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

МЕТОДЫ И СРЕДСТВА КОНТРОЛЯ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Направление подготовки (специальность) [1] 10.04.01 Информационная безопасность

Семестр	**Трудоемкость, кред.**	**Общий объем курса, час.**	**Лекции, час.**	**Практич. занятия, час.**	**Лаборат. работы, час.**	**В форме практической подготовки/ В**	**СРС, час.**	**КСР, час.**	**Форма(ы) контроля, экз./зач./КР/КП**
2	2	72	8	0	22		42	0	З
3	3	108	8	0	24		40	0	Э
Итого	5	180	16	0	46	12	82	0	

АННОТАЦИЯ

Целью учебной дисциплины «Методы и средства контроля эффективности защиты информации от несанкционированного доступа» является обеспечение требуемого уровня знаний, умений и навыков у студентов для организации и проведения работ в области выбора и применения методов и средств контроля эффективности защиты информации в АС от несанкционированного доступа. При проведении аттестационных испытаний ОИ в части защиты от НСД помимо общего комплекса работ специалисты-эксперты должны обладать дополнительными углубленными умениями и практическими навыками по целому ряду направлений работ, причем, каждое из направлений работ предполагает решение ряда частных задач, требующих от специалиста-эксперта определенных умений и практических навыков, в том числе по применению специализированных программных средств.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целями освоения учебной дисциплины «Методы и средства контроля эффективности защиты информации от несанкционированного доступа» является обеспечение требуемого уровня знаний, умений и навыков у студентов для организации и проведения работ в области выбора и применения методов и средств контроля эффективности защиты информации в АС от несанкционированного доступа.

Задачами дисциплины являются:

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

В результате обучения студенты должны ознакомиться с системой организационно-распорядительных, нормативных и информационных документов ФСТЭК России и Ростехрегулирования, определяющих организацию, правила и порядок осуществления деятельности в области контроля эффективности защиты информации от несанкционированного доступа, организацией контроля выполнения лицензионных требований и условий предприятиями-лицензиатами ФСТЭК России, получить профессиональные компетенции для выполнения ими трудовых функций соответствующих профессиональных стандартов (Раздел 3).

Дисциплина «Методы и средства контроля эффективности защиты информации от несанкционированного доступа» 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 «Методы и средства контроля эффективности защиты информации от несанкционированного доступа» относится к числу дисциплин специализации «Обеспечение безопасности значимых объектов критической информационной инфраструктуры» (блок Б1.ДВ.2.7 РУП).

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел хорошей физико-математической подготовкой, знаниями, умениями и навыками смежных дисциплин «Основы технической защиты информации конфиденциальной информации», «Целенаправленные атаки на компьютерные системы», «Технологии обеспечения информационной безопасности объектов», «Основы криптографической защиты информации».

Знания, полученные при изучении дисциплины «Методы и средства контроля эффективности защиты информации от несанкционированного доступа» 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**
проектный			
Проектирование систем обеспечения информационной безопасности (СОИБ) конкретных объектов на стадиях разработки,	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	З-ПК-2[1] - Знать: формальные модели безопасности компьютерных систем и сетей; способы обнаружения и нейтрализации последствий вторжений в компьютерные

эксплуатации и модернизации		*Основание:* Профессиональный стандарт: 06.032, 06.033, 06.034	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.
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.
контрольно-аналитический			
Контроль защищенности ЗО КИИ по требованиям безопасности информации; аттестация ЗО КИИ по требованиям безопасности информации; проведение сертификационных испытаний средств защиты информации ЗО КИИ на соответствие требованиям по безопасности информации	Объекты информатизации, информационные ресурсы и информационные технологии, компьютерные, автоматизированные, телекоммуникационные, информационные и информационно-аналитические системы, обеспечивающие безопасность критических процессов значимых объектов критической информационной инфраструктуры	ПК-4 [1] - Способен участвовать в планировании и реализации процессов контроля ИБ или процессов информационно-аналитических систем безопасности *Основание:* Профессиональный стандарт: 06.032, 06.034	З-ПК-4[1] - Знать: методы и методики оценки безопасности программно-аппаратных средств защиты информации; принципы построения программно-аппаратных средств защиты информации; принципы построения подсистем защиты информации в компьютерных системах; методы и методики контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок; средства контроля защищенности информации от утечки за счет побочных электромагнитных излучений и наводок; средства контроля защищенности информации от несанкционированного доступа порядок аттестации объектов информатизации на соответствие требованиям по защите информации; способы

			организации работ при проведении сертификации программно-аппаратных средств защиты; нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и сертификации средств защиты информации на соответствие требованиям по безопасности информации. ; У-ПК-4[1] - Уметь: оценивать эффективность защиты информации; применять разработанные методики оценки защищенности программно-аппаратных средств защиты информации; оформлять материалы аттестационных испытаний (протоколов аттестационных испытаний и заключения по результатам аттестации объектов вычислительной техники на соответствие требованиям по защите информации); анализировать компьютерную систему с целью определения уровня защищенности и доверия; применять инструментальные средства проведения сертификационных испытаний;

			разрабатывать программы и методики сертификационных испытаний программных (программно-технических) средств защиты информации от несанкционированного доступа на соответствие требованиям по безопасности информации; проводить экспертизу технических и эксплуатационных документов на сертифицируемые программные (программно-технические) средства защиты информации от несанкционированного доступа и материалов сертификационных испытаний. ; В-ПК-4[1] - Владеть: определением уровня защищенности и доверия программно-аппаратных средств защиты информации; основами проведения аттестационных испытаний объектов вычислительной техники на соответствие требованиям по защите информации; основами проведения экспериментальных исследований уровней защищенности компьютерных систем и сетей; основами подготовки протоколов испытаний и технического заключения по результатам сертификационных

			испытаний программных (программно-технических) средств защиты информации от несанкционированного доступа на соответствие требованиям по безопасности информации; основами проведения экспертизы технических и эксплуатационных документов на сертифицируемые программные (программно-технические) средства защиты информации от несанкционированного доступа и материалов сертификационных испытаний.

4. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

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

№ п.п	Наименование раздела учебной дисциплины	Недели	Лекции/ Практ. (семинары)/ Лабораторные работы, час.	Обязат. текущий контроль (форма*, неделя)	Максимальный балл за раздел**	Аттестация раздела (форма*, неделя)	Индикаторы освоения компетенции
	2 Семестр						
1	Раздел 1. Основные рекомендации по защите информации ограниченного доступа от НСД.	1-8	4/0/10		25	КИ-8	З-ПК-2, У-ПК-2, У-ПК-3, З-ПК-4, У-ПК-4
2	Раздел 2. Основные направления и подсистемы защиты информации от НСД	9-15	4/0/12		25	КИ-15	З-ПК-2, У-ПК-2, З-ПК-

							3, У-ПК-3, З-ПК-4, У-ПК-4
	Итого за 2 Семестр		8/0/22		50		
	Контрольные мероприятия за 2 Семестр				50	З	З-ПК-2, У-ПК-2, З-ПК-3, У-ПК-3, З-ПК-4, У-ПК-4
	3 Семестр						
1	Раздел 1. Организация контроля прав доступа к объекту.	1-8	4/0/12		25	КИ-8	З-ПК-2, У-ПК-2, В-ПК-2, З-ПК-3, У-ПК-3, В-ПК-3, З-ПК-4, У-ПК-4, В-ПК-4
2	Раздел 2. Особенности аттестационных испытаний АС на соответствие требованиям по защите информации от НСД.	9-16	4/0/12		25	КИ-16	З-ПК-2, У-ПК-2, В-ПК-2, З-ПК-3, У-ПК-3, В-ПК-3, З-ПК-

							4, У-ПК-4, В-ПК-4
	Итого за 3 Семестр		8/0/24		50		
	Контрольные мероприятия за 3 Семестр				50	Э	З-ПК-2, У-ПК-2, В-ПК-2, З-ПК-3, У-ПК-3, В-ПК-3, З-ПК-4, У-ПК-4, В-ПК-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
З	Зачет
Э	Экзамен

КАЛЕНДАРНЫЙ ПЛАН

Недели	**Темы занятий / Содержание**	**Лек., час.**	**Пр./сем., час.**	**Лаб., час.**
	2 Семестр	8	0	22
1-8	**Раздел 1. Основные рекомендации по защите информации ограниченного доступа от НСД.**	4	0	10
1 - 2	**Тема 1. Порядок выявления угроз безопасности информации ограниченного доступа, обусловленных несанкционированным дост** Основные предпосылки реализации угроз безопасности информации ограниченного доступа, обрабатываемой с использованием автоматизированных систем различного уровня и назначения, обусловленных	Всего аудиторных часов 1 Онлайн 0	0 0	0 0

	несанкционированным доступом (НСД) к ней и специальными воздействиями на нее. Классификация угроз безопасности информации по результатам реализации НСД и специальных воздействий на нее. Принципы выявления угроз НСД к информации и специальных воздействий на нее в системах обработки информации. Анализ опасности угроз.			
3 - 4	**Тема 2. Система документов, определяющих требования, нормы, рекомендации по защите информации ограниченного доступа от НСД и специальных воздействий на информацию.** Нормативные документы ФСТЭК России по аттестации объектов информатизации и защите информации. Основные руководящие документы ФСТЭК России по критериям защищенности средств вычислительной техники и автоматизированных систем. Основные зарубежные стандарты по критериям защищенности информационных технологий. Средства контроля защищенности от НСД.	Всего аудиторных часов		
		1	0	4
		Онлайн		
		0	0	0
5 - 6	**Тема 3. Типы аттестуемых объектов информатизации. Защищаемые объекты информатизации.** Основные технические средства и системы. Вспомогательные технические средства и системы. Классификация АС. Классификация защищенности АС от НСД к информации. Типовое содержание аттестационных испытаний АС. Испытания АС на соответствие требованиям по защите информации от несанкционированного доступа. Проверка выполнения требований и рекомендаций по выбору и защите технических средств. Типовое содержание программы аттестационных испытаний. Основные факторы, определяющие содержание и объем аттестационных испытаний. Каналы утечки информации в средствах и системах информатизации.	Всего аудиторных часов		
		1	0	4
		Онлайн		
		0	0	0
7 - 8	**Тема 4. Особенности защиты информации от НСД и их реализации на различных типах аттестуемых объектов.** Защита автоматизированных систем от несанкционированного доступа к обрабатываемой информации. Классификация автоматизированных систем и требования по защите информации. Методы оценки защищенности автоматизированных систем от НСД к обрабатываемой информации. Методики оценки защищенности подсистемы управления доступом в автоматизированных системах (АС), подсистемы регистрации и учета в АС, криптографической подсистемы защиты информации, обрабатываемой в АС, подсистемы обеспечения целостности информации, обрабатываемой в АС.	Всего аудиторных часов		
		1	0	2
		Онлайн		
		0	0	0
9-15	**Раздел 2. Основные направления и подсистемы защиты информации от НСД**	4	0	12
9 - 10	**Тема 5. Программно-математическое воздействия и вредоносные программы.**	Всего аудиторных часов		
		1	0	2

	Понятие программно-математического воздействия и вредоносной программы. Классификация вредоносных программ. Деструктивные функции вредоносных программ и способы их реализации. Особенности программно-математического воздействия в сетях общего пользования.	Онлайн		
		0	0	0
11 - 12	**Тема 6. Основные подсистемы защиты.** Требования к подсистемам в зависимости от типов АС (АРМ, ЛВС). Классы защищенности и требования к подсистемам, в зависимости от класса защищенности. Руководящий документ: Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа. Характеристики автоматизированных систем (в отличие от СВТ). Классификация нарушителей по уровню возможностей, представляемых им штатными средствами АС и СВТ.	Всего аудиторных часов		
		1	0	4
		Онлайн		
		0	0	0
13 - 14	**Тема 6. Основные подсистемы защиты.** Основные способы НСД. Функции обеспечивающих средств для СРД. Руководящий документ: Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации. Подсистемы СЗИ НСД. Требования к сертификации СВТ для использования в АС.	Всего аудиторных часов		
		1	0	4
		Онлайн		
		0	0	0
15	**Тема 7. Поиск уязвимостей в составе и настройках системного и прикладного программного обеспечения.** Понятия: Уязвимость, эксплойт, полезная нагрузка. Уязвимости переполнения буфера. Уязвимости форматных строк. Межсайтовое выполнение вредоносного программного кода. Внедрение в запросы к базам данных. Размещение вредоносного программного кода по предсказуемому адресу. Уязвимости использования памяти после ее освобождения. Методы поиска уязвимостей. Контроль уязвимостей на уровне сети. Контроль уязвимостей на уровне операционных систем и прикладного ПО. Контроль уязвимостей на уровне системы управления базами данных. Контроль настроек механизмов обновления системного и прикладного. Контроль механизмов идентификации и аутентификации пользователей» при работе со средствами защиты информации (СЗИ) от НСД «Аккорд» и «Соболь», и программными продуктами «НКВД 2.2» и «НКВД 2.3».	Всего аудиторных часов		
		1	0	2
		Онлайн		
		0	0	0
	3 Семестр	8	0	24
1-8	**Раздел 1. Организация контроля прав доступа к объекту.**	4	0	12
1 - 2	**Тема 8. Проверка правильности идентификации объектов доступа.** Проверка осуществляется путем обращения к ним субъектов доступа по идентификаторам объектов. Обращение должно осуществляться однозначно только к данному объекту. Объекты доступа определяются в соответствии с РД «Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите	Всего аудиторных часов		
		1	0	4
		Онлайн		
		0	0	0

	информации» и Актом классификации АС.			
3 - 4	**Тема 9. Проверка правильности идентификации субъектов доступа.** Проверки при входе в систему путем обращения субъектов АС к объектам доступа при помощи штатных средств. Для чего системе предъявляются персональные идентификаторы? Предъявление идентификатора, незарегистрированного в системе (средства управления должны приостанавливать процесс предоставления доступа). Неоднократное предъявление идентификатора, незарегистрированного в системе (средства управления должны прекратить процесс предоставления доступа). Предъявление идентификатора, зарегистрированного в системе (процесс предоставления доступа должен быть продолжен).	Всего аудиторных часов		
		1	0	4
		Онлайн		
		0	0	0
5 - 6	**Тема 10. Контроль прав доступа субъектов к объектам.** Проверка организации контроля доступа к объекту с использованием специализированных средств доверенной загрузки. Проверка настроек разрешительной системы доступа к файловым системам с использованием специализированных тестирующих средств и штатных средств из состава ОС. Проверка организации контроля доступа клиент-серверных приложений к объектам баз данных.	Всего аудиторных часов		
		1	0	2
		Онлайн		
		0	0	0
7 - 8	**Тема 11. Разграничение полномочий пользователей.** Разграничение полномочий пользователей с использованием ролей и привилегий. Детальный контроль доступа пользователей к базам данных. Мандатный контроль доступа пользователей к информации в базе данных. Проверка настроек механизмов контроля доступа специализированных средств защиты информации от НСД сетевых средств и ПЭВМ.	Всего аудиторных часов		
		1	0	2
		Онлайн		
		0	0	0
9-16	**Раздел 2. Особенности аттестационных испытаний АС на соответствие требованиям по защите информации от НСД.**	4	0	12
9 - 10	**Тема 12. Проверка настроек разрешительной системы доступа к файловым системам с использование** Программные средства создания и редактирования модели системы разграничения доступа (СРД). Структура ресурсов АРМ и ЛВС. Установленные права доступа файловой системы NTFS. Списки локальных и доменных пользователей системы. Информация о разрешительной системе. Разграничение доступа с помощью стандартных средств ОС Windows. Предотвращение попыток НСД. Изучение программ «Ревизор 1 XP», «Ревизор 2 XP». Разграничение доступа к объектам АРМ.	Всего аудиторных часов		
		1	0	4
		Онлайн		
		0	0	0
11 - 12	**Тема 13. Проверка настроек механизмов контроля доступа специализированных средств защиты информации от НСД сетевых средств и ПЭВМ.** Проверка настроек мандатного и дискреционного	Всего аудиторных часов		
		1	0	4
		Онлайн		
		0	0	0

	механизмов доступа, а также прав пользователей, работающих в системе. Реализация дискреционного механизма разграничения доступа. Активизация подсистемы управления доступом. Проверка настроек дискреционного механизма разграничения доступа с помощью программ «Ревизор 1 XP» и «Ревизор 2 XP». Реализация мандатного механизма разграничения доступа. Проверка настроек мандатного механизма разграничения доступа с помощью программ «Ревизор 1 XP» и «Ревизор 2 XP». Работа с сетевыми ресурсами.			
13 - 14	**Тема 14. Контроль подсистемы обеспечения целостности.** Контроль целостности программного обеспечения и специализированных средств защиты информации от НСД с помощью программ фиксации и контроля исходного состояния программными комплексами «ФИКС». Настройка средств контроля целостности на основе операций контрольного суммирования: • фиксация исходного состояния файлов программного комплекса; • контроль исходного состояния программного комплекса; • фиксация и контроль каталогов; • контроль различий в заданных файлах; • контроль целостности файлов программного комплекса.	Всего аудиторных часов		
		1	0	2
		Онлайн		
		0	0	0
15 - 16	**Тема 15. Контроль настроек и работы антивирусных средств.** Настройка Файлового Антивируса. Настройка Почтового Антивируса. Настройка Web-Антивируса. Настройка Проактивной защиты. Тестирование работоспособности антивируса. Контроль целостности приложения.	Всего аудиторных часов		
		1	0	2
		Онлайн		
		0	0	0

Сокращенные наименования онлайн опций:

Обозначение	**Полное наименование**
ЭК	Электронный курс
ПМ	Полнотекстовый материал
ПЛ	Полнотекстовые лекции
ВМ	Видео-материалы
АМ	Аудио-материалы
Прз	Презентации
Т	Тесты
ЭСМ	Электронные справочные материалы
ИС	Интерактивный сайт

ТЕМЫ ЛАБОРАТОРНЫХ РАБОТ

Недели	**Темы занятий / Содержание**
	2 Семестр
1 - 6	**Лабораторная работа № 1** Инвентаризация актуального состава технических и программных средств объекта информатизации с

	использованием штатных средств операционной системы и программного обеспечения
7 - 8	**Лабораторная работа № 2** Поиск отличий реально полученной информации от информации, заявленной в исходных данных на объекте информатизации
9 - 11	**Лабораторная работа № 3** Контроль уязвимостей на уровне сети и на уровне операционных систем и прикладного ПО.
12 - 13	**Лабораторная работа № 4** Контроль механизмов идентификации и аутентификации пользователей» при работе со средствами защиты информации (СЗИ) от НСД «Аккорд» и «Соболь», и программными продуктами «НКВД 2.2» и «НКВД 2.3».
	3 Семестр
9 - 10	**Лабораторная работа № 5** Проверка организации контроля доступа к объекту с использованием специализированных средств доверенной загрузки.
11 - 12	**Лабораторная работа № 6** Проверка настроек разрешительной системы доступа к файловым системам с использованием специализированных тестирующих средств и штатных средств из состава ОС.
13 - 14	**Лабораторная работа № 7** Настройка средств контроля целостности на основе операций контрольного суммирования.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В процессе изучения данной дисциплины используются традиционные образовательные технологии, направленные на развитие познавательной активности, творческой самостоятельности студентов; последовательное и целенаправленное выдвижение перед студентом познавательных задач, решая которые студенты активно усваивают знания, в т.ч. поисковые методы и постановка познавательных задач. В ходе обучения используются 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 объектов информатизации 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 лабораторные работы выносятся вопросы, усвоение которых требуется на уровне навыков и умений. Цикл лабораторных работ по отработке программно-аппаратных средств выявления угроз безопасности информации, обусловленных несанкционированным доступом к

ней, проводится в специализированной лаборатории с предварительной установкой необходимого программного обеспечения в компьютерной сети. Для проведения цикла лабораторных работ выделяются два преподавателя: ведущий преподаватель (лектор) и преподаватель для привития практических навыков. При проведении лабораторных работ необходимо отрабатывать задания, в том числе с проведением деловых игр (эпизодов).

Лабораторные работы по контролю эффективности защиты информации от несанкционированного доступа проводятся на автоматизированных рабочих местах в специализированных лабораториях. На каждом рабочем месте должен быть преподаватель, развёрнуто необходимое ПО контроля и средства защиты информации. Результаты, полученные в ходе лабораторных работ, используются студентами в качестве исходных данных при отработке итоговых пакетов документов.

В качестве форм промежуточного контроля полученных знаний могут быть использованы результаты собеседования, 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)**	**Аттестационное мероприятие (КП 2)**
ПК-2	З-ПК-2	З, КИ-8, КИ-15	Э, КИ-8, КИ-16
	У-ПК-2	З, КИ-8, КИ-15	Э, КИ-8, КИ-16
	В-ПК-2		Э, КИ-8, КИ-16
ПК-3	З-ПК-3	З, КИ-15	Э, КИ-8, КИ-16
	У-ПК-3	З, КИ-8, КИ-15	Э, КИ-8, КИ-16
	В-ПК-3		Э, КИ-8, КИ-16
ПК-4	З-ПК-4	З, КИ-8, КИ-15	Э, КИ-8, КИ-16
	У-ПК-4	З, КИ-8, КИ-15	Э, КИ-8, КИ-16
	В-ПК-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:

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. ЭИ А92 Аттестационные испытания автоматизированных систем от несанкционированного доступа по требованиям безопасности информации : учебное пособие, Москва: НИЯУ МИФИ, 2014

2. 004 А92 Аттестационные испытания автоматизированных систем от несанкционированного доступа по требованиям безопасности информации : учебное пособие, Москва: НИЯУ МИФИ, 2014

3. ЭИ К65 Контроль защищенности автоматизированных систем от несанкционированного доступа. Аттестационные испытания : лабораторный практикум, Москва: НИЯУ МИФИ, 2013

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

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

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

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

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

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

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА:

1. 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, Москва: НИЯУ МИФИ, 2014

2. 004 Д84 Контроль защищенности речевой информации в помещениях. Аттестационные испытания вспомогательных технических средств и систем по требованиям безопасности информации : учебное пособие, Москва: НИЯУ МИФИ, 2015

3. 004 К65 Контроль защищенности речевой информации в помещениях. Аттестационные испытания выделенных помещений по требованиям безопасности информации : учебное пособие, Москва: НИЯУ МИФИ, 2014

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ:

1. СПО «Ревизор -2XP» (Т-211)

2. СПО «Терьер-3.0» (Т-211)

3. СПО «Ревизор сети 1.0» (Т-211)

4. СПО «НКВД» (Т-211)

5. СПО «Агент инвентаризации» (Т-211)

6. СПО «Фикс 2.02» (Т-211)

7. СПО «Ревизор -1XP»

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

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 - Обеспечение безопасности значимых объектов критической информационной инфраструктуры, место курса в различных областях науки и техники. В том числе в области информационной безопасности; объекты и виды данной работы в профессиональной деятельности выпускника; требования образовательного стандарта к уровню его подготовки; содержание дисциплины, сущность и краткая характеристика входящих в нее разделов, их взаимосвязь, особенности организации образовательного процесса по данной дисциплине специальности.

КР8, КР15 - 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.

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 объектов информатизации 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 лабораторные работы выносятся вопросы, усвоение которых требуется на уровне навыков и умений. Цикл лабораторных работ по отработке программно-аппаратных средств выявления угроз безопасности информации, обусловленных несанкционированным доступом к

ней, проводится в специализированной лаборатории с предварительной установкой необходимого программного обеспечения в компьютерной сети. Для проведения цикла лабораторных работ выделяются два преподавателя: ведущий преподаватель (лектор) и преподаватель для привития практических навыков. При проведении лабораторных работ необходимо отрабатывать задания, в том числе с проведением деловых игр (эпизодов).

Лабораторные работы по НСД 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 и средства защиты информации и контроля. Результаты, полученные в ходе лабораторных работ, 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.

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 - Обеспечение безопасности значимых объектов критической информационной инфраструктуры, место курса в различных областях науки и техники. В том числе в области информационной безопасности; объекты и виды данной работы в профессиональной деятельности выпускника; требования образовательного стандарта к уровню его подготовки; содержание дисциплины, сущность и краткая характеристика входящих в нее разделов, их взаимосвязь, особенности организации образовательного процесса по данной дисциплине специальности.

КР8, КР15 - 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.

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 объектов информатизации 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 лабораторные работы выносятся вопросы, усвоение которых требуется на уровне навыков и умений. Цикл лабораторных работ по отработке программно-аппаратных средств выявления угроз безопасности информации, обусловленных несанкционированным доступом к ней, проводится в специализированной лаборатории с предварительной установкой необходимого программного обеспечения в компьютерной сети. Для проведения цикла лабораторных работ выделяются два преподавателя: ведущий преподаватель (лектор) и преподаватель для привития практических навыков. При проведении лабораторных работ необходимо отрабатывать задания, в том числе с проведением деловых игр (эпизодов).

Лабораторные работы по НСД, 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 и средства защиты информации и контроля. Результаты, полученные в ходе лабораторных работ, 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.

Автор(ы):

Дураковский Анатолий Петрович, к.т.н., доцент

Рецензент(ы):

Горбатов В.С.