МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
высшего образования - программа специалитета
по специальности
10.05.01 Компьютерная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Методы оценки защищенности компьютерных систем

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Информационная безопасность объектов информатизации на базе компьютерных систем

Форма обучения: Очная

Рабочая программа дисциплины (модуля) в виде электронного документа выгружена из единой корпоративной информационной системы управления университетом и соответствует оригиналу

Простая электронная подпись, выданная РУТ (МИИТ)
ID подписи: 2053
Подписал: заведующий кафедрой Баранов Леонид Аврамович
Дата: 01.06.2022

1. Общие сведения о дисциплине (модуле).

Целями изучения дисциплины «Методы оценки защищенности компьютерных систем» являются овладение студентами теоретических и практических основ организации и проведения оценки безопасности компьютерных систем; развитие в процессе обучения системного мышления, необходимого для решения задач программной защиты информации с учетом требований системного подхода; обучение студентов принципам построения защиты информации в ОС и анализа надежности, защиты компьютерных системах. Задачи дисциплины: изучение принципов построения подсистем защиты в компьютерных системах различной архитектуры; изучение средств и методов несанкционированного доступа к ресурсам компьютерных систем; изучение системного подхода к проблеме защиты информации в компьютерных системах; изучение механизмов защиты информации и возможностей по их преодолению. Основной целью изучения учебной дисциплины «Методы оценки защищенности компьютерных систем» является формирование у обучающегося компетенций для следующих видов деятельности: научно-исследовательская; организационно-управленческая. Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами деятельности): Научно-исследовательская деятельность: сбор, обработка, анализ и систематизация научно-технической информации, отечественного и зарубежного опыта по проблемам компьютерной безопасности; изучение и обобщение опыта работы других учреждений, организаций и предприятий по способам использования методов и средств обеспечения информационной безопасности с целью повышения эффективности и совершенствования работ по защите информации на конкретном объекте; подготовка научно-технических отчетов, обзоров, публикаций по результатам выполненных исследований. Организационно-управленческая деятельность: организация работы коллектива исполнителей, принятие управленческих решений в условиях спектра мнений, определение порядка выполнения работ.

2. Планируемые результаты обучения по дисциплине (модулю).

Перечень формируемых результатов освоения образовательной программы (компетенций) в результате обучения по дисциплине (модулю):

ПК-13 - Способен строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов;

ПК-19 - Способен разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации;

ПК-22 - Способен проводить тестирование систем защиты информации автоматизированных систем;

ПК-25 - Способен разрабатывать план мероприятий по защите информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации;

ПК-27 - Способен участвовать в создании системы защиты информации процессов проектирования, создания и модернизации объектов информатизации на базе компьютерных систем;

ПК-28 - Способен разрабатывать проекты нормативных правовых актов, руководящих и методических документов предприятия, учреждения, организации, регламентирующих деятельность по защите информации в объектах информатизации на базе компьютерных систем, а также процессов их проектирования, создания и модернизации.

Обучение по дисциплине (модулю) предполагает, что по его результатам обучающийся будет:

Владеть:

Строит математические модели для оценки безопасности компьютерных систем.

Уметь:

Анализирует компоненты системы безопасности с использованием современных математических методов.

Уметь:

Разрабатывает математические модели процессов, возникающих при работе программно- аппаратных средств защиты информации.

Уметь:

Анализирует математические модели процессов, возникающих при работе программно- аппаратных средств защиты информации.

Владеть:

Обосновывает адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации.

Уметь:

Проводит индивидуальное тестирование систем защиты информации в блоке автоматизированных систем.

Знать:

Знать основные процессы проектирования систем обеспечения информационной безопасности.

Уметь:

Уметь разрабатывать и реализовывать технологию проведения аудита информационной безопасности на объектах информатизации.

Знать:

Знать основные принципы и методы создания системы обеспечения информационной безопасности процессов проектирования, создания и модернизации объектов информатизации на базе компьютерных систем в защищенном исполнении.

Уметь:

Уметь создавать системы обеспечения информационной безопасности процессов проектирования, создания и модернизации объектов информатизации.

Владеть:

Владеть навыками создания систем обеспечения информационной безопасности.

Знать:

Знать основные принципы разработки нормативно правовых актов, руководящих и методических документов предприятия, учреждения, организации.

Уметь:

Уметь разрабатывать нормативно правовые акты, руководящие и методические документы, регламентирующие деятельность по обеспечению информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении и процессов их проектирования.

Владеть:

Владеть навыками разработки нормативной правовой документации.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 4 з.е. (144 академических часа(ов).

3.2. Объем дисциплины (модуля) в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Тип учебных занятий	Количество часов	
	Всего	Семестр №10
Контактная работа при проведении учебных занятий (всего):	36	36
В том числе:		
Занятия лекционного типа	18	18
Занятия семинарского типа	18	18

3.3. Объем дисциплины (модуля) в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации составляет 108 академических часа (ов).

3.4. При обучении по индивидуальному учебному плану, в том числе при ускоренном обучении, объем дисциплины (модуля) может быть реализован полностью в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации.

4. Содержание дисциплины (модуля).

4.1. Занятия лекционного типа.

№ п/п	Тематика лекционных занятий / краткое содержание
1	Введение Предметная область оценки защищенности компьютерных систем. История развития защиты информации и криптографии.
2	Методы и средства оценки защищённости компьютерных систем Конкурентная разведка. Поиск информации в открытых источниках. Основные виды уязвимостей.

№ п/п	Тематика лекционных занятий / краткое содержание
3	Инструментарий для оценки защищённости компьютерных систем Освоение сканнеров уязвимостей, фаззеров. Освоение анализаторов кода, инструментов изучения сети. Освоение специализированных дистрибутивов.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	ПЗ1 Введение Предметная область оценки защищенности компьютерных систем. История развития защиты информации и криптографии.
2	ПЗ2 Методы и средства оценки защищённости компьютерных систем Конкурентная разведка. Поиск информации в открытых источниках. Основные виды уязвимостей.
3	ПЗ3 Инструментарий для оценки защищённости компьютерных систем Освоение сканнеров уязвимостей, фаззеров. Освоение анализаторов кода, инструментов изучения сети. Освоение специализированных дистрибутивов.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	СР1 Введение Предметная область оценки защищенности компьютерных систем. История развития защиты информации и криптографии
2	СР2 Методы и средства оценки защищённости компьютерных систем Конкурентная разведка. Поиск информации в открытых источниках. Основные виды уязвимостей.
3	СР3 Инструментарий для оценки защищённости компьютерных систем Освоение сканнеров уязвимостей, фаззеров. Освоение анализаторов кода, инструментов изучения сети. Освоение специализированных дистрибутивов.
4	Подготовка к промежуточной аттестации.
5	Подготовка к текущему контролю.

5. Перечень изданий, которые рекомендуется использовать при освоении дисциплины (модуля).

№ п/п	Библиографическое описание	Место доступа

1	Информационная безопасность. Словарь по терминологии Гончаров И.В., Кирсанов Ю.Г., Райков О.В. ЗАО«НПО Инфобезопасность , 2015	
2	Информационная безопасность и защита информации В.П. Мельников, С.А. Клейменов, А.М. Петраков Книга Издательский центр "Академия" , 2012	ИТБ УЛУПС (Абонемент ЮИ); ИТБ УЛУПС (ЧЗ1 ЮИ)
3	Защита информации: учеб. пособие И.К. Астанин, Н.И. Астанин Воронеж. Гос. Ун-т, , 2006	
1	Шпионские штучки" и устройства для защиты объектов и информации: Справ. пособие Андрианов В.И., Бородин В.А., Соколов А.В. Лань , 1996	
2	Методы и инженерно– технические средства противодействия информационным угрозам Абалмазов Э.И. Маршрут , 2005	

6. Перечень современных профессиональных баз данных и информационных справочных систем, которые могут использоваться при освоении дисциплины (модуля).

http://library.miit.ru/ - электронно-библиотечная система Научно-технической библиотеки МИИТ. http://elibrary.ru/ - научно-электронная библиотека. www.chipinfo.ru http://siblec.ru/ www.defcon.ru http://xakep.ru/ http://kali.org/ http://www.intuit.ru http://habrahabr.ru http://semestr.ru http://www.intersystems.ru Поисковые системы: Yandex, Google, Mail.

7. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, необходимого для освоения дисциплины (модуля).

Для проведения лекционных занятийнеобходима специализированная лекционная аудитория с мультимедиа аппаратурой и интерактивной доской.Для проведения практических занятийнеобходимы компьютеры с рабочими местами в компьютерном классе. Компьютеры должны быть обеспечены лицензионными программными продуктами: Microsoft Office не ниже Microsoft Office 2007 (2013), программа виртуализации ОС VirtualBox, платформа для проведения аудита безопасности веб-приложений Burp Suite программа-анализатора трафика для компьютерных сетей Wireshark специализированный дистрибутив Kali Linux / windows-платформа для тестов на проникновение PentestBox среда визуального программирования MicroSoft Visual Studio 2013.

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю).

Для проведения аудиторных занятий и самостоятельной работы требуется:

1. Рабочее место преподавателя с персональным компьютером, подключённым к сетям INTERNET и INTRANET. 2. Специализированная лекционная аудитория с мультимедиа аппаратурой и интерактивной доской. 3. Компьютерный класс. Рабочие места студентов в компьютерном классе, подключённые к сетям INTERNET и INTRANET

Для проведения практических занятий:

компьютерный класс; компьютеры с минимальными требованиями – Pentium 4, ОЗУ 4 ГБ, HDD 100 ГБ, USB 2.0.

9. Форма промежуточной аттестации:

Экзамен в 10 семестре.

10. Оценочные материалы.

Оценочные материалы, применяемые при проведении промежуточной аттестации, разрабатываются в соответствии с локальным нормативным актом РУТ (МИИТ).

Авторы:

профессор, профессор, д.н. кафедры «Управление и защита информации» В.Г. Сидоренко

Согласовано:

Заведующий кафедрой УиЗИ Л.А. Баранов

Председатель учебно-методической комиссии С.В. Володин