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

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

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
3	3	108	8	24	0		40	0	Э
Итого	3	108	8	24	0	12	40	0	

АННОТАЦИЯ

Рабочая программа учебной дисциплины «Аудит информационной безопасности компьютерных систем» содержит описание целей освоения дисциплины, ее место в структуре ООП, ВО, формируемые в результате освоения дисциплины компетенции студента, структуру и содержание дисциплины, используемые во время освоения дисциплины образовательные технологии, оценочные средства для контроля успеваемости, учебно-методическое, информационное и материально-техническое обеспечение дисциплины.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целями освоения учебной дисциплины «Аудит информационной безопасности компьютерных систем» обеспечение требуемого уровня знаний, умений и навыков у студентов для организации и проведения работ по аудиту информационной безопасности компьютерных систем.

Задачами дисциплины являются:

дать основы правовых, организационно-распорядительных, нормативных и информационных документов в области технической защиты информации (ТЗИ); физических основ реализации угроз безопасности информации защищаемых помещений (ЗП) и порядка их выявления; практической отработки методик проведения специальных исследований ЗП в соответствии с методологией исследований защищенности помещений на соответствие требованиям по безопасности информации; организации и порядка проведения аттестации ЗП и отработки технических документов по результатам аттестационных испытаний.

В результате обучения студенты должны ознакомиться с:

концептуальными основами защиты информации в Российской Федерации и с содержанием документов, составляющих правовую основу ТЗИ;

системой организационно-распорядительных, нормативных и информационных документов ФСТЭК России и Ростехрегулирования, определяющих организацию, правила и порядок осуществления деятельности в области ТЗИ;

организацией лицензирования деятельности в области защиты информации, функциями участников системы лицензирования ФСТЭК России;

организацией сертификации средств защиты информации в системе сертификации ФСТЭК России №РОСС RU.0001.01.БИ00, функциями участников системы сертификации;

организацией контроля выполнения лицензионных требований и условий предприятиями-лицензиатами ФСТЭК России;

должны знать:

потенциальные угрозы безопасности информации, реализуемые на объектах информатизации и в автоматизированных (информационных) системах;

организационно-технические основы реализации угроз конфиденциальности, доступности и целостности информации ограниченного доступа;

физические основы возникновения технических каналов утечки информации при ее обработке на технических средствах;

организационно-технические основы реализации несанкционированного доступа к информации, циркулирующей в ЗП;

требования и рекомендации организационно-распорядительных и нормативных документов по обеспечению безопасности информации ограниченного доступа, а также

требования к форме и содержанию технических документов, разрабатываемых по результатам аттестации ЗП;

инструментальные, инструментально-расчетные и расчетные методы и процедуры выявления угроз безопасности информации для ЗП;

порядок организации защиты информации на предприятии, номенклатуру и требования к содержанию организационно-распорядительных документов внутреннего пользования предприятия;

номенклатуру и возможности технических, программно-технических и программ.

должны уметь:

проводить специальные исследования ЗП и аттестационные испытания ЗП по требованиям безопасности информации (БИ);

применять технические, программно-технические и программные средства контроля защищённости информации и средства оценки эффективности применяемых для ЗП средств защиты информации;

разрабатывать технические документы по результатам аттестационных испытаний ЗП;

должны владеть навыками:

выявления потенциальных угроз безопасности информации для ЗП;

применения расчётных, инструментально-расчетных и расчетных методов оценки защищённости информации, циркулирующей в ЗП;

разработки технических документов по результатам аттестационных испытаний ЗП по требованиям БИ.

Дисциплина «Основы аттестации защищаемых помещений» является неотъемлемой составной частью профессиональной подготовки магистров по образовательной программе подготовки «Обеспечение безопасности значимых объектов критической информационной инфраструктуры». Вместе с другими дисциплин специального цикла изучение данной дисциплины призвано вырабатывать такие качества, как:

строгость в суждениях,

творческое мышление,

организованность и работоспособность,

дисциплинированность,

самостоятельность и ответственность.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина «Аудит информационной безопасности компьютерных систем» относится к числу дисциплин специализации «Обеспечение безопасности значимых объектов критической информационной инфраструктуры».

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел хорошей физико-математической подготовкой, знаниями, умениями и навыками таких дисциплин, как «Физические основы технических каналов утечки информации», «Измерительная аппаратура анализа защищенности объектов», «Методы и средства контроля эффективности защиты информации от несанкционированного доступа», «Основы технической защиты конфиденциальной информации».

Знания, полученные при изучении дисциплины «Основы аттестации защищаемых помещений» являются базовыми, для дисциплин, входящих в вариативную часть профессионального цикла учебного плана подготовки магистров по направлению подготовки

10.04.01 «Информационная безопасность» по образовательной программе подготовки «Обеспечение безопасности значимых объектов критической информационной инфраструктуры».

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Универсальные и(или) общепрофессиональные компетенции:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции

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**
научно-исследовательский			
Анализ фундаментальных и прикладных проблем ИБ в условиях становления современного информационного общества; выполнение научных исследований в области ИБ; подготовка по результатам научных исследований отчетов, статей, докладов на научных конференциях	Фундаментальные и прикладные проблемы информационной безопасности; методы и средства проектирования, моделирования и экспериментальной отработки систем, средств и технологий обеспечения информационной безопасности значимых объектов критической информационной инфраструктуры	ПК-3 [1] - Способен самостоятельно ставить конкретные задачи научных исследований в области ИБ или информационно-аналитических систем безопасности и решать их с использованием новейшего отечественного и зарубежного опыта *Основание:* Профессиональный стандарт: 06.030	З-ПК-3[1] - Знать: руководящие и методические документы уполномоченных федеральных органов исполнительной власти, устанавливающие требования к организации и проведению аттестации и сертификационных испытаний средств и систем защиты сссэ от нсд, зткс; основные средства и способы обеспечения информационной безопасности, принципы построения средств и систем защиты сссэ от нсд, зткс; национальные, межгосударственные и международные стандарты,

			устанавливающие требования по защите информации, анализу защищенности сетей электросвязи и оценки рисков нарушения их информационной безопасности. ; У-ПК-3[1] - Уметь: организовывать сбор, обработку, анализ и систематизацию научно-технической информации, отечественного и зарубежного опыта по проблемам информационной безопасности сетей электросвязи.; В-ПК-3[1] - Владеть: организацией подготовки научно-технических отчетов, обзоров, публикаций по результатам выполненных исследований.

4. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Разделы учебной дисциплины, их объем, сроки изучения и формы контроля:

№ п.п	Наименование раздела учебной дисциплины	Недели	Лекции/ Практ. (семинары)/ Лабораторные работы, час.	Обязат. текущий контроль (форма*, неделя)	Максимальный балл за раздел**	Аттестация раздела (форма*, неделя)	Индикаторы освоения компетенции
	3 Семестр						
1	Раздел 1. Основы аудита информационной безопасности	1-8	4/12/0		25	КИ-8	З-ПК-3, У-ПК-3, В-ПК-3
2	Раздел 2. Аудит информационной безопасности	9-15	4/12/0		25	КИ-16	З-ПК-3, У-ПК-3, В-ПК-3
	Итого за 3 Семестр		8/24/0		50		
	Контрольные мероприятия за 3 Семестр				50	Э	З-ПК-3, У-ПК-3, В-ПК-3

* – 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.**
	3 Семестр	8	24	0
1-8	**Раздел 1. Основы аудита информационной безопасности**	4	12	0
1 - 2	**Тема 1. Основы кибербезопасности** Информационная безопасность как свойство. Угрозы информационной безопасности. Контрмеры. Управление информационной безопасность. Базовые линейки стандартов. Оценка соответствия по требованиям безопасности информации. Определение кибербезопасности. Специфические термины. Классификация атак. Понятие APT-атаки. Участники киберпротивоборства. Ключевые контрмеры. Международные законодательные нормативные акты.	Всего аудиторных часов 1 Онлайн 0	 2 0	 0 0
2 - 3	**Тема 2. Введение в тест на проникновение** Определение аудита. Нормативные требования. Классификация тестирования на проникновение. Понятие киберучений. Методические документы. Руководства по тестированию на проникновение. Сравнение и выбор руководства по тестированию на проникновение. Обзор полезные ресурсы по тематике. Обзор утилит. Введение в Metasploit Framework (Rapid7). Разбор типового теста на проникновение.	Всего аудиторных часов 1 Онлайн 0	 2 0	 0 0
3 - 4	**Тема 3. Поиск информации по открытым источникам** Определения и терминология, классификация сбора общей информации. Понятие разведки по открытым источникам. Поисковые системы. Техники на базе Google (Advance Google Hacking Techniques). Сбор информации через социальные сети, веб-порталы. Анализ следов электронной почты. Конкурентная разведка. Интернет-трафик компании. Регистрационная информация WHOIS. Данные по DNS. Зондирование сети. Обзор утилит.	Всего аудиторных часов 1 Онлайн 0	 2 0	 0 0
4 - 5	**Тема 4. Введение в сетевую безопасность.** Введение в сети. Модели сетевых коммуникаций. Классификации сетей. Стек протоколов TCP/IP. Протоколы прикладного. Протоколы транспортного уровня. Протоколы сетевого уровня. Протоколы	Всего аудиторных часов 1 Онлайн 0	 2 0	 0 0

	канального уровня. Понятие безопасного протокола. Классификация сетевых атак. Классификация сетевых средств защиты информации.			
5 - 6	**Тема 5. Технологии сканирования** Особенности протоколов 3 и 4 уровня. Зондирование сети. Сканирование портов. Техники скрытого сканирования. Утилиты сканирования. Введение в nmap. Контрмеры.	Всего аудиторных часов 0 Онлайн 0	2 0	0 0
7 - 8	**Тема 6. Инвентаризация ресурсов** Определение, систематизация. Методы и средства сбора информации. Захват баннеров. SMTP Enumeration. NetBIOS Enumeration. SNMP Enumeration. LDAP Enumeration. NTP Enumeration. Контрмеры	Всего аудиторных часов 0 Онлайн 0	2 0	0 0
9-15	**Раздел 2. Аудит информационной безопасности**	4	12	0
9 - 10	**Тема 7. Анализ защищенности** Таксономии и базы уязвимостей. Метрики оценки критичности уязвимостей. Обзор технологий сканирования уязвимостей. Выбор сканера уязвимостей. Введение в сканер уязвимостей Сканер-ВС. Управление уязвимостями. Руководство ФСТЭК России и НКЦКИ.	Всего аудиторных часов 1 Онлайн 0	2 0	0 0
10 - 11	**Тема 8. Парольная защита** Метрики паролей и политики парольной защиты. Подсистемы аутентификации ОС. Классификация атак на парольную защиту. Онлайн-атаки. Оффлайн-атаки. Обзор средств по аудиту парольной защиты.	Всего аудиторных часов 1 Онлайн 0	1 0	0 0
11 - 12	**Тема 9. Анализ трафика** Определения. Особенности протоколов канального уровня. Пассивный перехват. Активный перехват. Обзор атак на коммутаторы. Обзор средств. Контрмеры.	Всего аудиторных часов 1 Онлайн 0	2 0	0 0
12 - 13	**Тема 10. Социальная инженерия** Введение в социальную инженерию. Терминология. Концепции, фазы. Техники. Атаки, ориентированные на персонал. Атаки, использующие компьютерные платформы. Атаки, ориентированные мобильные приложения и сервисы. Обзор утилит. Контрмеры.	Всего аудиторных часов 1 Онлайн 0	1 0	0 0
13 - 14	**Тема 11. Аудит беспроводных сетей** Введение в беспроводные технологии и сети. Стандарты беспроводных сетей. Стандарты безопасности Wi-Fi. Механизмы безопасности Wi-Fi. Обзор угроз и типовых атак. Примеры инструментария.	Всего аудиторных часов 0 Онлайн 0	2 0	0 0
14 - 15	**Тема 12. Введение в криптографию** Понятийный аппарат. Элементарная и современная криптография. Симметричные алгоритмы. Ассиметричные алгоритмы. Криптографические приложения. Криптографические интернет-протоколы. Криптографические средства. Введение в криптографические атаки Понятие криптоанализа. Введение в криптографические атаки.	Всего аудиторных часов 0 Онлайн 0	2 0	0 0
15 - 16	**Тема 13. Введение программную безопасность** Понятие дефекта и уязвимости программного обеспечения. Таксономии и рейтинги. Разбор актуальных уязвимостей и атак на вебресурсы. Понятие статического и	Всего аудиторных часов 0 Онлайн 0	2 0	0 0

	динамического анализа.			

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**
	3 Семестр
1 - 2	**ПЗ №1. Сбор информации о доменах** Задание: Злоумышленники могут собирать информацию о сетевых доменах жертвы, которая может быть использована в ходе таргетинга. Информация о доменах и их свойствах может включать различные сведения, в том числе о том, каким доменом (доменами) владеет жертва, а также административные данные (например, имя, регистратор и т.д.) и более доступную информацию, такую как контакты (адреса электронной почты и номера телефонов), рабочие адреса и серверы имен.
3 - 4	**ПЗ №2. Запросы к DNS** Злоумышленники могут искать в данных DNS информацию о жертвах, которая может быть использована при проведении атак. Информация DNS может включать в себя различные сведения, в том числе зарегистрированные серверы имен, а также записи, определяющие адресацию поддоменов, почтовых серверов и других узлов жертвы.
5 - 6	**ПЗ №3. Запросы к сервису WHOIS** Злоумышленники могут искать в открытых данных WHOIS информацию о жертвах, которая может быть использована в процессе таргетинга. Данные WHOIS хранятся в региональных интернет-регистратурах (RIR), отвечающих за распределение и присвоение интернет-ресурсов, таких как доменные имена. Любой желающий может запросить на серверах WHOIS информацию о зарегистрированном домене, например, назначенные блоки IP-адресов, контактную информацию и DNS-серверы имен.
7 - 8	**ПЗ №4. Просмотр сертификатов** Злоумышленники могут искать в открытых цифровых сертификатах информацию о жертвах, которая может быть использована для целевой атаки. Цифровые сертификаты выдаются центром сертификации (ЦС) для криптографической проверки происхождения подписанного содержимого. Такие сертификаты, например, используемые для шифрования веб-трафика (HTTPS SSL/TLS), содержат информацию о зарегистрированной организации, например, ее название и местонахождение.
9 - 10	**ПЗ №5. Основные этапы проведения аттестации ЗП по требованиям безопасности информации.** Злоумышленники могут искать в общедоступных базах данных сканирования информацию о жертвах, которая может быть использована в ходе таргетинга. Различные онлайн-сервисы постоянно публикуют результаты

	сканирования/обследований Интернета, часто собирая такую информацию, как активные IP-адреса, имена хостов, открытые порты, сертификаты и даже баннеры серверов.
11 - 12	**ПЗ №6. Организация контроля защищенности информации ограниченного доступа на этапе эксплуатации защищаемого помещения** Злоумышленники могут собирать адреса электронной почты, которые могут быть использованы для таргетинга.
13 - 14	**ПЗ №7. Сбор информации об именах сотрудников организации** Злоумышленники могут собирать имена сотрудников, которые могут быть использованы для целеуказания. Имена сотрудников могут использоваться для получения адресов электронной почты, а также для проведения других разведывательных мероприятий и/или создания более правдоподобных приманок.
15 - 16	**ПЗ №8. Сбор информации о сотрудниках организации** Злоумышленники могут собирать учетные данные, которые могут быть использованы в процессе атаки. Учетные данные, собираемые злоумышленниками, могут быть непосредственно связаны с организацией-жертвой, или же они могут попытаться воспользоваться тенденцией использования пользователями одних и тех же паролей для личных и рабочих учетных записей.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

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 дисциплины "Аудит информационной безопасности компьютерных систем" необходимо использовать действующие правовые акты в области защиты информации, организационно-распорядительные, нормативные и информационные документы ФСТЭК России, других уполномоченных органов государственной власти, а также соответствующие учебно-методические пособия, иллюстративный материал (презентации).

На лекционных занятиях излагаются наиболее важные и сложные вопросы, являющиеся теоретической основой нормативных документов и практических действий по защите информации и аттестации защищаемых помещений по требованиям безопасности информации. Часть лекций может излагаться проблемным методом с привлечением студентов для решения сформулированной преподавателем проблемы. С целью текущего контроля знаний в ходе лекций могут использоваться различные приёмы тестирования.

На практические занятия выносятся вопросы, усвоение которых требуется на уровне навыков и умений. Практические занятия по аттестации защищаемых помещений по требованиям безопасности информации, обнаружению ТКУИ и отработке методического аппарата технического контроля проводятся по циклам на автоматизированных рабочих местах в специализированных лабораториях. На каждом рабочем месте должен быть преподаватель, развёрнуто необходимое оборудование технического контроля и средства имитации ТКУИ. Результаты используются студентами в качестве исходных данных при отработке итоговых пакетов документов.

В качестве форм промежуточного контроля полученных знаний могут быть использованы письменные работы (рефераты), собеседование, методы тестирования с

использованием компьютерных технологий. В процессе итогового контроля могут использоваться результаты, полученные студентами на лабораторных работах.

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-3	З-ПК-3	Э, КИ-8, КИ-16
	У-ПК-3	Э, КИ-8, КИ-16
	В-ПК-3	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</td></tr>
</table>

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

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

3. ЭИ Д84 Оценка защищенности речевой информации Ч.3 Проведение инструментального контроля в канале акустоэлектромагнитного преобразования, Дураковский А.П., Москва: НИЯУ МИФИ, 2018

4. ЭИ Д84 Оценка защищенности речевой информации Ч.4 Проведение инструментального контроля в канале высокочастотного навязывания, Дураковский А.П., Москва: НИЯУ МИФИ, 2018

5. ЭИ Д84 Оценка защищенности речевой информации Ч.5 Проведение инструментального контроля в канале высокочастотного облучения, Дураковский А.П., Москва: НИЯУ МИФИ, 2018

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

1. ЭИ А92 Аттестационные испытания автоматизированных систем от несанкционированного доступа по требованиям безопасности информации : учебное пособие, Дураковский А.П. [и др.], Москва: НИЯУ МИФИ, 2014

2. 004 А92 Аттестационные испытания автоматизированных систем от несанкционированного доступа по требованиям безопасности информации : учебное пособие, Дураковский А.П. [и др.], Москва: НИЯУ МИФИ, 2014

3. ЭИ К65 Контроль защищенности автоматизированных систем от несанкционированного доступа. Аттестационные испытания : лабораторный практикум, Дураковский А.П. [и др.], Москва: НИЯУ МИФИ, 2013

4. 004 К65 Контроль защищенности информации от утечки по техническим каналам за счет побочных электромагнитных излучений и наводок. Аттестационные испытания по требованиям

безопасности информации : учебное пособие, Чистяков М.С. [и др.], Москва: НИЯУ МИФИ, 2014

5. 004 К65 Контроль защищенности речевой информации в помещениях. Аттестационные испытания выделенных помещений по требованиям безопасности информации : учебное пособие, Куницын И.В. [и др.], Москва: НИЯУ МИФИ, 2014

6. ЭИ Д84 Оценка защищенности речевой информации Ч.3 Проведение инструментального контроля в канале высокочастотного акустоэлектрического преобразования, Дураковский А.П., Москва: НИЯУ МИФИ, 2015

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. ()

https://online.mephi.ru/

http://library.mephi.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

1. «Защита речевой информации от утечки за счет недостаточной звуко- и виброизоляции помещений (АВАК)»

2. «Защита информации от утечки по техническим каналам (ПЭМИН)»

9. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ СТУДЕНТОВ

Настоящие методические указания раскрывают рекомендуемый режим и характер учебной работы по изучению теоретических разделов курса, практическому применению изученного материала, по выполнению самостоятельной работы путем использования лекционного материала. Методические указания служат основой мотивации студента к самостоятельной работе и не подменяют рекомендуемую учебную литературу.

Данные указания определяют взаимосвязь курса с другими учебными дисциплинами образовательной программы, место курса в различных областях науки и техники, в том числе в области информационной безопасности.

Аттестация по разделам:

КР8, КР14 - максим.балл-25, мин. балл – 9. Раздел считается аттестованным при получении оценки не ниже минимальной по каждой контрольной работе и выполнении всех практических заданий раздела.

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

Особенности изучения разделов дисциплины

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

На лекционных занятиях излагаются наиболее важные и сложные вопросы, являющиеся теоретической основой нормативных документов и практических действий по защите информации и аттестации защищаемых помещений по требованиям безопасности информации. Часть лекций может излагаться проблемным методом с привлечением студентов для решения сформулированной преподавателем проблемы. С целью текущего контроля знаний в ходе лекций могут использоваться различные приёмы тестирования.

На практические занятия выносятся вопросы, усвоение которых требуется на уровне навыков и умений.

Практические занятия по Аудиту информационной безопасности компьютерных систем, обнаружению ТКУИ и отработке методического аппарата технического контроля проводятся по циклам на автоматизированных рабочих местах в специализированных лабораториях. На каждом рабочем месте должен быть преподаватель, развёрнуто необходимое оборудование технического контроля и средства имитации ТКУИ.

В качестве форм промежуточного контроля полученных знаний могут быть использованы письменные работы (рефераты), собеседование, методы тестирования с использованием компьютерных технологий. В процессе итогового контроля могут использоваться результаты, полученные студентами на лабораторных работах.

10. УЧЕБНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ

Настоящие методические указания раскрывают рекомендуемый режим и характер учебной работы по изучению теоретических разделов курса, практическому применению изученного материала, по выполнению самостоятельной работы путем использования лекционного материала. Методические указания служат основой мотивации студента к самостоятельной работе и не подменяют рекомендуемую учебную литературу.

Данные указания определяют взаимосвязь курса с другими учебными дисциплинами образовательной программы, место курса в различных областях науки и техники, в том числе в области информационной безопасности.

Аттестация по разделам:

КР8, КР14 - максим. балл-25, мин. балл – 9. Раздел считается аттестованным при получении оценки не ниже минимальной по каждой контрольной работе и выполнении всех лабораторных работ раздела.

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

1. Чтение лекций.

Первая лекция должна быть введением к дисциплине (разделу дисциплины, читаемому

в начинающемся семестре). Она должна содержать общий обзор содержания дисциплины. В ней следует отметить методические инновации в решении задач, рассматриваемых в дисциплине, дать перечень рекомендованной литературы и вновь появившихся литературных источников, обратив внимание студентов на обязательную и дополнительную литературу.

Изложению текущего лекционного материала должна предшествовать вводная часть, содержащая краткий перечень вопросов, рассмотренных на предыдущих лекциях. На этом этапе полезно задать несколько вопросов аудитории, осуществить выборочный контроль знания студентов.

При изложении лекционного материала следует поощрять вопросы непосредственно в процессе изложения, внимательно относясь к вопросам студентов и при необходимости давая дополнительные, более подробные пояснения.

При чтении лекций преимущественное внимание следует уделять качественным вопросам, опуская простые математические выкладки, либо рекомендуя выполнить их самим студентам, либо отсылая студентов к литературным источникам и методическим пособиям.

В процессе лекционного курса необходимо возможно чаще возвращаться к основным вопросам дисциплины, проводя выборочный экспресс-контроль знаний студентов.

Принятая преподавателем система обозначений должна чётко разъясняться в процессе её введения и использоваться в конспектах лекций

В лекциях, предшествующих практическим занятиям, следует кратко излагать содержание и основные задачи практического занятия, дать рекомендации студентам для подготовки к нему.

На последней лекции важно найти время для обзора основных положений, рассмотренных в дисциплине, перечню и формулировке вопросов, выносимых на экзамен или зачёт.

2. Указания по контролю самостоятельной работы студентов.

По усмотрению преподавателя задание на самостоятельную работу может быть индивидуальным или фронтальным.

При использовании индивидуальных заданий требовать от студента письменный отчет о проделанной работе, проводить его обсуждение.

При применении фронтальных заданий вести коллективные обсуждения со студентами основных теоретических положений.

С целью контроля качества выполнения самостоятельной работы требовать индивидуальные отчеты (допустимо вместо письменного отчета применять индивидуальные контрольные вопросы).

Автор(ы):

Марков Алексей Сергеевич

Рецензент(ы):

Горбатов В.С.