Силабус курсу
БЕЗПЕКА КОМП'ЮТЕРНИХ МЕРЕЖ

Ступінь вищої освіти – бакалавр
Рік навчання: 3
Семестр: 6
Кількість кредитів: 5
Мова викладання: українська

Керівник курсу

ПІП	Сергій ВОЗНЯК
Контактна інформація	sv@wunu.edu.ua

Опис дисципліни

Мета вивчення дисципліни «Безпека комп'ютерних мереж» полягає у формуванні у майбутніх спеціалістів умінь та компетенцій для забезпечення безпеки комп'ютерних мереж, необхідних для подальшої роботи та навчити їх застосуванню методів та засобів захисту як окремих вузлів, так і комп'ютерної мережі в цілому, від зовнішнього та внутрішнього втручання.

Вивчення курсу „Безпека комп'ютерних мереж" передбачає наявність систематичних та ґрунтовних знань із суміжних курсів („Основи кібербезпеки", „Основи програмування", „Операційні системи", „Архітектура комп'ютерів та систем", „Комп'ютерні мережі"), а також цілеспрямованої роботи на лекційних та лабораторних заняттях, самостійної роботи студентів. В результаті вивчення курсу «Безпека комп'ютерних мереж» студенти повинні: засвоїти основні фундаментальні поняття і принципи побудови безпеки комп'ютерних мереж для їх використання в сучасних інформаційних системах; знати принципи побудови брандмауерів та фільтруючих маршрутизаторів і їх використання в задачах захисту інформаційних систем; використовувати методи для протидії від внутрішнього та зовнішнього втручання в професійній діяльності; вміти використовувати програмні засоби, які реалізують функції безпеки комп'ютерних мереж; програмно реалізовувати скрипти для конфігурування та забезпечення типових задач захисту інформації в комп'ютерних мережах; проектувати різні рівні захисту в вузлах та комп'ютених мережах.

Структура курсу

Години лек/пр	Тема	Результати навчання	Завдання
2/2	Основи безпеки Internet.	Розуміти основні понятт Internet і безпеки. Організовувати IANA, RIR, LIR, AS та захист розподілу IP-адрес. Знання кореневих DNS та правил розподілу і функціонування доменних імен. Реалізація безпеки рівнів TCP/IP, захисту на рівнях моделі відкритих систем OSI/ISO.	Поточне опитування
2/2	Стандарти та групи та класи захисту комп'ютерних мереж	Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах.	Поточне опитування

2/2	Рівні безпеки комп'ютерних мереж	Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки	Поточне опитування
2/2	Безпека операційних систем серверів та мейнфремів	Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно телекомунікаційних системах	Поточне опитування
2/2	Основи захисту серверів ОС Windows	Реалізація аутентифікації користувачів в серверах ОС Windows, доступу на основі ресурсів серверів ОС Windows. Управління доступом в операційних системах Windows на основі Active Directory. Розуміння централізованих систем аутентифікації і авторизації LDAP.	Поточне опитування
2/2	Засоби захисту UNIX-подібних систем (зокрема, Linux)	Реалізація аутентифікації в ОС сімейства Unix. Використання прав груп і користувачів до файлів. Розуміння концепції єдиного логічного входу NIS. Робота з системою LDAP та Kerberos, протоколом SSH.	Поточне опитування
2/2	Безпека фізичного рівня та кабельної інфраструктури	Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно телекомунікаційних системах	Поточне опитування
2/2	Безпека канального рівня	Вирішувати задачі захисту інформації, що обробляється в інформаційно телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації	Поточне опитування
2/2	Фільтрація і моніторинг IP-трафіку	Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно телекомунікаційних системах	Поточне опитування
2/2	Поняття трансляції IP-адрес NAT	Розуміння та навики використання технологій NAT, SAT, PAT та Masqurade, IP-адрес для внутрішнього використання intarnet. Реалізація базової трансляції IP-адрес, мережевих портів, фаєрволів з функцією NAT.	Поточне опитування

2/2	Проксі-сервери	Розумяння поняття кешуючих серверів. Проксі-сервери Лінукс. Проксі-сервери Віндовс. Наскрізний transparent-proxy. Конфігурування кешуючих серверів.	Поточне опитування
2/2	ICMP та IP–атаки мережевого рівня.	Розуміння принципів ICMP-атаки. Перенаправлення трафіку. ICMP-атака Smurf. ICMP-затоплення. Пінг смерті і ping-затоплення. Echo/chargen-затоплення. IP-атаки. Атака на IP-опції. IP-атака на фрагментацію	Поточне опитування
2/2	Атаки на протоколи граничної маршрутизації	Вирішувати задачі захисту потоків даних в інформаційних, інформаційно телекомунікаційних (автоматизованих) системах	Поточне опитування
2/2	Атаки на транспортний та сеансовий рівні TCP/ UDP	Розуміння принципів UDP-атаки. UDP-затоплення. TCP-атаки. Затоплення SYN-пакетами Підробка TCP-сегмента. Скидання TCP-з'єднання	Поточне опитування
2/2	Безпека протоколів прикладного рівня	Розуміння та організація безпеки протоколів HTTP, FTP, SMTP, POP3, IMAP4v1, SNMP, Telnet. Протокол передачі гіпертексту HTTP. Протокол передачі файлів FTP. Простий протокол передачі пошти SMTP. Протокол отримання електронної пошти POP3. Протокол доступу до повідомлень мережі Інтернет IMAP4v1. Спам. Простий протокол керування мережевими пристроями SNMP. Протокол віддаленого доступу Telnet	Поточне опитування
2/2	Сертифікати SSL та безпечні прикладні протоколи SSH і HTTPS	Знання характеристики протоколу SSL. Ієрархія ключів та сертифікатів. Цифровий підпис даних в мережі. Протокол віддаленого доступу SSH. Протокол передачі гіпертексту HTTPS	Поточне опитування
2/2	Атаки на доменні імена	Розуміння принципів атаки на DNS. DNS-спуффінг. Отруєння кеша DNS. Атаки на кореневі DNS-сервери. DDoS-атаки відображенням від DNS-серверів. Методи захисту служби DNS	Поточне опитування
2/2	Сканери мереж	Виконання сканування мережі. Сканування портів. Виявлення мережевих сервісів та їх версій. Мережева розвідка. Виявлення версії операційної системи	Поточне опитування

		пристрою чи комп'ютера. Атаки на мережеві сервіси протоколів прикладного рівня. Сканер NMAP	
2/2	Моніторинг та виявлення атак	Реалізація моніторингу трафіку. Аналізатори протоколів. Система моніторингу NetFlow та JFlow. Системи виявлення вторгнень. Система SNORTD. Архітектура мережі з захистом периметра. Мережі із поділом внутрішніх зон	Поточне опитування
2/2	Віртуальні приватні мережі VPN	Реалізація способів створення захищеного каналу. Транспортний і тунельний режими. Ієрархія технологій захищеного каналу. VPN на основі шифрування. Протокол PPTP. Розподіл функцій між протоколами IPSec. Український стандарт симетричного шифрування «Калина». Світовий стандарт симетричного шифрування AES	Поточне опитування

Рекомендовані джерела інформації

1. Курс мережевої академії Cisco: Network Security. Режим доступу https://www.netacad.com/courses/cybersecurity/network-security
2. Jason Callaway. COMPUTER NETWORKING: 2 BOOKS IN 1 – All You Need to Know to Become a Networking Engineer from Scratch (Wireless Technologies, Network System, IP subnetting, Cybersecurity, and much more) - (October 8, 2021), 181 pages.
3. Scott Jernigan, Mike Meyers. CompTIA Network+ Certification All-in-One Exam Guide, Eighth Edition (Exam N10-008) 8th Edition - (March 28, 2022), 976 pages.
4. Russell Scott. Computer Networking: This Book Includes: Computer Networking for Beginners and Beginners Guide (All in One) - (December 28, 2019), 359 pages.
5. James Bernstein. Networking Made Easy: Get Yourself Connected (Computers Made Easy) Paperback – September 2, 2018, 149 pages.
6. Ramon Nastase. Computer Networking for Beginners: Your Guide for Mastering Computer Networking, Cisco IOS and the OSI Model (Computer Networking Series) Paperback – February 1, 2018, 188 pages.
7. Craig Berg. Cisco Networking Essentials: Complete Guide To Computer Networking For Beginners And Intermediates (Code tutorials) Paperback – June 15, 2020, 85 pages.
8. Larry L. Peterson, Bruce S. Davie. Computer Networks: A Systems Approach (The Morgan Kaufmann Series in Networking) 6th Edition- (March 29, 2021), 848 pages.
9. José Manuel Ortega. Mastering Python for Networking and Security: Leverage the scripts and libraries of Python version 3.7 and beyond to overcome networking and security issues, 2nd Edition - (January 4, 2021), 538 pages.
10. Лісовська Ю. Кібербезпека. Ризики та заходи. - К.: Кондор, 2019. - 272 с.
11. Касянчук М. Досконала форма системи залишкових класів: методи побудови та застосування (Монографія) / М.Касянчук. – Тернопіль: ТНЕУ, 2019. – 224 с.

Nigel Cawthorne. Alan Turing: The Enigma Man. – Acturus, 2019. – 128 p.

Політика оцінювання

Політика щодо дедлайнів та перескладання: Для виконання індивідуальних завдань і проведення контрольних заходів встановлюються конкретні терміни. Перескладання модулів відбувається з дозволу дирекції факультету за наявності поважних причин (наприклад, лікарняний).

Політика щодо академічної доброчесності: Використання друкованих і електронних джерел інформації під час контрольних заходів заборонено.

Політика щодо відвідування: Відвідування занять є обов'язковим компонентом оцінювання. За об'єктивних причин (наприклад, карантин, воєнний стан, хвороба, закордонне стажування) навчання може відбуватись в онлайн формі за погодженням із керівником курсу.

Оцінювання

Заліковий модуль 1	Заліковий модуль 2	Заліковий модуль 3	Заліковий модуль 4
20%	20%	20%	40%
1. Усне опитування на заняттях (10 тем по 2 балів) - max 20 балів. 2. Письмова робота - max 60 бали. 3. Практичне завдання (4 практичних завдань по 5 балів)- max 20 бали.	1. Усне опитування на заняттях (10 тем по 2 балів) - max 20 балів. 2. Письмова робота - max 50 бали. 3. Практичне завдання (3 практичні завдання по 10 балів) - max 30 бали.	1. Підготовка КПІЗ - max 30 балів. 2. Захист КПІЗ -max 40 балів. 3. Оцінка за тренінг - max 30 балів	1. Теоретичні питання: 3 питання по 20 балів - max 60 балів. 2. Практичне завдання - max 40 балів

Шкала оцінювання:

ECTS	**Бали**	**Зміст**
A	90–100	відмінно
B	85–89	добре
C	75-84	добре
D	65-74	задовільно
E	60-64	достатньо
FX	35-59	незадовільно з можливістю повторного складання
F	1-34	незадовільно з обов'язковим повторним курсом