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
09.04.01 Информатика и вычислительная техника,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Безопасность компьютерных сетей

Направление подготовки: 09.04.01 Информатика и вычислительная техника

Направленность (профиль): Компьютерные сети и технологии

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.

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;

• участие в фундаментальных и прикладных исследованиях в области связи, информационных и коммуникационных технологий;

• участие в научно-исследовательских и опытно-конструкторских разработках в области информатики и вычислительной техники на транспорте;

• научное руководство научно-исследовательскими и опытно-конструкторскими разработками в области информатики и вычислительной техники.

Проектная деятельность

• подготовка заданий на разработку проектных решений;

• разработка и реализация проектов по интеграции информационных систем в соответствии с методиками и стандартами информационной поддержки изделий, включая методики и стандарты документооборота, интегрированной логистической поддержки, оценки качества программ и баз данных, электронного бизнеса;

• проведение технико-экономического и функционально-стоимостного анализа эффективности проектируемых систем;

• разработка методических и нормативных документов, технической документации, а также предложений и мероприятий по реализации разработанных проектов и программ.

Производственно-технологическая деятельность

• Разработка технологических решений при проектировании систем безопасности компьютерных сетей;

• Разработка технологических решений для систем управления безопасностью компьютерных сетей.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-5 - Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем;

ПК-1 - Способность проектировать распределенные информационные системы, их компоненты и протоколы их взаимодействия.

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 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. №4
Контактная работа при проведении учебных занятий (всего):	32	32
В том числе:		
Занятия лекционного типа	16	16
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 112 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 Компьютерная сеть. Классификация сетей. Рассматриваются основные направления действия системы защиты информации в сети и принципы ее организации. Тема 2. Коммутация каналов, сообщений, пакетов. Рассматриваются вопросы безопасности сети предприятия, определяются направления действия политики защиты. Приводятся примерные варианты реализации политик защиты. Рассматривается работа транзисторного ключа, приводятся методика расчетов значений их элементов и получаемых характеристик. Тема 3. Атаки на коммуникационные протоколы сети. Рассматриваются компоненты системы и сегментирование сети критерия защиты информации и их совместное использование. Тема 4. Обеспечение безопасности транспортного уровня. Выявление уязвимостей, системы обнаружения вторжений, сканеры безопасности, DOS-атаки. Способы обеспечения работы сети при DDOS. Тема 5.Маршрутизация в виртуальных частных сетях с архитектурой клиент-сервер. Принцип построения тунельного интерфейса. Remote-accessVPN. CiscoAnyConnect. Создание туннельного интерфейса. Использование Cisco ASA в качестве VPN-сервера. Сравнение ФПСУ-IP клиента и CiscoAnyConnect

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	Лабораторная работа № 1. Анализ сетевого трафика. Определение критериев анализа и параметров подлежащих анализу и контролю. В результате выполнения работы студент получит практические навыки по анализу, передаваемой по сети, информации. Лабораторная работа № 2. DDOS и способы защиты. В результате выполнения работы студент получит практические навыки по приемам борьбы и понимание механизмов DDOS. Лабораторная работа № 3. Понятие уязвимости софта и способы тестирования . В результате выполнения работы студент получит практические навыки по приемам борьбы с уязвимостью софта и освоит навык понимания принципа. Лабораторная работа № 4. Уязвимости SNMP V2 и SNMP V3. В результате выполнения работы студент получит практические навыки по понимания различий протаколов версий V2 и V3. Лабораторная работа № 5. TCP-reset. В результате выполнения работы студент получит практические навыки по приемам борьбы с атакой «TCP-reset». Лабораторнаяработа № 6. ФПСУ-IP (Remote-accessVPN). В результате выполнения работы студент получит практические навыки по настройке Remote-accessVPN для российского ФПСУ-IP (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	Голиков, А. М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А. М.	URL: https://e.lanbook.com/book/110336 (дата обращения: 04.10.2022). — Режим доступа: для авториз. пользователей. — Текст : электронный

	Голиков. — Москва : ТУСУР, 2015. — 284 с. // Лань : электронно-библиотечная система.	
2	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
3	В.П. Соловьев, А.Е. Шубарев, Н.Н. Пуцко. Безопасность коммуникационных сетей МИИТ, 2007 86с : 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..
4	М. Голдовский, Б.В. Желенков, И.Е. Сафонова Криптографическая защита компьютерной информации. МИИТ, 2013 - 36 с. : ил. - Библиогр.: с. 46. - 100 экз. - (в пер.) : 39.78 р.	URL: http://195.245.205.171:8087/jirbis2/books/scanbooks_new/metod/03-42764.pdf. (дата обращения 04.10.2022)Текст : непосредственный.

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 .

Проектор для вывода изображения на экран для студентов, акустическая система, место для преподавателя оснащенное компьютером). Аудитория подключена к интернету МИИТ.

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

Аудиовизуальное оборудование для аудитории, АРМ управляющий, проектор, экран, персональные компьютеры ,мониторы, принтер, доска учебная. Аудитория подключена к интернету МИИТ.

- В случае проведении занятий с применением электронного обучения и дистанционных образовательных технологий необходимо наличие компьютерной 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:

Экзамен в 4 семестре.

10. Оценочные материалы.

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

Авторы:

Д.Н. Данилюк

Согласовано:

Заведующий кафедрой ВССиИБ	Б.В. Желенков
Председатель учебно-методической комиссии	Н.А.Клычева