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 траффика с целью выявления угроз безопасности сети;

• обработка инцидентов защиты компьютерных сетей.

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:

- методы и алгоритмы проектирования распределенных информационных систем, их компоненты и протоколы взаимодействия;
- методы и алгоритмы проектирования распределенных информационных систем, их компоненты и протоколы взаимодействия.

Уметь:

- выбирать средства для проектирования систем, компоненты проектирования протоколы их связей;
-выбирать средства для проектирования систем, компоненты проектирования протоколы их связей.

Владеть:

- навыками выбора инструментальных средств разработки и обеспечения безопасности компьютерных сетей;
- навыками определения набора средств обеспечения безопасности;
- навыками выбора средств создания и ведения репозитория, учета инцидентов информационной безопасности, сборки и непрерывной интеграции, базы знаний;
- навыками организации процесса использования инфраструктуры;
- навыками мониторинга функционирования инфраструктуры;
- навыками принятия управленческих решений.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 5 з.е. (180 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 №1

Контактная работа при проведении учебных занятий (всего):	64	64
В том числе:		
Занятия лекционного типа	32	32
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 116 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	Стандарты по опытной эксплуатации средств и систем защиты СССЭ от НСД Рассматриваемые вопросы: - безопасность информационных технологий; - методы и средства обеспечения безопасности, критерии оценки безопасности информационных технологий.
2	Типы сетевых атак. Рассматриваемые вопросы: - архитектура эшелонированой защиты сети; - классификация уязвимостей в сетях; - классификация атак в сетях; - механизмы и методы проведения сетевых атак с стеке протоколов TCP/IP.
3	Обеспечение безопасности на канальном уроне модели OSI. Рассматриваемые вопросы: - сетевые анализаторы, «снифферы» и их обнаружение; - аутентификация на основе MAC-адресов; - уязвимости сетевого оборудования канального уровня.
4	Обеспечение безопасности уровня интернет Рассматриваемые вопросы: - фильтрация пакетов; - ограничение маршрутной информации; - фильтрация трафика ICMP;

№ п/п	Тематика лекционных занятий / краткое содержание
	- фрагментация; - ARP Spoofing.
5	Обеспечение безопасности транспортного уровня Рассматриваемые вопросы: - сеансы протоколов TCP и UDP; - сканирование портов; - атаки UDP flood; - атаки SYN flood; - атаки TCP reset; - подмена участника TCP-соединения.
6	Обеспечение безопасности транспортного уровня.Протокол TCP Рассматриваемые вопросы: - атаки SYN flood; - атаки TCP reset; - подмена участника TCP - соединения.
7	Обеспечение безопасности служб прикладного уровня.Протокол DHCP Рассматриваемые вопросы: - уязвимость протокола DHCP; - ложный DHCP-сервер; - защита от атак DHCP.
8	Обеспечение безопасности служб прикладного уровня.Протокол DNS. Рассматриваемые вопросы: - угрозы DNS-атак; - подмена DNS-ответа; - атаки типа DNS- flood; - защита от атак на DNS.
9	Безопасность трафика на прикладном уровне Рассматриваемые вопросы: - протоколы SSL/TLS, SSH; - атака типа «человек посередине».
10	Маршрутизация в виртуальных частных сетях с архитектурой клиент-сервер Рассматриваемые вопросы: - remote-access VPN. - Cisco Any Connect. - создание туннельного интерфейса. - использование Cisco ASA в качестве VPN-сервера.
11	Обеспечение безопасности сети с помощью АПКШ «Континент» Рассматриваемые вопросы: - задачи комплекса; - используемые средства защиты; - принципы работы.
12	Обеспечение безопасности сети с помощью АПКШ «Континент» Рассматриваемые вопросы: - размещение элементов АПКШ в сети; - состав аппаратной платформы АПКШ; - сравнение версий; - работа с ПАК «Соболь».
13	Обеспечение безопасности сети с помощью АПКШ «Континент».Конфигурирование АПКШ. Инициализация компонентов системы. Рассматриваемые вопросы:

№ п/п	Тематика лекционных занятий / краткое содержание
	- инициализация ЦУС и СД; - установка программы управления комплексом; - конфигурация базы данных и настройка агента ЦУС и СД; - инициализация КШ.
14	Обеспечение безопасности сети с помощью АПКШ «Континент».Конфигурирование АПКШ. Подсистема управления комплексом Рассматриваемые вопросы: - установка подсистемы управления; - настройка контроля целостности; - запуск подсистемы управления и подключение к ЦУС.
15	Обеспечение безопасности сети с помощью АПКШ «Континент».Управление компонентами Рассматриваемые вопросы: - генерация главных ключей всех сетевых устройств; - генерация ключей для организации криптографической связи КШ; - смена ключей; - учетная запись администратора ЦУС; - учетная запись локального администратора КШ с ЦУС.
16	Обеспечение безопасности сети с помощью АПКШ «Континент».Фильтрация и IP-пакетов и трансляция Рассматриваемые вопросы: - межсетевой экран; - формирование правил фильтрации; - трансляция сетевых адресов.

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	Анализ сетевого трафика В результате выполнения работы студент получит практические навыки по анализу, передаваемой по сети, информации.
2	MAC-спуфинг В результате выполнения работы студент получит практические навыки по приемам борьбы с уязвимостью «MAC-спуфинг».
3	ARP-спуфинг В результате выполнения работы студент получит практические навыки по приемам борьбы с уязвимостью «ARP-спуфинг».
4	DHCP-спуфинг В результате выполнения работы студент получит практические навыки по приемам борьбы с уязвимостью «DHCP-спуфинг».
5	TCP-reset. В результате выполнения работы студент получит практические навыки по приемам борьбы с атакой «TCP-reset».
6	CiscoAnyConnect (Remote-accessVPN). В результате выполнения работы студент получит практические навыки по настройке Remote-accessVPN

№ п/п	Наименование лабораторных работ / краткое содержание
7	Инициализация ЦУС и СД АПКШ «Континент» В результате выполнения работы студент получит практические навыки по инициализации центра управления сетями и управления доступом
8	Установка подсистемы управления комплексом АПКШ В результате выполнения работы студент получит практические навыки по установке подсистемы управления комплексом.
9	Конфигурирование журналов баз данных. Настройка агента ЦУС и СД В результате выполнения работы студент получит практические навыки по конфигурированию журналов баз данных и настройке агента ЦУС и СД.
10	Инициализация КШ В результате выполнения работы студент получит практические навыки по инициализация КШ.
11	Смена ключей КШ В результате выполнения работы студент получит практические навыки по смене ключей КШ.
12	Управление учетными записями администраторов В результате выполнения работы студент получит практические навыки по управлению учетными записями администраторов.
13	Правила фильтрации между компьютерами из защищаемой сети и сети общего доступ В результате выполнения работы студент получит практические навыки по конфигурированию правил фильтрации между компьютерами из защищаемой сети и сети общего доступа
14	Правила фильтрации между компьютерами из внутренних сетей, защищаемых разными криптошлюзами В результате выполнения работы студент получит практические навыки по конфигурированию правил фильтрации между компьютерами из внутренних сетей, защищаемых разными криптошлюзами
15	Настройка исходящего правила трансляции В результате выполнения работы студент получит практические навыки по настройке исходящего правила трансляции
16	Настройка входящего правила трансляции

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	Костин В. Н. Методы и средства защиты	https://e.lanbook.com/book/116743 (дата обращения: 03.04.2024).

	компьютерной информации: информационная безопасность компьютерных сетей : учебное пособие / В. Н. Костин. — Москва : МИСИС, 2018. — 31 с. — ISBN 978-5-906953-53-7. — Текст : электронный // Лань : электронно-библиотечная система.	
2	Никифоров С. Н. Методы защиты информации. Защищенные сети : учебное пособие для вузов / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2021. — 96 с. — ISBN 978-5-8114-8123-1. — Текст : электронный // Лань : электронно-библиотечная система	https://e.lanbook.com/book/171868 (дата обращения: 03.04.2024)
3	Руденков Н.А., Технологии защиты информации в компьютерных сетях : учебное пособие / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. — 2-е изд. — Москва : ИНТУИТ, 2016. — 368 с. — Текст : электронный // Лань : электронно-библиотечная система. —	https://e.lanbook.com/book/100522 (дата обращения: 03.04.2024). — Режим доступа: для авториз. пользователей.
4	Руководящий документ. Безопасность информационных технологий.Положение по разработке профилей защиты и заданий по безопасности	https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/rukovodyashchij-dokument-2003-god
5	ГОСТ Р ИСО/МЭК 15408-1-2012 НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ	https://docs.cntd.ru/document/1200101777

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 ФПСУ https://www.fpsu.ru/

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

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 компьютеры. Программно-аппаратный комплекс СОТСБИ.

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

межсетевой экран, сетевое оборудование, рабочая станция преподавателя, проектор, экран.

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. Андриянова