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 - программы 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: 01.06.2023

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-20 - Способен подготовить обоснование необходимости защиты информации в автоматизированной системе;

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;

УК-2 - Способен управлять проектом на всех этапах его жизненного цикла.

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

Знать:

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

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:

- 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	Сем. №10
Контактная работа при проведении учебных занятий (всего):	48	48
В том числе:		

Занятия лекционного типа	16	16
Занятия семинарского типа	32	32

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 96 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 Рассматриваемые вопросы: - История развития защиты информации и криптографии.
2	Предметная область оценки защищенности компьютерных систем. Рассматриваемые вопросы: - Предметная область оценки защищенности компьютерных систем.
3	Методы и средства оценки защищённости компьютерных систем Рассматриваемые вопросы: - Методы и средства оценки защищённости компьютерных систем
4	Информация в открытых источниках Рассматриваемые вопросы: - Конкурентная разведка. - Поиск информации в открытых источниках. - Основные виды уязвимостей.
5	Оценка защищённости компьютерных систем Рассматриваемые вопросы: - Инструментарий для оценки защищённости компьютерных систем
6	Освоение сканнеров уязвимостей, фаззеров. Рассматриваемые вопросы: - Освоение сканнеров уязвимостей, фаззеров.
7	Освоение анализаторов кода, инструментов изучения сети. Рассматриваемые вопросы:

№ п/п	Тематика лекционных занятий / краткое содержание
	- Освоение анализаторов кода, инструментов изучения сети.
8	Освоение специализированных дистрибутивов. Рассматриваемые вопросы: - Освоение специализированных дистрибутивов.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	Компьютерные системы и защита информации В результате выполнения практического задания студент рассматривает предметная область оценки защищенности компьютерных систем и изучает историю развития защиты информации и криптографии.
2	Оценка защищённости компьютерных систем. В результате выполнения работы студент рассматривает основные методы и средства оценки защищённости компьютерных систем.
3	Информация в открытых источниках В результате выполнения лабораторной работы студент получает навык проведения конкурентная разведки и отрабатывает умение поиска информации в открытых источниках.
4	Основные виды уязвимостей. В результате выполнения работы студент изучает основные виды уязвимостей.
5	Инструментарий для оценки защищённости компьютерных систем В результате выполнения работы студент рассматривает основные инструментарии для оценки защищённости компьютерных систем
6	Освоение сканнеров уязвимостей, фаззеров. В результате выполнения лабораторной работы студент отрабатывает умение по освоению сканнеров уязвимостей, фаззеров.
7	Освоение анализаторов кода, инструментов изучения сети. В результате выполнения лабораторной работы студент отрабатывает умение по освоению анализаторов кода, инструментов изучения сети.
8	Освоение специализированных дистрибутивов. В результате работы студент отрабатывает умение по освоению специализированных дистрибутивов.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Изучение дополнительной литературы. Методы и средства оценки защищённости компьютерных систем Конкурентная разведка. Поиск информации в открытых источниках. Основные виды уязвимостей.
2	Подготовка к практическим занятиям. Инструментарий для оценки защищённости компьютерных систем Освоение сканнеров уязвимостей, фаззеров. Освоение анализаторов кода, инструментов изучения сети. Освоение специализированных дистрибутивов.
3	Подготовка к промежуточной аттестации.

№ п/п	Вид самостоятельной работы
4	Подготовка к текущему контролю.
5	Подготовка к промежуточной аттестации.
6	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	ЭБС
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	ЭБС
1	Шпионские штучки" и устройства для защиты объектов и информации: Справ. пособие Андрианов В.И., Бородин В.А., Соколов А.В. Лань , 1996	ЭБС
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).

Официальный сайт РУТ (МИИТ) (https://www.miit.ru/).

Научно-техническая библиотека РУТ (МИИТ) (http:/library.miit.ru).

Образовательная платформа «Юрайт» (https://urait.ru/).

Общие информационные, справочные и поисковые системы «Консультант Плюс», «Гарант».

Электронно-библиотечная система издательства «Лань» (http://e.lanbook.com/).

Электронно-библиотечная система ibooks.ru (http://ibooks.ru/).

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

Microsoft Internet Explorer (или другой браузер).

Операционная система Microsoft Windows.

Microsoft Office

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).

Учебные аудитории для проведения учебных занятий, оснащенные компьютерной техникой и наборами демонстрационного оборудования.

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