

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

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: 4196
Подписал: заведующий кафедрой Желенков Борис
Владимирович
Дата: 10.04.2024

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 мониторинга 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 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 №3
Контактная работа при проведении учебных занятий (всего):	48	48
В том числе:		
Занятия лекционного типа	32	32
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 132 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	<p>Стандарты по опытной эксплуатации средств и систем защиты СССЭ от НСД</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - безопасность информационных технологий; - методы и средства обеспечения безопасности, критерии оценки безопасности информационных технологий.
2	<p>Типы сетевых атак.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - архитектура эшелонированной защиты сети; - классификация уязвимостей в сетях; - классификация атак в сетях; - механизмы и методы проведения сетевых атак с стеке протоколов TCP/IP.
3	<p>Обеспечение безопасности на канальном уровне модели OSI.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - сетевые анализаторы, «снифферы» и их обнаружение; - аутентификация на основе MAC-адресов; - уязвимости сетевого оборудования канального уровня.
4	<p>Обеспечение безопасности уровня интернет</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - фильтрация пакетов; - ограничение маршрутной информации; - фильтрация трафика ICMP; - фрагментация; - ARP Spoofing.
5	<p>Обеспечение безопасности транспортного уровня</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - сеансы протоколов TCP и UDP; - сканирование портов; - атаки UDP flood; - атаки SYN flood; - атаки TCP reset; - подмена участника TCP-соединения.
6	<p>Обеспечение безопасности транспортного уровня.Протокол TCP</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - атаки SYN flood; - атаки TCP reset; - подмена участника TCP - соединения.
7	<p>Обеспечение безопасности служб прикладного уровня.Протокол DHCP</p> <p>Рассматриваемые вопросы:</p>

№ п/п	Тематика лекционных занятий / краткое содержание
	<ul style="list-style-type: none"> - уязвимость протокола DHCP; - ложный DHCP-сервер; - защита от атак DHCP.
8	<p>Обеспечение безопасности служб прикладного уровня. Протокол DNS.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - угрозы DNS-атак; - подмена DNS-ответа; - атаки типа DNS- flood; - защита от атак на DNS.
9	<p>Безопасность трафика на прикладном уровне</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - протоколы SSL/TLS, SSH; - атака типа «человек посередине».
10	<p>Маршрутизация в виртуальных частных сетях с архитектурой клиент-сервер</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - remote-access VPN. - Cisco Any Connect. - создание туннельного интерфейса. - использование Cisco ASA в качестве VPN-сервера.
11	<p>Обеспечение безопасности сети с помощью АПКШ «Континент»</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - задачи комплекса; - используемые средства защиты; - принципы работы.
12	<p>Обеспечение безопасности сети с помощью АПКШ «Континент»</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - размещение элементов АПКШ в сети; - состав аппаратной платформы АПКШ; - сравнение версий; - работа с ПАК «Соболь».
13	<p>Обеспечение безопасности сети с помощью АПКШ «Континент». Конфигурирование АПКШ. Инициализация компонентов системы.</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - инициализация ЦУС и СД; - установка программы управления комплексом; - конфигурация базы данных и настройка агента ЦУС и СД; - инициализация КШ.
14	<p>Обеспечение безопасности сети с помощью АПКШ «Континент». Конфигурирование АПКШ. Подсистема управления комплексом</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - установка подсистемы управления; - настройка контроля целостности; - запуск подсистемы управления и подключение к ЦУС.
15	<p>Обеспечение безопасности сети с помощью АПКШ «Континент». Управление компонентами</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - генерация главных ключей всех сетевых устройств; - генерация ключей для организации криптографической связи КШ; - смена ключей; - учетная запись администратора ЦУС;

№ п/п	Тематика лекционных занятий / краткое содержание
	- 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	Спуфинг В результате выполнения работы студент получит практические навыки по приемам борьбы с уязвимостями «MAC-спуфинг», «ARP-спуфинг», DHCP-спуфинг».
3	TCP-reset В результате выполнения работы студент получит практические навыки по приемам борьбы с атакой «TCP-reset».
4	Инициализация ЦУС и СД АПКШ «Континент» В результате выполнения работы студент получит практические навыки по инициализации центра управления сетями и управления доступом.
5	Установка подсистемы управления комплексом АПКШ «Континент» В результате выполнения работы студент получит практические навыки по установке подсистемы управления комплексом, конфигурированию журналов баз данных и настройке агента ЦУС и СД
6	Инициализация КШ В результате выполнения работы студент получит практические навыки по инициализация КШ.
7	Смена ключей КШ В результате выполнения работы студент получит практические навыки по смене ключей КШ.
8	Управление учетными записями администраторов В результате выполнения работы студент получит практические навыки по управлению учетными записями администраторов.

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 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.	https://e.lanbook.com/book/116743 (дата обращения: 03.04.2024).
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	Технологии защиты информации в компьютерных сетях : учебное пособие / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суоров. — 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.miiit.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:

Экзамен в 3 семестре.

10. Оценочные материалы.

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

Авторы:

доцент кафедры «Вычислительные
системы, сети и информационная
безопасность»

Д.Н. Данилюк

Согласовано:

Заведующий кафедрой ВССиИБ

Б.В. Желенков

Председатель учебно-методической
комиссии

Н.А. Андриянова