Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ:
Директор
_____А. В. Замятин
«16» июня 2023 г.

Рабочая программа дисциплины

Основы построения защищённых компьютерных сетей

по направлению подготовки / специальности

10.05.01 Компьютерная безопасность

Направленность (профиль) подготовки / специализация:
Анализ безопасности компьютерных систем

Форма обучения
Очная

Квалификация
Специалист по защите информации

Год приема
2023

Код дисциплины в учебном плане: Б1.О.06.03

СОГЛАСОВАНО:
Руководитель ОП
_____В.Н. Тренькаев

Председатель УМК
_____С.П. Сущенко

Томск – 2023

1. Цель и планируемые результаты освоения дисциплины

Целью освоения дисциплины является формирование следующих компетенций:

– ОПК-9 – Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации.

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

– ОПК-18 – Способен проводить анализ защищенности и осуществлять поиск уязвимости компьютерной системы.

– ПК-3 – Способен проектировать программно-аппаратные средств защиты информации компьютерных систем и сетей.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-9.1 Учитывает современные тенденции развития методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных при решении задач своей профессиональной деятельности.

ИОПК-9.2 Обладает знанием и демонстрирует навыки применения базовых методов защиты информации в операционных системах, компьютерных сетях и системах управления базами данных.

ИОПК-16.1 Осуществляет оценку работоспособности применяемых средств защиты информации в компьютерных системах и сетях с использованием штатных средств и методик.

ИОПК-16.2 Осуществляет оценку эффективности применяемых средств защиты информации в компьютерных системах и сетях с использованием штатных средств и методик.

ИОПК-16.3 Определяет уровень защищенности и доверия средств защиты информации в компьютерных системах и сетях.

ИОПК-18.1 Определяет уровень защищенности и доверия в компьютерных системах и прогнозирует возможные пути развития действий нарушителя информационной безопасности.

ИОПК-18.2 Оценивает соответствие механизмов безопасности компьютерной системы требованиям существующих нормативных документов, а также их адекватности существующим рискам.

ИОПК-18.3 Составляет и оформляет аналитический отчет по результатам проведенного анализа, разрабатывает предложения по устранению выявленных уязвимостей.

ИПК-3.1 Разработка технических заданий, эскизных, технических и рабочих проектов работ по защите информации.

2. Задачи освоения дисциплины

– познакомить студентов с основными классическим сетевыми атаками: изучить сетевые атаки: ARP Spoofing, MAC Flooding, MAC Spoofing, VLAN Hopping, ГР Spoofing, TCP Hijacking, DoS- и DDoS-атаки;

– рассмотреть основные протоколы: рассматреть основные протоколы, технологии и механизмы защиты от сетевых атак: VPN, ШР5, Firewall, Proxy, Load Balancing, Post Security.

– рассмотреть технологии и механизмы защиты от сетевых атак: технологии анализа защищенности компьютерных сетей - идентификация устройств, идентификация открытых портов, идентификация сетевых служб и программного обеспечения, уязвимостей.

3. Место дисциплины в структуре образовательной программы

Дисциплина относится к обязательной части образовательной программы. Дисциплина входит в модуль "Специализация".

4. Семестр(ы) освоения и форма(ы) промежуточной аттестации по дисциплине

Седьмой семестр, зачет с оценкой
Восьмой семестр, зачет

5. Входные требования для освоения дисциплины

Для успешного освоения дисциплины требуются результаты обучения по дисциплине «Компьютерные сети».

6. Язык реализации

Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 6 з.е., 216 часов, из которых:
-лекции: 32 ч.
-лабораторные: 64 ч.
в том числе практическая подготовка: 64 ч.
Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины, структурированное по темам

Тема 1. Защита от атак канального уровня
Тема 2. Защита коммутации
Тема 3. Технология VPN
Тема 4. Защита от атак DoS н DDoS
Тема 5. Защита маршрутизации
Тема 6. Защита транспортного уровня
Тема 7. Защита сетевых устройств
Тема 8. Технологии межсетевого экранирования
Тема 9. Методы н технологии обнаружения вторжений
Тема 10. Сканирование защищенности сетей
Тема 11. Дизайн защищенных сетей

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине проводится путем контроля посещаемости, проведения контрольных работ, ответов на вопросы по лекционному материалу, проверки выполнения лабораторных работ и фиксируется в форме контрольной точки не менее одного раза в семестр.

Практическая подготовка оценивается по результатам выполненных лабораторных работ.

10. Порядок проведения и критерии оценивания промежуточной аттестации

Зачет с оценкой в седьмом семестре проводится в письменной форме по билетам. Билет содержит теоретический вопрос. Продолжительность зачета 1,5 часа.

Примерный перечень теоретических вопросов

1. Атаки на STP.

2. Методы и технологии защиты от атак канального уровня.
3. Протоколы GRE и IPSec.
4. Технология SYN Cookie и SYN Proxy.
5. Методы защиты от IP Spoofing.
6. Методы защиты протоколов маршрутизации.
7. Протоколы SSL/TLS.
8. Защищенная настройка TLS.
9. Защищенная настройка маршрутизаторов и коммутаторов.
10. Технологии NAT, statefiil inspection, stateless inspection.
11. Методы обнаружения вторжений в сетях.
12. Атаки MAC Flooding, MAC Spoofing, VLAN Hopping, ARP Spoofing.

Результаты зачета с оценкой определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценка «отлично» ставится, если полно раскрыто содержание материала вопроса; материал изложен грамотно, в определенной логической последовательности.

«Хорошо»: вопрос изложен систематизировано и последовательно; продемонстрировано умение анализировать материал, однако в изложении допущены небольшие пробелы, не исказившие содержание ответа.

«Удовлетворительно»: неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса и продемонстрированы умения, достаточные для дальнейшего усвоения материала.

«Неудовлетворительно»: полностью отсутствует ответ; не раскрыто основное содержание вопроса; обнаружено незнание или непонимание большей или наиболее важной части вопроса.

11. Учебно-методическое обеспечение

а) Электронный учебный курс по дисциплине в электронном университете «Moodle» - https://moodle.tsu.ru/course/view.php?id= 10190, https://moodle.tsu.ru/course/view.php?id= 10192

б) Оценочные материалы текущего контроля и промежуточной аттестации по дисциплине (Приложение 1).

12. Перечень учебной литературы и ресурсов сети Интернет

а) основная литература:

– W. Richard Stevens, Kevin R. Fall. TCP/IP Illustrated, Volume 1: The Protocols (2nd edition), 2012. Addison Wesley.

– Sean Convery. Network Security Architectures. -ISBN-13: 978-1587142970.

б) дополнительная литература:

– Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости: учеб, пособие. М.: Издательский центр «Академия», 2009. 272 с.

в) ресурсы сети Интернет:

– Cisco Network Security Baseline. - URL:

http://www.cisco.com/c/en/us/td/docs/solutions/Enteiprise/Security/BaseUne_Security/seciirebas ebook.html.

– Cisco SAFE reference Guide. - URL: http://www.cisco.coш/c/en/us/td/docs/solutions/Enteφrise/Security/SAFE_RG/SAFE_rg.htшl

– TCP-IP Guide. - URL: http://www.tcpipguide.com/

– Общероссийская Сеть КонсультантПлюс Справочная правовая система. http://www.consultant.ru

13. Перечень информационных технологий

а) лицензионное и свободно распространяемое программное обеспечение:
Cisco Packet Tracer, GNS3, VirtualBox, VMWare Player, Metasploit, Metasploitable 2/3, Kali Linux.

б) информационные справочные системы:

– Электронный каталог Научной библиотеки ТГУ – http://chamo.lib.tsu.ru/search/query?locale=ru&theme=system

– Электронная библиотека (репозиторий) ТГУ – http://vital.lib.tsu.ru/vital/access/manager/Index

– ЭБС Лань – http://e.lanbook.com/

– ЭБС Консультант студента – http://www.studentlibrary.ru/

– Образовательная платформа Юрайт – https://urait.ru/

– ЭБС ZNANIUM.com – https://znanium.com/

– ЭБС IPRbooks – http://www.iprbookshop.ru/

14. Материально-техническое обеспечение

Аудитории для проведения занятий лекционного типа.

Аудитории для проведения лабораторных занятий, индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации.

Помещения для самостоятельной работы, оснащенные компьютерной техникой и доступом к сети Интернет, в электронную информационно-образовательную среду и к информационным справочным системам.

15. Информация о разработчиках

Колегов Денис Николаевич, канд. техн. наук, доцент, кафедра компьютерной безопасности, доцент