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

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ:
Проректор по ОД

_____ Е.В. Луков

«03» сентября 2025 г.

Рабочая программа дисциплины

Основы построения защищенных компьютерных сетей

по направлению подготовки

10.03.01 Информационная безопасность

Направленность (профиль) подготовки:
Безопасность компьютерных систем

Форма обучения
Очная

Квалификация
Бакалавр

Год приема
2026

СОГЛАСОВАНО:
Руководитель ОП
В.Н. Тренькаев

Председатель УМК
С.П. Сущенко

Томск – 2025

1. Цель и планируемые результаты освоения дисциплины

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-1.4. Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями.

ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты.

ОПК-12. Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений.

ПК-3. Способен проводить анализ уязвимостей внедряемой системы защиты информации.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-1.4.1. Понимает принципы организации, состав и алгоритмы работы механизмов защиты информации, стандарты оценивания безопасности компьютерных систем и сетей.

ИОПК-1.4.2. Определяет уровень защищенности компьютерных систем и сетей и прогнозирует возможные пути развития действий нарушителя информационной безопасности.

ИОПК-1.4.3. Оценивает соответствие механизмов безопасности требованиям существующих нормативных документов, а также их адекватности существующим рискам.

ИОПК-10.1. Понимает принципы формирования политики информационной безопасности в соответствии с нормативными требованиями.

ИОПК-10.2. Умеет организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности на защищаемом объекте.

ИОПК-10.3. Демонстрирует навыки формирования и реализации политики информационной безопасности на защищаемом объекте.

ИОПК-12.1. Понимает принципы работы информационных систем, средств обеспечения защиты информации, методики построения моделей угроз безопасности информации.

ИОПК-12.2. Демонстрирует навыки формирования исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений.

ИПК-3.1. Проводит анализ уязвимости средств системы защиты информации.

ИПК-3.2. Устраняет выявленные уязвимости системы защиты информации.

ИПК-3.3. Разрабатывает предложения по совершенствованию системы управления защитой 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

Пятый семестр, экзамен
Шестой семестр, экзамен

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 8 з.е., 288 часов, из которых:
– лекции: 64 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 выполнения практических контрольных заданий, 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

Экзамен в пятом и шестом семестрах проводится в письменной форме по билетам. Экзаменационный билет содержит два теоретических вопроса. Продолжительность экзамена 1,5 часа.

Результаты экзамена определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Условием допуска к экзамену является выполнение более 50% лабораторных работ. Сдача более 80% лабораторных работ является условием получения оценки «хорошо» или «отлично» на экзамене.

Оценка «отлично» ставится, если полно раскрыто содержание материала вопроса; материал изложен грамотно, в определенной логической последовательности; сдано более 80% лабораторных работ.

«Хорошо»: ответ на вопрос изложен систематизировано и последовательно; продемонстрировано умение анализировать материал, однако в изложении допущены небольшие пробелы, не исказившие содержание ответа; сдано более 80% лабораторных работ.

«Удовлетворительно»: неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса и продемонстрированы умения, достаточные для дальнейшего усвоения материала; сдано не менее 50% лабораторных работ.

«Неудовлетворительно»: полностью отсутствует ответ; не раскрыто основное содержание вопроса; обнаружено незнание или непонимание большей/наиболее важной части вопроса; сдано менее 50% лабораторных работ.

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

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

в) Семинарских / практических занятий по дисциплине нет.

г) Методические указания по организации самостоятельной работы студентов.

Самостоятельная работа организуется в следующих формах: работа с материалами лекции; изучение вопросов, выносимых за рамки лекционных занятий; подготовка к лабораторным занятиям; подготовка к рубежному контролю по теме/разделу (аттестации). Работу с конспектом лекции целесообразно проводить непосредственно после ее прослушивания. Необходимым является глубокое освоение содержания лекции и свободное владение им, в том числе использованной в ней терминологии. Изучение вопросов, выносимых за рамки лекционных занятий, предполагает самостоятельное изучение студентами дополнительной литературы. Лабораторные работы, приведенные в планах занятий, выполняются студентами в обязательном порядке. Методические указания обучающимся по освоению дисциплины: целенаправленно, систематически и планомерно работать со слайдами лекций; изучать рекомендуемую литературу, добывая новые/обобщая полученные знания; консультироваться с преподавателем при возникновении вопросов; активно использовать учебно-методический комплекс на базе LMS IDO ТГУ; работать с тематическими форумами в сети Интернет.

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/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.

Наименование оборудованных учебных кабинетов, объектов для проведения практических занятий, объектов физической культуры и спорта с перечнем основного оборудования	Адрес (местоположение) учебных кабинетов, объектов для проведения практических занятий, объектов физической культуры и спорта (с указанием площади и номера помещения в соответствии с документами бюро технической инвентаризации)
Учебная аудитория для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Аудитория № 118. Учебная мебель, оборудование, программное обеспечение: 45 столов по 2 места; 90 стульев; 1 интерактивная доска; Microsoft Windows 10, Microsoft Office 2010. (Лицензия №47729022 от 26.11.2010).	634050,Томская область, г. Томск, пр-т Ленина, 36, стр.7 (78 по паспорту БТИ) Площадь 61,1 м^2.
Учебная аудитория для проведения лабораторных и практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Аудитория № 103 Учебная мебель, оборудование, программное обеспечение: 13 столов по 1 месту; 13 стульев; 1 меловая доска; 1 интерактивная доска; 1 проектор; 13 системных блоков (Intel Core Core i7-8700, AsusTek TUFB360-plus gaming, 16Гб DDR3); 13 мониторов; Microsoft Windows 10 Professional x64, Microsoft Office 2010 Standart, Microsoft Office 2003 Professional (only for MS Access), Microsoft Visual Studio 2022	634050,Томская область, г. Томск, пр-т Ленина, 36, стр.7 (7 по паспорту БТИ) Площадь 42,3 м^2.

Community, Visual Studio Code, Dr.Web Desktop Security Suite, 1С:Предприятие учебная версия, 7-Zip, Adobe Reader, Android Studio, Far Manager, FreeCommander, Google Chrome, Яндекс Браузер, GPL Ghostscript, Gsview, IntelliJ IDEA Community Edition, Java SDK, Lazarus, Mathsoft Mathcad 13, 15, Mathsoft Prime 3.1, StatSoft Statistica 13, FreeMat, Scilab, NetBeans IDE 22, Eclipse IDE 2024, PyCharm Community 2024, R Project, RapidMiner Studio, Rstudio, Anaconda, JASP (Лицензия №47729022 от 26.11.2010, договор №7193 от 14.10.2015, договор № 2016 от 16.04.2018) нелинейный локатор «ЦИКЛОН - М1А», локатор-рефлектометр двухпроводных линий «БОР-1», сканирующий приемник AR 8200, оборудование радиодоступа WOP-2ac, Simple Promela Interpreter, ОС Astra Linux Special Edition, Secret Net Studio, ViPNet CSP, JaCarta SecurLogon, IDS/IPS Suricata, Infection Monkey, Wireshark, PfSense, Ntopng, Grype, Metasploit framework, Cisco Packet Tracer, GNS-3, EVE-NG, KatharaFramework, InfoWatch Traffic Monitor.	
Учебная аудитория для самостоятельной работы Аудитория № 103А Учебная мебель, оборудование, программное обеспечение: 13 столов по 1 месту; 13 стульев; 1 меловая доска; 1 интерактивная доска; 1 проектор; 13 системных блоков (Intel Core i7-4790/Ga H97 HD 3/2x 8Gb DDR 3); 13 мониторов; Microsoft Windows 10 Professional x64, Microsoft Office 2010 Standart, Microsoft Office 2003 Professional (only for MS Access), Microsoft Visual Studio 2022 Community, Visual Studio Code, Dr.Web Desktop Security Suite, 1С:Предприятие учебная версия, 7-Zip, Adobe Reader, Android Studio, Far Manager, FreeCommander, Google Chrome, Яндекс Браузер, GPL Ghostscript, Gsview, IntelliJ IDEA Community Edition, Java SDK, Lazarus, Mathsoft Mathcad 13, 15, Mathsoft Prime 3.1, StatSoft Statistica 13, FreeMat, Scilab, NetBeans IDE 22, Eclipse IDE 2024, PyCharm Community 2024, R Project, RapidMiner Studio, Rstudio, Anaconda, JASP (Лицензия №47729022 от 26.11.2010, договор №7193 от 14.10.2015, договор № 2016 от 16.04.2018).	634050,Томская область, г. Томск, пр-т Ленина, 36, стр.7 (72 по паспорту БТИ) Площадь 43 м^2.

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.