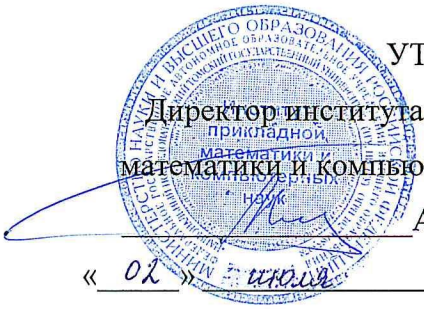
МИНОБРНАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Институт прикладной математики и компьютерных наук



УТВЕРЖДАЮ
Директор института прикладной
математики и компьютерных наук
_____А.В. Замятин
«_02_» _июля_ 2021 г.

Основы построения защищённых компьютерных сетей

рабочая программа дисциплины

Закреплена за кафедрой	*компьютерной безопасности*
Учебный план	*10.05.01 Компьютерная безопасность,* *профиль «Анализ безопасности компьютерных систем»*
Форма обучения	*очная*
Общая трудоёмкость	*6 з.е.*
Часов по учебному плану	*216*
в том числе:	
аудиторная контактная работа	*103,3*
самостоятельная работа	*112,7*
Вид(ы) контроля в семестрах	
экзамен/зачет/зачет с оценкой	*Семестр 7 – зачет с оценкой* *Семестр 8 – зачет*

Томск-2021

Программу составил:
канд. техн. наук, доцент,
заведующий кафедрой компьютерной безопасности С.А. Останин

Рецензент:
канд. физ.-мат. наук, доцент,
доцент кафедры компьютерной безопасности Н.А. Вихорь

Рабочая программа дисциплины «Основы построения защищённых компьютерных сетей» разработана в соответствии с образовательным стандартом высшего образования – специалитет, самостоятельно устанавливаемым федеральным государственным автономным образовательным учреждением высшего образования «Национальный исследовательский Томский государственный университет» по специальности 10.05.01 Компьютерная безопасность (Утвержден Ученым советом НИ ТГУ, протокол от 30.06.2021 г. № 06).

Рабочая программа одобрена на заседании кафедры компьютерной безопасности

Протокол от 02 июня 2021 г. № 06

Заведующий кафедрой компьютерной безопасности,
канд. техн. наук, доцент С.А. Останин

Рабочая программа одобрена на заседании учебно-методической комиссии института прикладной математики и компьютерных наук (УМК ИПМКН)

Протокол от 17 июня 2021 г. № 05

Председатель УМК ИПМКН,
д-р техн. наук, профессор С.П. Сущенко

Цель освоения дисциплины

Цель – познакомить студентов с основными классическим сетевыми атаками; рассмотреть основные протоколы, технологии и механизмы защиты от сетевых атак.

1. Место дисциплины в структуре ОПОП

Дисциплина «Основы построения защищённых компьютерных сетей» относится к обязательной части Блока 1 «Дисциплины», входит в модуль «Специализация».

Пререквизиты дисциплины: Компьютерные сети.

Постреквизиты дисциплины: Научно-исследовательская работа.

2. Компетенции и результаты обучения, формируемые в результате освоения дисциплины

Таблица 1.

Компетенция	**Индикатор компетенции**	**Код и наименование результатов обучения** (планируемые результаты обучения по дисциплине, характеризующие этапы формирования 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.	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.	ОР-9.1.1 Умеет формулировать и настраивать политику безопасности основных операционных систем. ОР-9.1.2 Умеет формулировать и настраивать политику безопасности локальных компьютерных сетей
ОПК-16 Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях.	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.	ОР-16.1.1 Владеет средствами инструментального анализа работоспособности и защищенности компьютерных сетей ОР-16.1.2 Оценивает эффективность применяемых средств защиты информации в компьютерных системах и сетях
ОПК-18. Способен проводить анализ защищенности и осуществлять поиск уязвимости компьютерной системы.	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	ОР-18.1.1 Знает механизмы реализации атак в сетях, реализующих протоколы интернет транспортного и сетевого уровней, защитные механизмы и средства обеспечения сетевой безопасности ОР-18.1.2 Знает средства и методы предотвращения вторжений ОР-18.1.3 Владеет основными средствами

	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.	анализа защищенности компьютерных сетей ОР-18.1.4 Умеет применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в компьютерных сетях

3. Структура и содержание дисциплины
3.1. Структура и трудоемкость видов учебной работы по дисциплине

Общая трудоемкость дисциплины составляет 12 зачетных единиц, 432 часа.

Таблица 2.

Вид учебной работы	Трудоемкость в академических часах		
	7 семестр	8 семестр	всего
Общая трудоемкость	144	72	216
Контактная работа:	69,45	33,85	103,3
Лекции (Л):	32		32
Практики (ПЗ)			
Лабораторные работы (ЛР)	32	32	64
Семинары (СЗ)			
Групповые консультации	2		2
Индивидуальные консультации	3,2	1,6	4,8
Промежуточная аттестация	0,25	0,25	0,5
Самостоятельная работа обучающегося:	74,55	38,15	112,7
- изучение учебного материала, публикаций	30	-	30
- подготовка к лабораторным/практическим занятиям/коллоквиумам	37,8	33	70,8
- подготовка к рубежному контролю по теме/разделу	6,75	5,15	6,75
Вид промежуточной аттестации (зачет, зачет с оценкой, экзамен)	**Зачет с оценкой**	**Зачет**	**Зачет с оценкой, зачет**

3.2. Содержание и трудоемкость разделов дисциплины

Таблица 3.

Код занятия	Наименование разделов и тем и их содержание	Вид учебной работы, занятий, контроля	Семестр	Часы в электронной форме	Всего (час.)	Литература	Код (ы) результата(ов) обучения
1	Защита от атак канального уровня	Лекции Лаб.раб.	7		2 2	1, 2, 3	ОР-16.1.1, ОР-16.1.2, ОР-18.1.1 – 18.1.4
2	Защита коммутации	Лекции Лаб.раб.	7		3 3	1, 2, 3	ОР-16.1.1, ОР-16.1.2, ОР-18.1.1 – 18.1.4
3	Технология VPN	Лекции Лаб.раб.	7		3 3	1, 2, 3	ОР-9.1.1, ОР-9.1.2 ОР-16.1.1, ОР-16.1.2,
4	Защита от атак DoS н DDoS	Лекции Лаб.раб.	7		3 3	1, 2, 3	ОР-16.1.1, ОР-16.1.2, ОР-18.1.1 – 18.1.4
5	Защита маршрутизации	Лекции Лаб.раб.	7		3 3	1, 2, 3	ОР-16.1.1, ОР-16.1.2,
6	Защита транспортного уровня	Лекции Лаб.раб.	7		3 3	1, 2, 3	ОР-18.1.1 – 18.1.4
7	Защита сетевых устройств	Лекции Лаб.раб.	7		3 3	1, 2, 3	ОР-16.1.1, ОР-16.1.2, ОР-18.1.1 – 18.1.4
8	Технологии межсетевого экранирования	Лекции Лаб.раб.	7		3 3	1, 2, 3	ОР-9.1.1, ОР-9.1.2
9	Методы н технологии обнаружения вторжений	Лекции Лаб.раб.	7		3 3	1, 2, 3	ОР-9.1.1, ОР-9.1.2
10	Сканирование защищенности сетей	Лекции Лаб.раб.	7		3 3	1, 2, 3	ОР-16.1.1, ОР-16.1.2, ОР-18.1.1 – 18.1.4
11	Дизайн защищенных сетей	Лекции Лаб.раб.	7		3 3	1, 2, 3	ОР-9.1.1, ОР-9.1.2
12	СРС (изучение учебного материала, подготовка к лабораторным занятиям)	СРС	7		67,8	1, 2, 3	ОР-9.1.1, ОР-9.1.2 ОР-16.1.1, ОР-16.1.2, ОР-18.1.1 – 18.1.4
13	Защита от атак канального уровня	Лаб.раб.	8		3	1, 2, 3	ОР-18.1.1 – 18.1.4
14	Защита коммутации	Лаб.раб.	8		3	1, 2, 3	ОР-18.1.1 – 18.1.4
15	Технология VPN	Лаб.раб.	8		3	1, 2, 3	ОР-9.1.1, ОР-9.1.2 ОР-18.1.1 – 18.1.4
16	Защита от атак DoS н DDoS	Лаб.раб.	8		3	1, 2, 3	ОР-18.1.1 – 18.1.4
17	Защита маршрутизации	Лаб.раб.	8		3	1, 2, 3	ОР-18.1.1 – 18.1.4

18	Защита транспортного уровня	Лаб.раб.	8		3	1, 2, 3	ОР-18.1.1 – 18.1.4
19	Защита сетевых устройств	Лаб.раб.	8		3	1, 2, 3	ОР-18.1.1 – 18.1.4
20	Технологии межсетевого экранирования	Лаб.раб.	8		3	1, 2, 3	ОР-9.1.1, ОР-9.1.2
21	Методы н технологии обнаружения вторжений	Лаб.раб.	8		3	1, 2, 3	ОР-9.1.1, ОР-9.1.2
22	Сканирование защищенности сетей	Лаб.раб.	8		3	1, 2, 3	ОР-16.1.1, ОР-16.1.2, ОР-18.1.1 – 18.1.4
23	Дизайн защищенных сетей	Лаб.раб.	8		2	1, 2, 3	ОР-9.1.1, ОР-9.1.2
24	СРС (подготовка к лабораторным занятиям)	СРС	7		33	1, 2, 3	ОР-9.1.1, ОР-9.1.2 ОР-16.1.1, ОР-16.1.2, ОР-18.1.1 – 18.1.4
25	Подготовка к промежуточной аттестации в форме зачета с оценкой	СРС	7		6,75	1, 2, 3	ОР-9.1.1, ОР-9.1.2 ОР-16.1.1, ОР-16.1.2, ОР-18.1.1 – 18.1.4
26	Прохождение промежуточной аттестации в форме зачета с оценкой	ЗО	7		2,25		ОР-9.1.1, ОР-9.1.2 ОР-16.1.1, ОР-16.1.2, ОР-18.1.1 – 18.1.4
27	Подготовка к промежуточной аттестации в форме зачета	СРС	7		5,15	1, 2, 3	ОР-9.1.1, ОР-9.1.2 ОР-16.1.1, ОР-16.1.2, ОР-18.1.1 – 18.1.4
28	Прохождение промежуточной аттестации в форме зачета	З	7		0,25		ОР-9.1.1, ОР-9.1.2 ОР-16.1.1, ОР-16.1.2, ОР-18.1.1 – 18.1.4

4. Образовательные технологии, учебно-методическое и информационное обеспечение для освоения дисциплины

Формат обучения – лекции, лабораторные работы, самостоятельная работа.

Во вводной части изучаются основные классические сетевые атаки: ARP Spoofing, MAC Flooding, MAC Spoofing, VLAN Hopping, IP Spoofing, TCP Hijacking, DoS- и DDoS-атаки. Во второй части рассматриваются основные протоколы, технологии и механизмы защиты от сетевых атак: VPN, ШР5, Firewall, Proxy, Load Balancing, Post Security. В третьей части курса рассматривается технология анализа защищенности компьютерных сетей: идентификация устройств, идентификация открытых портов, идентификация сетевых служб и программного обеспечения, уязвимостей.

Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения, характеризующих этапы формирования компетенций, и методические материалы, определяющие процедуры оценивания результатов обучения, приведены в Приложении 1 к рабочей программе «Фонд оценочных средств».

Типовые контрольные задания или иные материалы, необходимые для текущей аттестации, и методические материалы, определяющие процедуры оценивания результатов текущей аттестации, приведены в Приложении 2 к рабочей программе «Примерные оценочные средства текущей аттестации».

4.1. Рекомендуемая литература и учебно-методическое обеспечение

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

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

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

4.2. Базы данных и информационно-справочные системы, в том числе зарубежные

1. Cisco Network Security Baseline. - URL: http://www.cisco.com/c/en/us/td/docs/solutions/Enteiprise/Security/BaseUne_Security/seciirebasebook.html.
2. Cisco SAFE reference Guide. - URL: http://www.cisco.coш/c/en/us/td/docs/solutions/Enteφrise/Security/SAFE_RG/SAFE_rg.html
3. TCP-IP Guide. - URL: http://www.tcpipguide.com

4.3. Перечень лицензионного и программного обеспечения

Cisco Packet Tracer, GNS3, VirtualBox, VMWare Player, Metasploit, Metasploitable 2/3, Kali Linux.

4.4. Оборудование и технические средства обучения

Для реализации дисциплины необходимы лекционные аудитории и аудитории для проведения лабораторных занятий. Специальные технические средства (проектор, компьютер и т.д.) требуются для демонстрации материала в рамках изучаемых разделов.

5. Преподавательский состав, реализующий дисциплину

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

7. Язык преподавания – русский язык.