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 магистратуры
по направлению подготовки
10.04.01 Информационная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Безопасность компьютерных сетей

Направление подготовки: 10.04.01 Информационная безопасность

Направленность (профиль): Безопасность компьютерных систем и сетей

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Целями освоения учебной дисциплины «Безопасность компьютерных сетей» являются формирование компетенций по основным разделам теоретических и практических основ по организации безопасности компьютерных сетей, дать необходимые знания по уязвимостям в компьютерных сетях, навыки попрактическому использованию средств анализа трафика и мониторинта инцидентов защиты в сетях, включая использование возможностей ограничения доступа к защищаемым ресурсам.

Слушатель получает систематизированные теоретические и практические знания в области обеспечения безопасности компьютерных сетей, должен научиться определять возможные уязвимости, использовать современные обеспечения безопасности, в том числе, предоставляемые сетевым оборудованием для уменьшения уязвимости компьютерных сетей.

Основными задачами дисциплины являются:

• изучение принципов структурной и архитектурной организации современных средств обеспечения безопасности компьютерных сетей;

• рассмотрение и анализ перспектив развития средств безопасности компьютерных сетей;

• изучение средств мониторинга сетевых событий с точки зрения обеспечения безопасности;

• изучение направлений атак и уязвимостей в компьютерных сетях;

• конфигурирование средств для оповещения и выявления инцидентов защиты;

• анализ трафика с целью выявления угроз безопасности сети;

• обработка инцидентов защиты компьютерных сетей.

Дисциплина предназначена для получения знаний, необходимых для решения следующих профессиональных задач (в соответствии с видами деятельности):

Научно-исследовательская деятельность

• участие в фундаментальных и прикладных исследованиях в области профессиональной деятельности;

• разработка планов, программ и методик проведения исследований объектов профессиональной деятельности;

• подготовка по результатам научных исследований отчетов;

• научное руководство научно-исследовательскими и опытно-конструкторскими разработками в области информационной безопасности.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-2 - Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности ;

ОПК-5 - Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи;

ПК-4 - Способность проводить экспериментальные исследования защищенности объектов с применением соответствующих физических и математических методов, технических и программных средств обработки результатов эксперимента.

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

Знать:

-принципы построения компьютерных систем и сетей;

-принципы построения подсистем защиты информации в компьютерных системах;

-методы оценки эффективности политики безопасности;

-национальные, межгосударственные и международные стандарты, устанавливающие требования к организации и проведению научно-исследовательских, опытно-конструкторских работ, опытной эксплуатации 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.

Уметь:

-определять параметры функционирования программно-аппаратных средств защиты информации; оценивать эффективность защиты информации;

- применять разработанные методики оценки защищенности программно-аппаратных средств защиты информации;

-организовывать сбор, обработку, анализ и систематизацию научно-технической информации, отечественного и зарубежного опыта по проблемам информационной безопасности компьютерных сетей, выработку предложений по вопросам комплексного обеспечения информационной безопасности компьютерных сетей;

проводить выбор, исследовать эффективность и разрабатывать технико-экономическое обоснование проектных решений средств и систем защиты от НСД

Владеть:

-навыками оценки работоспособности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик в компьютерных сетях;

-определение уровня защищенности и доверия программно-аппаратных средств защиты информации;

-организации опытной эксплуатации средств и систем защиты компьютерных сетей от НСД.

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. №1
Контактная работа при проведении учебных занятий (всего):	50	50
В том числе:		
Занятия лекционного типа	34	34
Занятия семинарского типа	16	16

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 94 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	Тема 1. Типы сетевых атак. Механизмы и методы проведения сетевых атак с стеке протоколов TCP/IP. Обзор методов защиты. Тема 2. Обеспечение безопасности уровня сетевого доступа. Сетевые анализаторы, «снифферы» и их обнаружение. Аутентификация на основе MAC-адресов. Уязвимости сетевого оборудования канального уровня. Тема 3. Обеспечение безопасности уровня интернет. Фильтрация пакетов. Ограничение маршрутной информации, фильтрация трафика ICMP, ARP Spoofing, DHCP Spoofing, фрагментация. Тема 4. Обеспечение безопасности транспортного уровня. Выявление уязвимостей, системы обнаружения вторжений, сканеры безопасности, DOS-атаки. Тема 5.Маршрутизация в виртуальных частных сетях с архитектурой клиент-сервер. Remote-access VPN. Cisco Any Connect. Создание туннельного интерфейса. Использование Cisco ASA в качестве VPN-сервера.

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	Лабораторная работа № 1. Анализ сетевого трафика. В результате выполнения работы студент получит практические навыки по анализу, передаваемой по сети, информации. Лабораторная работа № 2. MAC-спуфинг. В результате выполнения работы студент получит практические навыки по приемам борьбы с уязвимостью «MAC-спуфинг».

№ п/п	Наименование лабораторных работ / краткое содержание
	Лабораторная работа № 3. ARP-спуфинг. В результате выполнения работы студент получит практические навыки по приемам борьбы с уязвимостью «ARP-спуфинг». Лабораторная работа № 4. DHCP-спуфинг. В результате выполнения работы студент получит практические навыки по приемам борьбы с уязвимостью «DHCP-спуфинг». Лабораторная работа № 5. TCP-reset. В результате выполнения работы студент получит практические навыки по приемам борьбы с атакой «TCP-reset». Лабораторнаяработа № 6. Cisco AnyConnect (Remote-accessVPN). В результате выполнения работы студент получит практические навыки по настройке Remote-accessVPN

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Подготовка к лабораторным работам
2	Работа с лекционным материалом
3	Подготовка к промежуточной аттестации.
4	Подготовка к текущему контролю.

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

№ п/п	Библиографическое описание	Место доступа
1	Голдовский Я.М., Желенков Б.В., Сафонова И.Е. Криптографическая защита компьютерной информации : метод. указ. к лаб. раб. по дисц. "Теоретические основы компьютерной безопасности" для студ., обуч. по напр. "Информационная безопасность" / МИИТ. Каф. "Вычислительные системы и сети". - М. :	URL: http://195.245.205.171:8087/jirbis2/books/scanbooks_new/metod/03-42764.pdf. (дата обращения 04.10.2022)004 Г60

	МГУПС(МИИТ), 2013. - 36 с. : ил. - Библиогр.: с. 46. - 100 экз. - (в пер.) : 39.78 р.	
2	.П. Соловьев, А.Е. Шубарев, Н.Н. Пуцко. Безопасность коммуникационных сетей : учеб. пособие для студ., обуч. по магистерской программе "Безопасность и защита информации" напр. "Информатика и выч. Тех МИИТ. Центр компетентности "Защита и безопасность информации". - М. : МИИТ, 2007. - 86 с. : ил. - (Инновационная образовательная программа - МИИТ). - Библиогр.: с. 84 (4 назв.). - Б. ц. -	- URL: http://195.245.205.171:8087/jirbis2/books/scanbooks_new/upos/04-35188.pdf.(дата обращения: 04.10.2022)Текст : непосредственный.
3	Мэйволд Эрик. Безопасность сетей: курс лекций Москва :Интуит НОУ, 2016. — 572 с. — ISBN 978-5-9570-0046-9	URL: https://book.ru/book/917577 (дата обращения: 04.10.2022). — Текст : электронный.

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

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

Официальный сайт по поддержке решений Cisco https://www.cisco.com/

Форум специалистов по информационным технологиям http://citforum.ru/

Интернет-университет информационных технологий http://www.intuit.ru/

Тематический форум по информационным технологиям http://habrahabr.ru/

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

Для проведения лекционных занятий необходима специализированная лекционная аудитория с мультимедиа аппаратурой. Компьютер должен быть обеспечен лицензионными программными продуктами:

Microsoft Windows

Microsoft Office

Для проведения лабораторных работ необходимы персональные компьютеры с рабочими местами. Компьютер должен быть обеспечен лицензионными программными продуктами:

Microsoft Windows

Microsoft Office

В случае проведении занятий с применением электронного обучения и дистанционных образовательных технологий может понадобиться наличие следующего программного обеспечения (или их аналогов): ОС Windows, Microsoft Office, Интернет-браузер, Microsoft Teams и т.д.

В образовательном процессе, при проведении занятий с применением электронного обучения и дистанционных образовательных технологий, могут применяться следующие средства коммуникаций: ЭИОС РУТ(МИИТ), Microsoft Teams, электронная почта, скайп, Zoom, WhatsApp и т.п.

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

Учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций

Аудиовизуальное оборудование для аудитории, АРМ управляющий, проектор, экран проекционный Аудитория подключена к интернету МИИТ.

Учебная аудитория для проведения практических занятий, лабораторных работ.

персональные компьютерыв. Программно-аппаратный комплекс СОТСБИ.

Учебная аудитория для проведения занятий лекционного типа, практических занятий, лабораторных работ

Рабочие станции для студентов , коммутатор CISCO, маршрутизатор CISCO, межсетевой экран Cisco, сетевое оборудование, рабочая станция преподавателя, проектор, экран.

В случае проведении занятии с применением электронного обучения и

дистанционных образовательных технологии необходимо наличие компьютернои техники, для организации коллективных и индивидуальных форм общения педагогических работников со студентами, посредством используемых средств коммуникации. Допускается замена оборудования его виртуальными аналогами.

9. Форма промежуточной аттестации:

Зачет в 1 семестре.

10. Оценочные материалы.

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

Авторы:

заведующий кафедрой, доцент, к.н.
кафедры «Вычислительные системы,
сети и информационная
безопасность» Б.В. Желенков

Согласовано:

Заведующий кафедрой ВССиИБ Б.В. Желенков

Председатель учебно-методической
комиссии Н.А.Клычева