Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Смирнов Сергей Николаевич
Должность: врио ректора
Дата подписания: 13.10.2023 13:56:24
Уникальный программный ключ:
69e375c64f7e975d4e8830e7b4fcc2ad1bf35f08

Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «Тверской государственный университет»

Утверждаю:
Руководитель ООП:
_____ Н.А. Семыкина
«9» 06 2023 г.

Рабочая программа дисциплины (с аннотацией)

Основы построения защищенных компьютерных сетей

Специальность
10.05.01 Компьютерная безопасность

Специализация
Математические методы защиты информации

Для студентов V курса очной формы обучения

Составитель:
к.ф.-м.н., доцент _____ Н.А. Семыкина

Тверь 2023

I. Аннотация

1. Наименование дисциплины (или модуля) в соответствии с учебным планом

Основы построения защищенных компьютерных сетей

2. Цель и задачи дисциплины (или модуля)

Целью изучения дисциплины «Основы построения защищенных компьютерных сетей» является 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.

Задачи дисциплины:

– 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.

3. Место дисциплины (или модуля) в структуре ООП

Дисциплина «Основы построения защищенных компьютерных сетей» относится к числу дисциплин базовой части ООП.

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин:

«Информатика» – знание основных понятий информатики;

«Языки программирования» – знание языков программирования высокого уровня и языка ассемблера персонального компьютера, владение навыками разработки, документирования, тестирования и отладки программ;

«Основы информационной безопасности» – знание основных средств и способов обеспечения информационной безопасности, принципов построения систем защиты информации, владение профессиональной терминологией в области информационной безопасности;

«Операционные системы» – знание принципов построения современных операционных систем и особенностей их применения, владение навыками конфигурирования и администрирования операционных систем;

«Защита в операционных системах» – знание защитных механизмов и средств обеспечения безопасности операционных систем, умение формулировать и настраивать политику безопасности основных операционных систем;

«Защита программ и данных» – знание основных средств и методов анализа программных реализаций, владение навыками анализа программных реализаций.

4. Объем дисциплины (или модуля):

3 зачетные единицы, 108 академических часов, **в том числе**

контактная работа: лекции 15 часов, практические занятия 30 часов, лабораторные работы 0 часов, **самостоятельная работа:** 18 часов, **контроль**: 45 часов.

5. Перечень планируемых результатов обучения по дисциплине (или модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Планируемые результаты освоения образовательной программы (формируемые компетенции)	**Планируемые результаты обучения по дисциплине (или модулю)**
ОПК-3 – способностью понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и в иных источниках информации	**Владеть:** методиками анализа результатов работы средств обнаружения вторжений. **Уметь:** формулировать политику безопасности основных операционных систем, а также локальных компьютерных сетей, построенных на их основе. **Знать:** средства и методы хранения и передачи аутентификационной информации.
ПК-11. Способностью участвовать в проведении экспериментально-исследовательских работ при проведении	**Владеть:** навыками настройки межсетевых экранов; методиками анализа сетевого трафика. **Уметь:** применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.

сертификации средств защиты информации в компьютерных системах по требованиям безопасности информации	**Знать:** механизмы реализации атак в сетях TCP/IP; основные протоколы идентификации и аутентификации абонентов сети; защитные механизмы и средства обеспечения сетевой безопасности; средства и методы предотвращения и обнаружения вторжений.

6. Форма промежуточной аттестации - экзамен

7. Язык преподавания русский**.**

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

1. Для студентов очной формы обучения

Учебная программа – наименование разделов и тем	Всего (час.)	Контактная работа (час.)		Самостоятельная работа (час.)	Контроль
		Лекции	Практические (лабораторные) занятия		
Раздел 1. Типовые угрозы сетевой безопасности	36	5	10	6	15
Раздел 2. Крипографические методы защиты информации в компьютерных сетях	36	5	10	6	15
Раздел 3. Программно-аппаратные средства обеспечения информационной безопасности в компьютерных сетях	36	5	10	6	15
ИТОГО	108	15	30	18	45

III. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Методические рекомендации по организации самостоятельной работы студентов

Самостоятельная работа студентов по изучаемой дисциплине призвана, не только, закреплять знания, полученные во время аудиторных занятий, но и способствовать развитию у студентов творческих навыков, инициативы, умению организовывать свое время.

Все виды самостоятельной работы и планируемые на их выполнение затраты времени в часах исходят из того, что студент достаточно активно работал в аудитории, слушая лекции и решая задачи на практических занятиях. В случае пропуска лекций и практических занятий студенту потребуется сверхнормативное время на освоение пропущенного материала.

При выполнении плана самостоятельной работы студенту необходимо прочитать теоретический материал, содержащийся в указанной учебной литературе и Интернет-ресурсах. Составить словарь основных терминов и тематические конспекты, в которые необходимо включить теоретическое описание метода и привести примеры алгоритмов.

Планы практических занятий и методические рекомендации к ним

Раздел 1. Типовые угрозы сетевой безопасности

Тема №1. Сетевые атаки.

Стадии проведения сетевой атаки. Классификации сетевых угроз, уязвимостей и атак. Атаки на реализации сетевых протоколов, отдельные узлы и службы. Основные механизмы проведения сетевых атак на различных уровнях модели ISO/OSI. Проблемы обеспечения конфиденциальности, целостности и доступности информации на различных уровнях модели ISO/OSI.

Тема №2. Механизмы реализации атак в сетях TCP/IP.

Удаленное определение версии ОС с использованием особенностей реализации стека протоколов TCP/IP. Методы сканирования портов. Методы обнаружения пакетных сниферов. Методы обхода МЭ.

Тема №3. Методы перехвата сетевых соединений в сетях TCP/IP.

Имперсонация вслепую. Десинхронизация TCP-соединений. Атаки, направленные на сетевую инфраструктуру.

Тема №4. Примеры сетевых атак в сетях TCP/IP. Технические меры защиты от сетевых атак.

Принуждение к ускоренной передаче. Атаки, направленные на отказ в обслуживании. Изменение конфигурации и состояния хостов. Недостатки протоколов семейства TCP/IP с точки зрения обеспечения безопасности информации. Технические меры защиты от сетевых атак.

Раздел 2. Крипографические методы защиты информации в компьютерных сетях

Тема № 5. Криптографические протоколы обеспечения безопаности

Протоколы аутентификации на прикладном уровне. Протокол Kerberos. Протоколы аутентификации на транспортном уровне. Протокол SSL/TLS. Достоинства и недостатки аутентификации на различных уровнях модели ISO/OSI.

Тема № 6. Защита виртуальных частных сетей (VPN)

Назначение, основные возможности, принципы функционирования и варианты реализации VPN. Организация туннелирования на различных уровнях модели ISO/OSI. Достоинства и недостатки применения VPN. Протокол IPSEC. Протоколы AH и ESP. Особенности работы протокола IPSEC в туннельном и транспортном режимах. Протокол управления ключами ISAKMP/Oakley. Использование протокола L2TP для организации виртуальных частных сетей.

Тема № 7. Разработка защищенных сетевых приложений

Аутентификация, шифрование, обеспечение целостности с использованием программного интерфейса SSPI. Программный интерфейс OpenSSL.

Раздел 3. Программно-аппаратные средства обеспечения информационной безопасности в компьютерных сетях

Тема №8. Средства защиты локальных сетей при подключении к Интернет.

Межсетевые экраны (МЭ). Место и роль МЭ в обеспечении сетевой безопасности. Классификация МЭ. Требования к МЭ. Основные возможности и схемы развертывания МЭ. Достоинства и недостатки МЭ. Построение правил фильтрации. Методы сетевой трансляции адресов (NAT). Шлюзы уровня приложений. Реализация сетевой политики безопасности с использованием МЭ. Методы обхода межсетевых экранов.

Тема № 9. Защита серверов и рабочих станций. Средства и методы предотвращения и обнаружения вторжений.

Системы обнаружения вторжений (СОВ). Назначение и возможности средств обнаружения вторжений на хосты, протоколы и сетевые службы. Место и роль средств обнаружения вторжений в общей системе обеспечения сетевой безопасности. Классификация СОВ. Выявление атак на основе сигнатур атак и выявления аномалий. Аудит прикладных служб. Средства обнаружения уязвимостей сетевых служб. Способы противодействия вторжениям. Системы виртуальных ловушек (Honey Pot и Padded Cell).

IV. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Типовые контрольные задания для проверки уровня сформированности компетенции ОПК-3, ПК – 11.

Этап формирования компетенции, в котором участвует	Типовые контрольные задания для оценки знаний, умений, навыков (2-3 примера)	Показатели и критерии оценивания компетенции, шкала оценивания

дисциплина		
Базовый, **Владеть**	1. Преимущество - Проблемой безопасности может заниматься один администратор: он формирует политику безопасности и применяет ее в отношении каждого пользователя сети: A) защита; B) разделение ресурсов; C) резервное копирование данных; D) избыточность; E) аппаратное обеспечение 2. Маршрутизатор – это: A) устройства, перенаправляющие сигнал; B) устройства, отслеживающие, от какого компьютера поступает сигнал; C)устройства для соединения сетей, использующих различные протоколы и архитектуры; D) устройства, соединяющие все компьютеры рабочей группы; E) устройства, способствующие затуханию сигнала	Имеется полное верное решение, включающее правильный ответ – 3 балла В решении имеются лишние или неверные записи, не отделенные от решения – 2 балла Решение не дано или дано неверное решение – 0 баллов
Базовый, **Уметь**	1. Строит таблицу маршрутизации: A) мост; B) шлюз; C) репитер; D) маршрутизатор; E) концентратор 2 Распространяет по сети все широковещательные пакеты: A) мост; B) шлюз; C) репитер; D) маршрутизатор; E) концентратор	Имеется полное верное решение, включающее правильный ответ – 3 балла В решении имеются лишние или неверные записи, не отделенные от решения – 2 балла Решение не дано или дано неверное решение – 0 баллов
Базовый, **Знать**	1. Разрыв сетевого кабеля или отсоединение одного из его концов приводит к: A) сеть продолжает функционировать; B) функционирует только та часть, где разрыв не произошел;	Имеется полное верное решение, включающее правильный ответ – 3 балла В решении имеются лишние или неверные записи, не отделенные от

	C) прекращению функционирования сети; D) будет продолжаться доставка данных, но сеть не будет функционировать; E) когда данные будут доставлены, тогда сеть перестанет функционировать 2. Этот стандарт, иногда называемый Fast Ethernet, является расширением существующей сетевой архитектуры Ethernet и соответствует протоколу физического уровня IEEE 802.30: A) стандарт 100BaseX Ethernet; B) стандарт 10Base2; C) стандарт 10Base5; D) стандарт 10BaseT; E) стандарт 10BaseFL	решения – 2 балла Решение не дано или дано неверное решение – 0 баллов

V. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (или модуля)

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

VI. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

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

VII. Методические указания для обучающихся по освоению дисциплины

Требования к рейтинг-контролю

Модуль 1.

Максимальная сумма баллов по модулю – 50, из них 30 баллов отводится на текущий контроль учебной работы студента, 20 баллов на рубежный контроль по модулю. Текущая работа студента складывается из ответов в аудитории, min – 0 баллов, max - 2 балла. Рубежный контроль проводится в форме контрольной работы.

Модуль 2.

Максимальная сумма баллов по модулю – 50, из них 30 баллов отводится на текущий контроль учебной работы студента, 20 баллов на

рубежный контроль по модулю. Текущая работа студента складывается из ответов в аудитории и подготовке сообщений, min – 0 баллов, max – 2 балла. Рубежный контроль проводится в форме контрольной работы.

Вопросы для подготовки к зачету

1. Развертывание VPN базовыми средствами ОС Linux с использованием IPSEC.
2. Развертывание VPN базовыми средствами ОС Linux с использованием L2TP.
3. Организация туннелей с использованием ssh.
4. Настройка и использование встроенного пакетного фильтра ОС Linux iptables.
5. Настройка и использование прокси-сервера SQUID.
6. Использование и настройка средства обнаружения вторжений Snort.

VIII. Перечень педагогических и информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (или модулю), включая перечень программного обеспечения и информационных справочных систем (по необходимости)

Преподавание учебной дисциплины строится на сочетании лекций, практических занятий и различных форм самостоятельной работы студентов.

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

IX. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Учебная аудитория с мультимедийной установкой (Ноутбук, проектор, колонки), наличие классной доски. Класс ПЭВМ.

X. Сведения об обновлении рабочей программы дисциплины (или модуля)

№ п.п.	Обновленный раздел рабочей программы дисциплины (или модуля)	Описание внесенных изменений	Дата и протокол заседания кафедры, утвердившего изменения
1.			
2.			