АС;

В результате изучения дисциплины студенты должны

иметь представление:

- о перспективных направлениях развития теории компьютерной безопасности и методах противодействия созданию каналов утечки информации;
- о методах анализа угроз информации, архитектуре защищенных АС;
- о принципах построения защищенных систем и типичных атаках на защищенные АС;

знать:

- угрозы и методы нарушения безопасности АС и методы противодействия созданию каналов утечки информации;
- формальные модели, лежащие в основе систем защиты АС от утечки по техническим каналам,
- методы и средства реализации защищенных АС,
- методы и средства верификации и анализа надежности защищенных АС;

уметь:

- реализовывать системы защиты информации в АС;
- осуществлять выбор средств верификации и анализа надежности защищенных АС

владеть:

- навыками использования критериев оценки защищенности АС от утечки по техническим каналам;
- навыками построения формальных моделей систем защиты информации АС от утечки по техническим каналам.

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.

Значительное место отведено методам оценки соответствия средств защиты информации, защищенности автоматизированных систем и методам противодействия созданию каналов утечки информации с помощью технических средств, которым в современных технологиях уделяется повышенное внимание в процессе переноса информации.

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 «Основы технической защиты конфиденциальной информации» относится к числу дисциплин специализации «Обеспечение безопасности значимых объектов критической информационной инфраструктуры».

Для усвоения учебной дисциплины «Основы технической защиты конфиденциальной информации» студенты должны знать следующие дисциплины: «Общая алгебра»; «Математический анализ»; «Линейная алгебра»; «Теория вероятностей и математическая статистика»; «Дискретная математика»; «Информатика»; «Теория информации».

Требования к «входным» знаниям, умениям и готовностям студента, необходимым при освоении данной дисциплины:

- знать потенциальные угрозы безопасности информации за счет технических каналов утечки информации;
- уметь использовать математический аппарат теории вероятностей и дискретной математики;
- владеть основами электротехники и радиотехники.

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
УК-1 [1] – Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	З-УК-1 [1] – Знать: методы системного и критического анализа; методики разработки стратегии действий для выявления и решения проблемной ситуации У-УК-1 [1] – Уметь: применять методы системного подхода и критического анализа проблемных ситуаций; разрабатывать стратегию действий, принимать конкретные решения для ее реализации В-УК-1 [1] – Владеть: методологией системного и критического анализа проблемных ситуаций; методиками постановки цели, определения способов ее достижения, разработки стратегий действий

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	Глава 1. Концепция технической защиты информации. Системный подход. Глава 2. Теоретические основы технической защиты информации	1-8	8/8/0		25	КИ-8	З-УК-1, У-УК-1, В-УК-1
2	Глава 3. Методы и средства добывания и защиты информации. Глава 4. Защита информации от несанкционированного доступа (НСД). Методы и средства контроля эффективности защиты информации	9-16	8/8/0		25	КИ-16	З-УК-1, У-УК-1, В-УК-1
	Итого за 1 Семестр		16/16/0		50		

	Контрольные мероприятия за 1 Семестр				50	З	З-УК-1, У-УК-1, В-УК-1

* – сокращенное наименование формы контроля

** – сумма максимальных баллов должна быть равна 100 за семестр, включая зачет и (или) экзамен

Сокращение наименований форм текущего контроля и аттестации разделов:

Обозначение	**Полное наименование**
КИ	Контроль по итогам
З	Зачет

КАЛЕНДАРНЫЙ ПЛАН

Недели	**Темы занятий / Содержание**	**Лек., час.**	**Пр./сем., час.**	**Лаб., час.**
	1 Семестр	16	16	0
1-8	**Глава 1. Концепция технической защиты информации. Системный подход. Глава 2. Теоретические основы технической защиты информации**	8	8	0
1 - 2	**Глава 1. Концепция технической защиты информации. Системный подход.** Ведение в дисциплину. Физические основы образования технических каналов утечки информации (ТКУИ). Основы прикладной акустики. Основы теории электромагнитного поля (ЭМП). Основы оптики. Цели и задачи технической защиты конфиденциальной информации (ТКЗИ). Основные понятия, термины и определения в области ТКЗИ. Защищаемая информация и информационные ресурсы. Государственная система защиты информации в РФ. Основные задачи ТЗКИ. Защищаемая информация и информационный ресурс. Информационные ресурсы, находящиеся в введении органов государственной власти и организаций.	Всего аудиторных часов 2 Онлайн 0	 2 0	 0 0
3 - 4	**Глава 1. Концепция технической защиты информации. Системный подход.** Сущность системного подхода. Угрозы безопасности. Модель нарушителей информационной безопасности на объекте. Модель угроз информационной безопасности на объекте. Область интересов и методы коммерческой разведки. Эффективность защиты безопасности информации. Базовые принципы технической защиты информации. Основные принципы построения системы защиты информации (СЗИ). Виды контролируемых зон. Типовые зоны и рубежи организации. Требования к защищаемым помещениям, где циркулирует конфиденциальная информации. Организация защиты информации. Характеристика защищаемой информации (ЗИ). Виды защищаемой информации. Классификация и	Всего аудиторных часов 2 Онлайн 0	 2 0	 0 0

	виды демаскирующих признаков объектов защиты, сигналов и веществ. Источники и носители информации. Характеристика угроз безопасности информации. Типовые причины возникновения канала несанкционированного доступа. Источники угроз безопасности информации.			
5 - 6	**Глава 2. Теоретические основы технической защиты информации.** Технические каналы утечки информации (ТКУИ). Особенности утечки информации. Типовая структура и виды ТКУИ. Основные показатели ТКУИ. Комплексное использование ТКУИ. Акустические каналы утечки информации. Оптические каналы утечки информации. Радиоэлектронные каналы утечки информации. Вещественные каналы утечки информации. Побочные электромагнитные излучения и наводки (ПЭМИН). Побочные преобразования акустических сигналов в электрические сигналы. Паразитные связи и наводки. НЧ и ВЧ излучения технических средств. Электромагнитные излучения сосредоточенных источников. Электромагнитные излучения распределенных источников. Утечка информации по цепям электропитания и заземления.	Всего аудиторных часов		
		2	2	0
		Онлайн		
		0	0	0
7 - 8	**Глава 2. Теоретические основы технической защиты информации.** Методы добывания информации. Основные принципы разведки. Классификация технической разведки. Технология добывания информации. Способы доступа органов добывания к источникам информации. Показатели эффективности добывания информации. Методы технической (инженерной) защиты конфиденциальной информации. Факторы обеспечения защиты информации от угроз воздействия. Факторы обеспечения защиты информации от угроз утечки информации. Классификация методов технической защиты информации. Категорирование объектов защиты. Характеристика методов физической защиты информации	Всего аудиторных часов		
		2	2	0
		Онлайн		
		0	0	0
9-16	**Глава 3. Методы и средства добывания и защиты информации. Глава 4. Защита информации от несанкционированного доступа (НСД). Методы и средства контроля эффективности защиты информации**	8	8	0
9 - 10	**Глава 3. Методы и средства добывания и защиты информации.** Методы противодействия наблюдению и подслушиванию. Обнаружение и подавление закладных устройств. Способы контроля помещений на отсутствие закладных устройств. Методы предотвращения несанкционированной записи речевой информации на диктофон. Методы подавления опасных сигналов акустоэлектрических преобразователей. Экранирование побочных излучений и наводок. Предотвращение утечки информации по цепям электропитания и заземления. Методы предотвращения	Всего аудиторных часов		
		2	2	0
		Онлайн		
		0	0	0

	утечки информации по вещественному каналу. Структура системы технической разведки. Классификация технических средств добывания информации. Возможности средств технической разведки. Технические средства подслушивания. Средства скрытного наблюдения. Средства перехвата сигналов. Средства добывания информации о радиоактивных веществах.			
11 - 12	**Глава 3. Методы и средства добывания и защиты информации.** Система ТЗКИ. Структура системы ТЗКИ. Подсистема физической защиты источников информации. Подсистема ТЗКИ от ее утечки. Управление силами и средствами системы ТЗКИ. Классификация средств ТЗИ. Средства инженерной защиты и технической охраны объектов. Ограждения территории. Ограждения зданий и помещений. Двери и ворота. Окна. Металлические шкафы, сейфы и хранилища. Средства систем контроля и управления доступом. Средства обнаружения злоумышленников и пожара. Извещатели. Средства контроля и управления средствами охраны. Средства телевизионной охраны. Средства освещения. Средства нейтрализации угроз.	Всего аудиторных часов		
		2	2	0
		Онлайн		
		0	0	0
13 - 14	**Глава 3. Методы и средства добывания и защиты информации.** Лицензирование деятельности (ЗИ) и ответственность за правонарушения. Организационно-правовые основы лицензирования деятельности в области ЗИ. Ответственность за правонарушения в области ЗИ. Планирование работ по ТЗИ. Порядок разработки, согласования и утверждения планов мероприятий по ТЗИ. Сертификация средств защиты информации. Общий порядок сертификации СЗИ. Порядок сертификации продукции, используемой в целях ЗИ (конфиденциальной). Аттестация объектов информатизации по требованиям безопасности информации. Порядок проведения аттестации ОИ по требованиям безопасности информации. Программы и методики аттестационных испытаний. Заключение по результатам аттестации ОИ. Аттестат соответствия объекта информатизации.	Всего аудиторных часов		
		2	2	0
		Онлайн		
		0	0	0
15 - 16	**Глава 4. Защита информации от несанкционированного доступа. Методы и средства контроля эффективности защиты информации.** Общая характеристика и классификация мер и средств ЗИ от НСД. Защита информации на АРМ-ах на базе автономных ПЭВМ. Защита информации в локальных вычислительных сетях. Защита информации при межсетевом взаимодействии. Защита информации при работе с системами управления базами данных. Особенности реализации требований по ЗИ при взаимодействии абонентов с ИС ОП. Основные задачи контроля состояния технической защиты информации.	Всего аудиторных часов		
		2	2	0
		Онлайн		
		0	0	0

	Классификация видов контроля состояния ТЗИ (организационный и технический контроль). Системы документов по контролю состояния ТЗИ. Вопросы, подлежащие контролю состояния ТЗИ в организации. Методы и средства контроля ЗИ, обрабатываемой ТС, от утечки за счет ПЭМИН. Утечка по ТК: методы и средства контроля защищенности акустической (речевой) информации. Методы и средства контроля защищенности информации от несанкционированного доступа.			

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 ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Недели	**Темы занятий / Содержание**
	1 Семестр
1 - 2	**Глава 1. Концепция технической защиты информации. Системный подход.** Физические основы образования технических каналов утечки информации (ТКУИ). Основы прикладной акустики. Основы теории электромагнитного поля (ЭМП). Основы оптики. Цели и задачи технической защиты конфиденциальной информации (ТКЗИ). Защищаемая информация и информационные ресурсы. Государственная система защиты информации в РФ. Основные задачи ТЗКИ. Защищаемая информация и информационный ресурс. Информационные ресурсы, находящиеся в введении органов государственной власти и организаций.
3 - 4	**Глава 1. Концепция технической защиты информации. Системный подход.** Сущность системного подхода. Угрозы безопасности. Модель нарушителей и модель угроз информационной безопасности на объекте. Область интересов и методы коммерческой разведки. Эффективность защиты безопасности информации. Базовые принципы ТЗКИ. Основные принципы построения системы защиты информации. Организация защиты информации. Характеристика и виды защищаемой информации (ЗИ). Классификация и виды демаскирующих признаков объектов защиты, сигналов и веществ. Источники и носители информации. Типовые причины возникновения канала несанкционированного доступа. Источники угроз безопасности информации.
5 - 6	**Глава 2. Теоретические основы технической защиты информации.** Особенности утечки информации. Типовая структура и виды ТКУИ. Основные показатели ТКУИ. Комплексное использование ТКУИ. Акустические каналы утечки информации. Оптические каналы утечки информации. Радиоэлектронные каналы утечки информации. Вещественные каналы утечки информации. Побочные электромагнитные излучения и наводки (ПЭМИН). Побочные преобразования акустических сигналов в электрические сигналы. Паразитные связи и наводки. НЧ и ВЧ излучения технических средств. Электромагнитные излучения сосредоточенных и

	распределенных источников. Утечка информации по цепям электропитания и заземления.
7 - 8	**Глава 2. Теоретические основы технической защиты информации.** Методы добывания информации. Основные принципы разведки. Классификация технической разведки. Технология добывания информации. Способы доступа органов добывания к источникам информации. Показатели эффективности добывания информации. Методы технической (инженерной) защиты конфиденциальной информации. Факторы обеспечения защиты информации от угроз воздействия. Факторы обеспечения защиты информации от угроз утечки информации. Классификация методов ТЗКИ. Категорирование объектов защиты. Характеристика методов физической защиты информации
9 - 10	**Глава 3. Методы и средства добывания и защиты информации.** Методы противодействия наблюдению и подслушиванию. Обнаружение и подавление закладных устройств. Способы контроля помещений на отсутствие закладных устройств. Методы подавления опасных сигналов акустоэлектрических преобразователей. Экранирование побочных излучений и наводок. Предотвращение утечки информации по цепям электропитания и заземления. Методы предотвращения утечки информации по вещественному каналу. Структура системы технической разведки. Классификация технических средств добывания информации. Возможности средств технической разведки.
11 - 12	**Глава 3. Методы и средства добывания и защиты информации. Система и структура системы ТЗКИ.** Подсистема физической защиты источников информации. Подсистема ТЗКИ от ее утечки. Управление силами и средствами системы ТЗКИ. Классификация средств ТЗИ. Средства инженерной защиты и технической охраны объектов. Средства систем контроля и управления доступом. Средства обнаружения злоумышленников и пожара. Средства контроля и управления средствами охраны. Средства телевизионной охраны, освещения, нейтрализации угроз.
13 - 14	**Глава 3. Методы и средства добывания и защиты информации.** Лицензирование деятельности (ЗИ) и ответственность за правонарушения. Организационно-правовые основы лицензирования деятельности в области ЗИ. Ответственность за правонарушения в области ЗИ. Планирование работ по ТЗИ. Порядок разработки, согласования и утверждения планов мероприятий по ТЗИ. Сертификация средств защиты информации. Общий порядок сертификации СЗИ. Порядок сертификации продукции, используемой в целях ЗИ (конфиденциальной). Аттестация объектов информатизации по требованиям безопасности информации. Порядок проведения аттестации ОИ по требованиям безопасности информации.
15 - 16	**Глава 4. Защита информации от несанкционированного доступа. Методы и средства контроля эффективности защиты информации.** Общая характеристика и классификация мер и средств ЗИ от НСД. Защита информации на АРМ-ах на базе автономных ПЭВМ. Защита информации в локальных вычислительных сетях, при межсетевом взаимодействии и при работе с системами управления базами данных. Особенности реализации требований по ЗИ при взаимодействии абонентов с ИС ОП. Основные задачи контроля. Системы документов по контролю состояния ТЗИ. Вопросы, подлежащие контролю состояния ТЗИ в организации. Методы и средства контроля ЗИ, обрабатываемой ТС, от утечки за счет ПЭМИН. Утечка по ТК: методы и средства контроля защищенности акустической (речевой) информации. Методы и средства контроля защищенности информации от несанкционированного доступа.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В соответствии с целью формирования и развития профессиональных навыков студентов и требованиями ОС НИЯУ МИФИ 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.

В процессе изучения данной дисциплины необходимо использовать действующие правовые акты в области технической защиты конфиденциальной информации, организационно-распорядительные, нормативные и информационные документы ФСТЭК России, других уполномоченных органов государственной власти, а также соответствующие учебно-методические пособия по техническим каналам утечки информации, иллюстративный материал (презентации).

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)**
УК-1	З-УК-1	З, КИ-8, КИ-16
	У-УК-1	З, КИ-8, КИ-16
	В-УК-1	З, КИ-8, КИ-16

Шкалы оценки образовательных достижений

Шкала каждого контрольного мероприятия лежит в пределах от 0 до установленного максимального балла включительно. Итоговая аттестация по дисциплине оценивается по 100-балльной шкале и представляет собой сумму баллов, заработанных студентом при выполнении заданий в рамках текущего и промежуточного контроля.

Итоговая оценка выставляется в соответствии со следующей шкалой:

Сумма баллов	Оценка по 4-ех балльной шкале	Оценка ECTS	Требования к уровню освоению учебной дисциплины
90-100	5 – *«отлично»*	A	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой,

			использует в ответе материал монографической литературы.
85-89	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 Б90 Защита от утечки информации по техническим каналам : учеб. пособие, Кондратьев А.В., Бузов Г.А., Калинин С.В., М.: Горячая линия - Телеком, 2005

2. 004 Д84 Контроль защищенности речевой информации в помещениях. Аттестационные испытания вспомогательных технических средств и систем по требованиям безопасности информации : учебное пособие, Куницын И.В., Дураковский А.П., Лаврухин Ю.Н., Москва: НИЯУ МИФИ, 2015

3. ЭИ Д84 Оценка защищенности речевой информации Ч.1 Выявление акустических и вибрационных каналов утечки речевой информации, Дураковский А.П., Москва: НИЯУ МИФИ, 2015

4. ЭИ Д84 Оценка защищенности речевой информации Ч.2 Проведение инструментального контроля в канале низкочастотного акустоэлектрического преобразования, Дураковский А.П., Москва: НИЯУ МИФИ, 2015

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

Методические рекомендации студентам по изучению дисциплины «Основы технической защиты конфиденциальной информации»

Методические рекомендации по организации работы студента на лекциях

Во время лекции по дисциплине «Основы технической защиты конфиденциальной информации» 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 «Основы технической защиты конфиденциальной информации» 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 на практических занятиях

По курсу «Основы технической защиты конфиденциальной информации» важное место в учебном процессе занимают практические занятия, призванные закреплять полученные студентами теоретические знания.

Перед практическим занятием студенту необходимо восстановить в памяти теоретический материал по теме практического занятия. Для этого следует обратиться к соответствующим конспекту лекций, главам учебника, настоящим методическим указаниям.

Каждое занятие начинается с повторения теоретического материала по соответствующей теме. Студенты должны уметь чётко ответить на вопросы, поставленные преподавателем. По характеру ответов преподаватель делает вывод о том, насколько тот или иной студент готов к выполнению упражнений.

После такой проверки студентам предлагается выполнить соответствующие задания и задачи. Что касается типов задач, решаемых на практических занятиях, то это различные ситуационные задачи на усвоение студентами теоретического материала.

Порядок решения задач студентами может быть различным. Преподаватель может установить такой порядок, согласно которому каждый студент в отдельности самостоятельно решает задачу без обращения к каким – либо материалам или к преподавателю. Может быть использован и такой порядок решения задачи, когда предусматривается самостоятельное решение каждым студентом поставленной задачи с использованием конспектов, учебников и других методических и справочных материалов. При этом преподаватель обходит студентов, наблюдая за ходом решения и давая индивидуальные указания.

В конце занятия преподаватель подводит его итоги, даёт оценку активности студентов и уровня их знаний.

Методические рекомендации по организации самостоятельной работы студента

Для эффективного достижения указанных выше целей обучения по дисциплине «Основы технической защиты конфиденциальной информации» 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 «Основы технической защиты конфиденциальной информации» 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 практических занятиях 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 зачету и порядок его проведения

Итоговой формой контроля знаний студентов в семестре по дисциплине «Основы технической защиты конфиденциальной информации» является зачет. Перед проведением зачета студенту необходимо восстановить в памяти теоретический материал по всем темам курса. Для этого следует обратиться к соответствующим конспекту лекций, главам учебника и другим источникам. Зачет по курсу «Основы технической защиты конфиденциальной информации» может быть проведен в традиционной устной форме, но с обязательной записью основных формулировок по каждому вопросу в зачетном листе. Данный лист может служить документом при подаче аппеляции. В качестве методической помощи студентам при подготовке к зачету рекомендуется перечень вопросов для подготовки к зачету. Зачет 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 «Основы технической защиты конфиденциальной информации». Форма проведения зачета сообщается студентам на последних занятиях.

Зачет определяется на основе суммы баллов, полученных по всем разделам по результатам самостоятельной работы при условии, что студент по каждому виду набрал

количество баллов не менее зачетного минимума. Так зачет 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 «Основы технической защиты конфиденциальной информации»

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 «Основы технической защиты конфиденциальной информации»

- 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 «Основы технической защиты конфиденциальной информации»

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 практикумов, 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).

• Ситуационные (творческие) задачи, вопросы для обсуждения (закрепление представлений учащихся об экономических понятиях и явлениях, 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 экономической 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 «Основы технической защиты конфиденциальной информации»

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

Методические рекомендации по организации изучения дисциплины «Основы технической защиты конфиденциальной информации»

Методически обосновано изучать дисциплину в аудитории на лекциях и практических занятиях.

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 на практических занятиях.

При неаттестации хотя бы по одному из разделов, студент не допускается к зачету

Автор(ы):

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

Рецензент(ы):
Дураковский