Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Тверской государственный университет»

Утверждаю:
Руководитель ООП
Н.А. Семыкина
«4» 09 2021 г.

Рабочая программа дисциплины (с аннотацией)

Основы построения защищенных компьютерных сетей

Специальность

10.05.01 Компьютерная безопасность

Специализация

«Математические методы защиты информации»

Для студентов очной формы обучения

СПЕЦИАЛИТЕТ

Для студентов 5 курса ОФО

Составитель:
Семыкина Н. А.

Тверь 2023

I. Аннотация

1. Цель и задачи дисциплины

Целью освоения дисциплины - теоретическая и практическая подготовка специалистов к деятельности, связанной с построением защищенных сетевых автоматизированных систем, а также обучение принципам и методам защиты информации в компьютерных сетях.

Задачами освоения дисциплины являются:

- 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. Место дисциплины в структуре ООП

Данная дисциплина входит в обязательную часть учебного плана, связана с другими дисциплинами образовательной программы: «Основы информационной безопасности», «Компьютерные сети»», «Операционные системы», «Защита в операционных системах».

Дисциплины, для которых освоение данной дисциплины необходимо как предшествующее: «Научно-исследовательская работа», «Проектно-технологическая практика», «Преддипломная практика».

3. Объем дисциплины: 5 зачетные единицы, 180 академических часов, в том числе:

контактная аудиторная работа: лекции – 34 часов, в т.ч. практическая подготовка – 0 часов;

лабораторные занятия – 34 часов, в т.ч. практическая подготовка – 4 часа;

самостоятельная работа: 112 часа, в том числе контроль 27 часов.

4. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Планируемые результаты освоения образовательной программы (формируемые компетенции)	Планируемые результаты обучения по дисциплине
ОПК-8. Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей	**ОПК-8.4** Применяет методики анализа сетевого трафика

ОПК-10 Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности	**ОПК-10.5** Использует основные протоколы идентификации и аутентификации абонентов сети
ОПК-11. Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации	**ОПК-11.1.** Использует основные формальные модели дискреционного, мандатного, ролевого управления доступом, модели изолированной программной среды и безопасности информационных потоков
ОПК-15 Способен администрировать компьютерные сети и контролировать корректность их функционирования	**ОПК-15.1** Осуществляет проектирование и оптимизацию функционирования компьютерных сетей
	ОПК-15.2 Работает с сетевым оборудованием и сетевым программным обеспечением
ОПК-16. Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях	**ОПК-16.1.** Применяет защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях
	ОПК-16.2. Осуществляет меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты

5. Форма промежуточной аттестации и семестр прохождения – экзамен в 10 семестре.

6. Язык преподавания русский**.**

II. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

Очная форма обучения

		Контактная работа (час.)	

Учебная программа – наименование разделов и тем	Всего (час.)	Лекции	Практические занятия		Самостоятельная работа, в том числе Контроль (час.)
			всего	в т.ч. практическая подготовка	
Раздел 1. Типовые угрозы сетевой безопасности	50	10	10	0	30
Раздел 2. Крипографические методы защиты информации в компьютерных сетях	65	12	10	2	41
Раздел 3. Программно-аппаратные средства обеспечения информационной безопасности в компьютерных сетях	65	12	10	2	41
ИТОГО	180	34	30	4	112

III. Образовательные технологии

Учебная программа – наименование разделов и тем	Вид занятия	Образовательные технологии
Раздел 1. Типовые угрозы сетевой безопасности	лекция лабораторное	Дискуссионные технологии, дистанционные образовательные технологии, проблемная лекция.
Раздел 2. Крипографические методы защиты информации в компьютерных сетях	лекция лабораторное	Дискуссионные технологии, дистанционные образовательные технологии, проблемная лекция, кейс-технология, технология развития креативного мышления
Раздел 3. Программно-аппаратные средства обеспечения информационной безопасности в компьютерных сетях	лекция лабораторное	Дискуссионные технологии, кейс-технология, методы группового решения творческих задач.

IV. Оценочные материалы для проведения текущей и промежуточной аттестации

Оценочные материалы для проведения <u>текущей аттестации</u>

<u>Задания для практических (семинарских) занятий</u>

Раздел I.

Задание 1 (ОПК-8.4, ОПК-15.1; ОПК-15.2): Определите настройки протокола TCP/IP вашего компьютера. Установите и запустите средство анализа сетевого трафика. Осуществите захват сетевого трафика. Осуществите просмотр трафика. В полученных сетевых пакетах убедитесь в наличии полей «источник», «приемник», «тип протокола».

Задание 2 (ОПК-8.4, ОПК-10.5, ОПК-16.1; ОПК-16.2): Создайте на виртуальном компьютере, работающем под управлением ОС Windows 2000, каталоги и в нем небольшой текстовый файл. Предоставьте созданный каталог в сетевой доступ. Включите захват трафика. В основной ОС откройте в сетевом окружении на виртуальном компьютере созданный текстовый файл. Просмотрите полученный трафик. Какой протокол используется для файлового обмена? Какие номера TCP-портов задействованы на приемнике и источнике? Найдите пакет, в котором передается текст открытого вами файла (описание пакета начинается с «R read & X»). Передается ли текст файла в зашифрованном виде?

Раздел II.

Задание 1 (ОПК-8.4, ОПК-11.1, ОПК-15.1; ОПК-15.2): Проверьте возможность анализа сетевого трафика при отключенном протоколе IPSec. Запустите анализатор сетевого трафика. Отправьте текстовый файл (набранный латинскими буквами) на виртуальный компьютер. Просмотрите захваченные пакеты. Убедитесь, что файл передается по протоколу SMB, текст файла передается в открытом виде. Осуществите настройку протокола IPsec.

Задание 2 (ОПК-8.4; ОПК-10.5, ОПК-11.1, ОПК-16.1; ОПК-16.2): Разработать политику для web-сервера, на котором разрешен только трафик через порты TCP/80 и TCP/443 из любой точки.

Задание 3 (ОПК-8.4; ОПК-11.1, ОПК-15.1; ОПК-15.2, ОПК-16.1; ОПК-16.2): Пусть существует некая организация, в которой в удаленных друг от друга офисах работают два пользователя. Требуется с использованием технологии виртуальных машин создать структуру сети, состоящую из двух виртуальных узлов, и установить защищенное соединение (рис. 4.31). Основная ОС имитирует работу компьютера стороннего наблюдателя и используется для анализа сетевого трафика.

Раздел III.

Задание 1 (ОПК-10.5, ОПК-11.1, ОПК-16.1; ОПК-16.2): Запустить приложение администрирования WinRoute, подключившись к «LocalHost» как пользователь Admin с пустым паролем. Создать необходимые правила для разрешения web-сервиса внутренним пользователям и правило, запрещающее все остальное (для этой цели можно использовать последнюю строку «Any interface»). Проверить правильность функционирования МЭ.

Задание 2 (ОПК-10.5, ОПК-11.1, ОПК-15.1; ОПК-15.2, ОПК-16.1; ОПК-16.2): Необходимо ограничить пользователя компьютера «PC» в использовании web-сервиса так, чтобы он мог работать только с сервером «OUT2» (рисунок). Обратите внимание на правильную последовательность определения правил фильтрации.

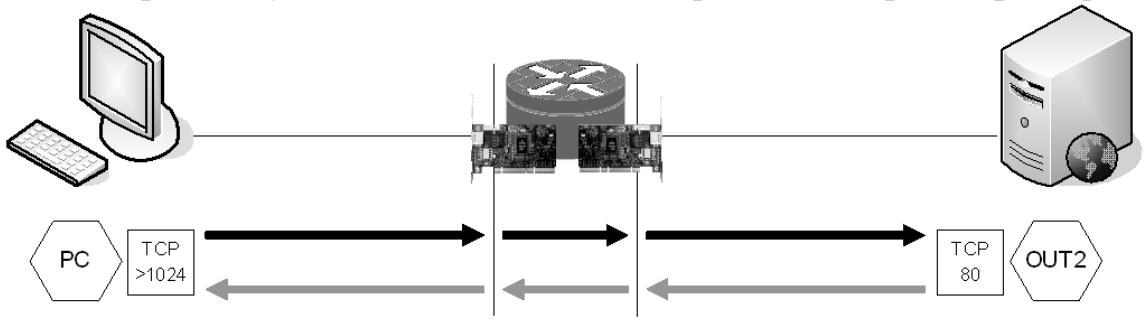

Схема информационного обмена по условию задачи № 2

Оценочные материалы для проведения <u>промежуточной аттестации</u>

Проверяемые индикаторы достижения компетенций: ОПК-8.4; ОПК-10.5; ОПК-11.1; ОПК-15.1; ОПК-15.2; ОПК-16.1; ОПК-16.2.

Каждый студент решает индивидуальное задание и отвечает на теоретический вопрос.

Примерные вопросы к экзамену

1. Классификации сетевых угроз, уязвимостей и атак.
2. Атаки на реализации сетевых протоколов, отдельные узлы и службы.
3. Основные механизмы проведения сетевых атак на различных уровнях модели ISO/OSI.
4. Проблемы обеспечения конфиденциальности, целостности и доступности информации на различных уровнях модели ISO/OSI.
5. Удаленное определение версии ОС с использованием особенностей реализации стека протоколов TCP/IP.
6. Методы сканирования портов. Методы обнаружения пакетных сниферов. Методы обхода МЭ.
7. Методы перехвата сетевых соединений в сетях TCP/IP.
8. Примеры сетевых атак в сетях TCP/IP. Технические меры защиты от сетевых атак.
9. Криптографические протоколы обеспечения безопаности
10. Назначение, основные возможности, принципы функционирования и варианты реализации VPN.
11. Развертывание VPN базовыми средствами ОС Linux с использованием IPSEC.
12. Развертывание VPN базовыми средствами ОС Linux с использованием L2TP.
13. Организация туннелей с использованием ssh.
14. Настройка и использование встроенного пакетного фильтра ОС Linux iptables.
15. Настройка и использование прокси-сервера SQUID.
16. Использование и настройка средства обнаружения вторжений Snort.
17. Межсетевые экраны (МЭ). Место и роль МЭ в обеспечении сетевой безопасности. Классификация МЭ. Требования к МЭ.

18. Реализация сетевой политики безопасности с использованием МЭ.
19. Системы обнаружения вторжений (СОВ). Назначение и возможности средств обнаружения вторжений на хосты, протоколы и сетевые службы.
20. Выявление атак на основе сигнатур атак и выявления аномалий.
21. Аудит прикладных служб.
22. Средства обнаружения уязвимостей сетевых служб. Способы противодействия вторжениям.
23. Системы виртуальных ловушек (Honey Pot и Padded Cell).

Вид и способ проведения промежуточной аттестации: индивидуальный устный опрос сочетается с самостоятельной практической работой студента.

Критерии оценивания и шкала оценивания:

Максимально возможное количество баллов – **5** баллов. Для получения положительной оценки на экзамене необходимо выполнить задачу и ответить на теоретический вопрос с суммарной оценкой не менее 3-х балов.

5 баллов:

Ответ на вопрос демонстрирует знание и корректное использование терминологии. Факты и примеры в полном объеме обосновывают выводы. Имеется полное верное решение задачи, включающее правильный ответ.

4 балла:

Ответ на вопрос демонстрирует знание и корректное использование терминологии. Ответ не содержит фактических ошибок. Дано верное решение задачи, но в решении имеются неверные записи И/ИЛИ арифметические ошибки.

3 балла:

Ответ демонстрирует знание и корректное использование терминологии. Решение содержит фактические ошибки, не искажающие общего смысла.

0-2 баллов:

В ответе преобладают рассуждения общего характера И/ИЛИ содержит существенные фактические ошибки, искажающие смысл. Решение не дано ИЛИ дано неверное решение.

V. Учебно-методическое и информационное обеспечение дисциплины

1) Рекомендуемая литература

а) Основная литература

Долозов Н.Л. Компьютерные сети [Электронный ресурс]: учебно-методическое пособие/ Долозов Н.Л.— Электрон. текстовые данные.— Новосибирск: Новосибирский государственный технический университет, 2013.— 112 c.— Режим доступа: http://www.iprbookshop.ru/45377.html

Урбанович П. П. Компьютерные сети : учебное пособие / П. П. Урбанович, Д. М. Романенко; Белорусский государственный технологический университет. - Вологда : Инфра-Инженерия, 2022. - 460 с. - ВО - Бакалавриат. Режим доступа: https://znanium.com/catalog/document?id=417225

Воробьев С. П. Компьютерные сети и сетевая безопасность [Электронный ресурс] : учебное пособие / С. П. Воробьев, С. Н. Широбокова, Р. К. Литвяк. -

Новочеркасск : ЮРГПУ (НПИ), 2022. - 216 с. – Режим доступа: https://e.lanbook.com/book/292247

Артюшенко В. В. Компьютерные сети и телекоммуникации : учебно-методическая литература / В. В. Артюшенко, А. В. Никулин; Новосибирский государственный технический университет. - Новосибирск : Новосибирский государственный технический университет (НГТУ), 2020. - 72 с. - ВО - Бакалавриат. – Режим доступа: https://znanium.com/catalog/document?id=396946

б) Дополнительная литература

Борисов С. П. Компьютерные сети. Анализ и диагностика : учебное пособие. Ч. 1 : Компьютерные сети. Анализ и диагностика. Часть 1 / С. П. Борисов. - Москва : РТУ МИРЭА, 2021. - 67 с. – Режим доступа: https://e.lanbook.com/book/176562

Борисов С. П. Компьютерные сети. Анализ и диагностика : учебное пособие. Ч. 2 : Компьютерные сети. Анализ и диагностика. Часть 2 / С. П. Борисов. - Москва : РТУ МИРЭА, 2022. - 72 с. – Режим доступа: https://e.lanbook.com/book/240026

Борисов С. П. Компьютерные сети. Анализ и диагностика : учебное пособие. Ч. 3 : Компьютерные сети. Анализ и диагностика. Часть 3 / С. П. Борисов. - Москва : РТУ МИРЭА, 2022. - 77 с. – Режим доступа: : https://e.lanbook.com/book/240179

2) Программное обеспечение

Google Chrome	бесплатно
Kaspersky Endpoint Security 10 для Windows	Акт на передачу прав ПК545 от 16.12.2022
Lazarus	бесплатно
OpenOffice	бесплатно
Многофункциональный редактор ONLYOFFICE бесплатное ПО	бесплатно
ОС Linux Ubuntu бесплатное ПО	бесплатно

3) Современные профессиональные базы данных и информационные справочные системы

1. ЭБС Лань https://e.lanbook.com/ Договор № 4-е/23 от 02.08.2023 г.

2. ЭБС Znanium.com https://znanium.com/ Договор № 1106 эбс от 02.08.2023 г.

3. ЭБС Университетская библиотека online https://biblioclub.ru Договор № 02-06/2023 от 02.08.2023 г.

4. ЭБС ЮРАЙТ https://urait.ru/ Договор № 5-е/23 от 02.08.2023 г.

5. ЭБС IPR SMART https://www.iprbookshop.ru/ Договор № 3-е/23К от 02.08.2023 г.

6. https://cyberleninka.ru/ научная электронная библиотека «Киберленинка».
7. Научная электронная библиотека eLIBRARY.RU (подписка на журналы) https://elibrary.ru/projects/subscription/rus_titles_open.asp;
8. Репозитарий ТвГУ http://eprints.tversu.ru

4) Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины:

www.fstec.ru Федеральная служба по техническому и экспортному контролю (ФСТЭК России)

http://www.intuit.ru/ Национальный Открытый Университете «ИНТУИТ»

http://www.cisco.com/c/ru_ru/index.html Сетевой Академии Cisco

VI. Методические материалы для обучающихся по освоению дисциплины

Методические рекомендации по организации самостоятельной работы студентов

На лекциях будет представлен необходимый теоретически материал по темам и представлены практические задания для решения на занятиях в аудитории под руководством преподавателя и самостоятельно. Многие задачи являются стандартными и имеют уже готовые шаблоны (алгоритмы) решения, тем не менее, для получения большего познавательного и учебного эффекта, рекомендуется написание собственного оригинального кода.

Самостоятельная работа студентов в рамках данной дисциплины в основном состоит в подготовке к практическим занятиям и работе с разными источниками. Освоению учебного материала большую помощь окажет личный творческий подход, связанный с дополнительным просмотром материала по отдельным темам.

Самостоятельная работа является необходимой на всей стадиях и при всех формах изучения предмета. Важно помнить, что часы для самостоятельной работы, из всего объема времени затраченного на дисциплину, будут превосходить иные виды работ. Важно продумать стиль фиксации нового и важного материала.

Рекомендуется немедленно обсуждать любые возникшие в процессе обучения вопросы, проблемы и неясности с преподавателем, не откладывая это обсуждение до контрольной точки. Проконсультироваться с преподавателем можно во время и после практических занятий, во время консультаций, а также по электронной почте и в личном кабинете электронной образовательной среды (LMS).

Требования к рейтинг-контролю для студентов очной формы обучения.

Текущая работа студентов очной формы обучения оценивается в 60 баллов, которые распределяются между двумя модулями (периодами обучения) следующим образом:

Модуль (период обучения)	Максимальная сумма баллов в модуле	Максимальная сумма баллов за работу на практических занятиях	Реферирование, представление научной статьи, создание и отладка кода	Максимальный балл за рейтинговую контрольную работу
1	30	10	5	15
2	30	10	5	15

Правила формирования рейтинговой оценки и шкалу пересчета рейтинговых баллов в оценку на экзамене см. в «Положении о рейтинговой системе обучения в ТвГУ»:
https://tversu.ru/sveden/files/204-

R_Pologhenie_o_reytingovoy_sisteme_obucheniya_v_TvGU.pdf

VII. Материально-техническое обеспечение

Учебный процесс по данной дисциплине проводится в аудиториях, оснащенных мультимедийными средствами обучения. Для организации самостоятельной работы студентов необходимо наличие персональных компьютеров с доступом в Интернет.

Наименование специальных* помещений и помещений для самостоятельной работы	**Оснащенность специальных помещений и помещений для самостоятельной работы**	**Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа**
Помещение для самостоятельной работы, учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, практики Компьютерный класс 203а 170002, г.Тверь, Садовый пер-к, д. 35.	Набор учебной мебели, меловая доска, Переносной ноутбук, Интерактивная система Smart Board 660iv со встроенным проектором	Google Chrome-бесплатно; Kaspersky Endpoint Security 10 для Windows-Акт на передачу прав ПК545 от 16.12.2022; Lazarus –бесплатно; OpenOffice – бесплатно; Многофункциональный редактор ONLYOFFICE бесплатное ПО- бесплатно; ОС Linux Ubuntu бесплатное ПО- бесплатно
Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, *у*чебная аудитория 224, 170002, г.Тверь, Садовый пер-к, д. 35	Набор учебной мебели, меловая доска, Переносной ноутбук, Мультимедийный проектор BenQ MP 724 с потолочным креплением и экраном 1105	Google Chrome-бесплатно; Kaspersky Endpoint Security 10 для Windows-Акт на передачу прав ПК545 от 16.12.2022; Lazarus –бесплатно; OpenOffice – бесплатно; Многофункциональный редактор ONLYOFFICE бесплатное ПО- бесплатно; ОС Linux Ubuntu бесплатное ПО- бесплатно

Наличие учебно-наглядных пособий, презентаций для проведения занятий лекционного и семинарского типа, обеспечивающих тематические иллюстрации.

VIII. Сведения об обновлении рабочей программы дисциплины

№п.п.	**Обновленный раздел рабочей программы**	**Описание внесенных изменений**	**Дата и протокол заседания кафедры,**

	дисциплины (или модуля)		**утвердившего изменения**
1.	V. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	Обновление списка литературы.	Протокол № 11 от 26.06.2013
2.	VII. Методические указания для обучающихся по освоению дисциплины	Корректировка планов практических (семинарских) занятий и методических рекомендаций к ним.	Протокол № 10 от 24.06.2014
3.	V. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	Обновление списка литературы. Обновление ссылок из ЭБС.	Протокол № 1 от 27.09.2015
4.	VII. Методические указания для обучающихся по освоению дисциплины.	Корректировка планов практических (семинарских) занятий и методических рекомендаций к ним.	Протокол № 1 от 01.09.2016
5.	I - X	Корректировка всех разделов в соответствии с новым стандартом	Протокол № 6 от 28.02.2017
6.	V. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	Дополнение списков. Обновление ссылок из ЭБС.	Протокол № 1 от 01.09.2018
7.	I - VIII	Корректировка всех разделов в соответствии с новым стандартом	Протокол № 10 от 29.06.2021
8.	V. Учебно-методическое и информационное обеспечение дисциплины	Обновление списков ПО. Обновление ссылок из ЭБС.	Протокол № 1 от 1.09.2023