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)

Основы построения защищенных компьютерных сетей

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: 01.06.2024

1. Общие сведения о дисциплине (модуле).

Целью изучения дисциплины «Основы построение защищенных компьютерных сетей» является теоретическая и практическая подготовка обучающихся к деятельности, связанной с построением защищенных сетевых автоматизированных систем, а также обучение принципам и методам защиты информации в компьютерных сетях.

Задачи дисциплины:

- изучение типовых угроз безопасности в компьютерных сетях;
- изучение криптографических и программно-аппаратных методов обеспечения информационной безопасности в компьютерных сетях;
- приобретение навыков настройки и эксплуатации средств обеспечения безопасности в компьютерных сетях;
- овладение средствами и методами проектирования и построения защищенных сетевых автоматизированных систем;
- овладение средствами и методами выявления и нейтрализации попыток нарушения безопасности в компьютерных сетях.

2. Планируемые результаты обучения по дисциплине (модулю).

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

ОПК-10 - Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности;

ОПК-16 - Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях;

ОПК-17 - Способен анализировать основные этапы и закономерности исторического развития России, ее место и роль в контексте всеобщей истории, в том числе для формирования гражданской позиции и развития патриотизма;

ПК-7 - Способен проводить анализ информационной безопасности объектов и систем, принимать участие в организации и сопровождении аттестации объекта информатизации на предмет соответствия требованиям защиты информации;

ПК-9 - Способен участвовать в управлении информационной безопасностью компьютерной системы, разрабатывать предложения по ее совершенствованию;

ПК-11 - Способен проводить проверки эффективности и выполнять работы по восстановлению работоспособности программных, программно-аппаратных и технических средств, подсистем защиты информации;

ПК-12 - Способен выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности, проводить мониторинг и анализ эффективности реализации систем защиты информации и действующих политик безопасности в компьютерных системах.

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

Знать:

- основные методы и средства криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности;
- нормативно-правовую документацию в области информационной безопасности, защиты информации.
- средства защиты информации в компьютерных системах и сетях;

Уметь:

- применять на практике методы и средства оценки эффективности операционных систем и систем управления базами данных.
- анализировать результаты оценки эффективности реализации действующих политик безопасности операционных систем и систем управления базами данных; делать соответствующие выводы и строить свою деятельность в зависимости от достигнутых результатов и полученных выводов.
- применять на практике методы и средства контроля корректности функционирования программно-аппаратных средств защиты информации в компьютерных системах и сетях

Владеть:

- методами и средствами контроля корректности функционирования программно-аппаратных средств защиты информации в компьютерных системах и сетях.
- методами анализа безопасности компьютерных систем, в том числе с использованием методов моделирования, на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности.

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	Семестр №8
Контактная работа при проведении учебных занятий (всего):	80	80
В том числе:		
Занятия лекционного типа	32	32
Занятия семинарского типа	48	48

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 64 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	КС и их организация / Сетевые атаки. Рассматриваемые вопросы: - Основные механизмы проведения сетевых атак на различных уровнях модели ISO/OSI.
2	Механизмы реализации атак в сетях TCP/IP. Рассматриваемые вопросы: - Методы сканирования портов. - Методы обнаружения пакетных снифферов. - Методы обхода МЭ.
3	Методы перехвата сетевых соединений в сетях TCP/IP.

№ п/п	Тематика лекционных занятий / краткое содержание
	Рассматриваемые вопросы: - Технические меры защиты от сетевых атак. - Атаки направленные на сетевую инфраструктуру
4	Примеры сетевых атак в сетях TCP/IP. Рассматриваемые вопросы: - Технические меры защиты от сетевых атак - Принуждение к ускоренной передаче. - Атаки, направленные на отказ в обслуживании. - Изменение конфигурации и состояния хостов. - Программно-технические меры защиты от сетевых атак
5	Криптографические методы защиты информации в компьютерных сетях. Рассматриваемые вопросы: - Криптографические протоколы обеспечения безопасности. - Протоколы аутентификации на прикладном уровне. - Протокол Kepberos. - Протоколы аутентификации на транспортном уровне: протокол SSI/TLS
6	Защита виртуальных частных сетей (VPN). Рассматриваемые вопросы: - Назначение, основные возможности и варианты реализации VPN. - Достоинства и недостатки применения VPN - Протокол IPSEC/ Протоколы AH и ESP. - Использование протокола L2TP для организации виртуальных частных сетей.
7	Разработка защищенных сетевых приложений. Рассматриваемые вопросы: - Аутентификация, шифрование, обеспечение целостности с использованием программного интерфейса SSPI. - Программный интерфейс Open SSI.
8	Программно-аппаратные средства обеспечения безопасности в компьютерных сетях. Рассматриваемые вопросы: - Средства защиты локальных сетей при подключении к Интернет. - Место и роль МЭ в обеспечении сетевой безопасности. - Основные возможности и схемы развертывания МЭ
9	Методы сетевой трансляции адресов (NAT). Рассматриваемые вопросы: - Построение правил фильтрации. - Реализация сетевой политики безопасности с использованием МЭ. - Методы обхода межсетевых экранов
10	Защита серверов и рабочих станций. Рассматриваемые вопросы: - Системы обнаружения вторжений (СОВ). - Место и роль СОВ в общей системе обеспечения сетевой безопасности. - Классификация СОВ.
11	Средства и методы предотвращения в обнаружении вторжений. Рассматриваемые вопросы: - Выявление атак на основе сигнатур атак и выявление аномалий. - Аудит прикладных служб. - Средства обнаружения уязвимостей сетевых служб. - Системы виртуальных ловушек (Honey Pot и Paded Geet).

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	Средства проведения атак В результате выполнения лабораторной работы студент рассматривает основные инструментальные средства проведения атак.
2	Сети TSP/IP В результате выполнения лабораторной работы студент изучает методы и средства перехвата в сетях TSP/IP.
3	Меры защиты от сетевых атак В результате выполнения лабораторной работы студент рассматривает технические меры защиты от сетевых атак.
4	VPN с использованием IPSEC В результате выполнения лабораторной работы студент рассматривает особенности развертывания VPN с использованием IPSEC.
5	Программный интерфейс SSPI В результате выполнения лабораторной работы студент рассматривает особенности обеспечения целостного с использованием программного интерфейса SSPI
6	VPN базовыми средствами ОС Linux В результате выполнения лабораторной работы студент получает навык развертывания VPN базовыми средствами ОС Linux с использованием L2TP.
7	Пакетный фильтр ОС Linux iptables. В результате выполнения лабораторной работы студент отрабатывает умение по настройке и использование встроенного пакетного фильтра ОС Linux iptables.
8	Прокси-сервер SQUID В результате выполнения лабораторной работы студент учится настроивать и использовать прокси-сервера SQUID.
9	Средства обнаружения вторжений Snort В результате выполнения лабораторной работы студент отрабатывает умение по использованию и настройке средств обнаружения вторжений Snort.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Изучение дополнительной литературы.
2	Подготовка к практическим занятиям.
3	Выполнение курсовой работы.
4	Подготовка к промежуточной аттестации.
5	Подготовка к текущему контролю.

4.4. Примерный перечень тем курсовых работ

1) Технология SIEM и ее функциональные возможности. Преимущества и недостатки по сравнению с другими решениями.

2) Сетевые пакетные фильтры и их разновидности.

3) Посредники и особенности их применения для сетевой защиты.

4) Технология NAT и варианты ее развития

5) Сеансовый посредник SoC и специфика его применения

6) Инспекторы состояния как инструмент фильтрации для обеспечения требуемого уровня ИБ.

7) Обеспечение межсетевой защиты ресурсов посредством UTM-устройств и NG firmware

8) Виртуальные частные сети и наиболее часто используемые протоколы VPN

9) Характеристика и архитектура протокола IPsec.

10) Системы обнаружения вторжений структуры и принципы построения

11) Сравнительный анализ систем обнаружения вторжений и для сетевой безопасности

12) DLP-системы и их возможности. Анализ часто применяемых DLP-систем.

13) Сетевые сканеры уязвимостей, как средства анализа защищенности сетей

14) Ловушки, как средство сбора информации о злоумышленнике.

15) Защита локальных вычислительных сетей от атак канального уровня

16) Защита информации от ПЭМИН

17) Обеспечение аутентификации пользователей и разграничение доступа к информационным ресурсам

18) Обеспечение защиты информационных ресурсов компании от сетевых атак

19) Построение систем безопасности сетевого уровня на базе протокола IPSec

20) Построение отказоустойчивой ЛВС на базе протокола STP

21) Защита рабочих станций сети от вредоносного ПО и несанкционированных действий сотрудников

22) Защита информации и конфиденциальных данных, передаваемых по e-mail

23) Система обнаружения вторжений RealSecure

24) Управление ключами в вычислительных системах

25) Инструментальные средства предотвращения сетевых атак

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

№ п/п	Библиографическое описание	Место доступа
1	Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта В.В. Яковлев, А.А. Корниенко Однотомное издание УМК МПС России , 2002	НТБ (уч.4); НТБ (фб.); НТБ (чз.1)
2	Компьютерные сети. Принципы, технологии, протоколы В.Г. Олифер, Н.А. Олифер Питер , 2006	НТБ (уч.3)
1	Стандарты ИБ. Курс лекций Галатенко В.А. ИНТУИТ.РУ, Интернет-Университет Информ. Технологий М. ,	
2	Безопасность корпоративных сетей Биячуев Т.А. СПБ , 2006	

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).

Microsoft Office.

Распространяемая система виртуализации Virtual Box.

Операционная система Linux.

Свободно распространяемый пакетный фильтр iptables.

Свободно распространяемый прокси-сервер SQUID.

Свободно распространяемые ПО для организации виртуальных сетей OPEN VPN.

Свободно распространяемая система обнаружения вторжений Snort.

Свободно распространяемый сервер удаленного доступа OPENSSH.

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:

Курсовая работа в 8 семестре.
Экзамен в 8 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» М.Я. Клепцов

Согласовано:

Заведующий кафедрой УиЗИ Л.А. Баранов

Председатель учебно-методической
комиссии С.В. Володин