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

Институт прикладной математики и компьютерных наук

УТВЕРЖДЕНО:
Директор
А. В. Замятин

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
**2024**

СОГЛАСОВАНО:
Руководитель ОП
В.Н. Тренькаев

Председатель УМК
С.П. Сущенко

Томск – 2024

## 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: рассмотреть 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 Блоку 1 «Дисциплины (модули)».

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

Методы защиты информации, передаваемой на уровне канала связи. Обсуждаются такие атаки, как ARP Spoofing и атаки на Ethernet.

Тема 2. Защита коммутации

Подходы к защите сетевых коммутаторов и предотвращению атак, направленных на эксплуатацию уязвимостей в сетевых устройствах.

Тема 3. Технология VPN

Изучение виртуальных частных сетей (VPN), их архитектуры, протоколов и методов защиты данных при передаче по сетям общего пользования

Тема 4. Защита от атак DoS н DDoS.

Обсуждаются виды атак «отказ в обслуживании», их последствия, рассматриваются методы предотвращения и смягчения таких атак.

Тема 5. Защита маршрутизации

Обеспечение безопасности протоколов маршрутизации и предотвращение злоупотребления, такие как маршрутизация по ложным путям.

Тема 6. Защита транспортного уровня

Изучение механизмов защиты, таких как TLS/SSL, и их роль в обеспечении конфиденциальности и целостности данных на транспортном уровне.

Тема 7. Защита сетевых устройств

Рассматриваются методы, используемые для защиты маршрутизаторов, коммутаторов и других сетевых устройств от атак и несанкционированного доступа.

Тема 8. Технологии межсетевого экранирования

Межсетевые экраны (firewall), их типы, конфигурация и использование для защиты сетевой инфраструктуры.

Тема 9. Методы и технологии обнаружения вторжений

Рассматриваются системы обнаружения вторжений (IDS), методы их работы и тактики для выявления злонамеренной активности в сети.

Тема 10. Сканирование защищенности сетей

Методы анализа безопасности сетевой инфраструктуры, включая сканирование уязвимостей и тестирование на проникновение.

Тема 11. Дизайн защищенных сетей.

Обсуждаются принципы проектирования сетей с учетом безопасности, включая архитектуру, выбор оборудования и создание политик безопасности.

**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.

Оценочные материалы текущего контроля размещены на сайте ТГУ в разделе «Информация об образовательной программе» - https://www.tsu.ru/sveden/education/eduop/.

**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 с оценкой 1 час.

Зачет в восьмом семестре проводится в письменной форме по билетам. Билет содержит теоретический вопрос. Продолжительность зачета 1 час.

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.

Оценочные материалы для проведения промежуточной аттестации размещены на сайте ТГУ в разделе «Информация об образовательной программе» - https://www.tsu.ru/sveden/education/eduop/.

**11. Учебно-методическое обеспечение**

а) Электронный учебный курс по дисциплине в LMS IDO

- 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.

## 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.cou/c/en/us/td/docs/solutions/Enteфrise/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

Останин Сергей Александрович, канд. техн. наук, доцент, доцент кафедры компьютерной безопасности.

Вихорь Наталия Анатольевна, канд. физ.-мат. наук, доцент, доцент кафедры компьютерной безопасности.