Міністерство освіти і науки України
Національний університет «Чернігівська політехніка»
Навчально-науковий інститут
електронних та інформаційних технологій
Кафедра кібербезпеки та математичного моделювання

СИЛАБУС
Технології безпеки бездротових і мобільних мереж

ЗАТВЕРДЖУЮ
Завідувачка кафедри
_____ __Ткач Ю.М.____
(підпис) (прізвище та ініціали)

« 26 » серпня 2024 р.

Розробник: Семендяй Сергій Матвійович, старший викладач кафедри кібербезпеки та математичного моделювання _____

Силабус навчальної дисципліни обговорено на засіданні кафедри кібербезпеки та математичного моделювання

Протокол від « 26 » серпня 2024 р. № 7

Узгоджено з гарантом освітньої програми: _____ __Ткач Ю.М.____

---

1. Загальна інформація про дисципліну

Тип дисципліни	*Обов'язкова*
Мова викладання	Українська
Рік навчання та семестр	Перший рік, другий семестр. 125 Кібербезпека та захист інформації ОПП Кібербезпека
Викладач (-і)	Семендяй Сергій Матвійович, старший викладач кафедри кібербезпеки та математичного моделювання
Профайл викладача (-ів)	https://mmi.stu.cn.ua/personal-kafedry/ https://scholar.google.com/citations?hl=ru&user=0T31xGYAAAAJ https://orcid.org/0000-0002-7751-5956 https://www.scopus.com/authid/detail.uri?authorId=58751294500
Контакти викладача	+380952859046, serhii_semendiai@icloud.com
Сторінка курсу в системі дистанційного навчання	https://eln.stu.cn.ua/course/view.php?id=4443

2. Анотація курсу.

Дисципліна “Технології безпеки бездротових і мобільних мереж” спрямована на вивчення сучасних загроз, методів захисту та технологій забезпечення безпеки бездротових (Wi-Fi, Bluetooth, NFC) та мобільних (3G, 4G, 5G) мереж.

У межах курсу студенти ознайомляться з архітектурою бездротових і мобільних мереж, моделями загроз, стандартами безпеки (WPA3, EAP, IPSec, TLS), методами шифрування, автентифікації та захисту даних. Значна увага приділяється практичним аспектам: налаштуванню безпечних мереж, аналізу трафіку, виявленню вразливостей, тестуванню на проникнення (Pentesting) та використанню спеціалізованих інструментів (Wireshark, Aircrack-ng, Kali Linux).

Курс орієнтований на формування у студентів компетентностей, необхідних для аналізу ризиків, розробки та впровадження заходів захисту, а також реагування на кіберзагрози в бездротових і мобільних комунікаціях.

Дисципліна є важливою складовою підготовки фахівців у галузі кібербезпеки, тестування на проникнення та управління інформаційною безпекою.

3. Мета та цілі курсу.

Метою викладання навчальної дисципліни “Технології безпеки бездротових і мобільних мереж” є формування у студентів теоретичних знань і практичних навичок щодо забезпечення безпеки бездротових (Wi-Fi, Bluetooth, NFC) та мобільних (3G, 4G, 5G) мереж, аналізу вразливостей і розробки заходів захисту.

Основними завданнями вивчення дисципліни “Технології безпеки бездротових і мобільних мереж” є:

- ознайомлення з архітектурою, протоколами та стандартами безпеки бездротових і мобільних мереж;
- аналіз основних загроз, атак та методів їхнього виявлення й усунення;
- вивчення криптографічних механізмів захисту даних у бездротових комунікаціях;
- освоєння інструментів тестування безпеки (Wireshark, Aircrack-ng, Kali Linux);
- формування навичок налаштування безпечного з’єднання та захисту інфраструктури мобільних і бездротових мереж.

4. Результати навчання

Під час вивчення дисципліни здобувач вищої освіти має набути або розширити наступні загальні (КЗ) та фахові (КФ) компетентності, передбачені освітньою програмою спеціальності 125 "Кібербезпека та захист інформації":

КЗ1. Здатність застосовувати знання у практичних ситуаціях.

КЗ2. Здатність проводити дослідження на відповідному рівні.

КЗ5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань/видів економічної діяльності).

КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

Під час вивчення дисципліни ЗВО має досягти або вдосконалити наступні програмні результати навчання, передбачені освітньою програмою:

ПРН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.

ПРН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

ПРН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об’єктах інформаційної діяльності та критичної інфраструктури.

ПРН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

У підсумку ЗВО повинні знати :

- архітектуру та принципи роботи бездротових і мобільних мереж (Wi-Fi, Bluetooth, NFC, 3G, 4G, 5G);
- моделі загроз та типові атаки на бездротові та мобільні мережі (перехоплення трафіку, підміна точок доступу, DoS-атаки, атакуючі сценарії MITM тощо);
- стандарти безпеки бездротових комунікацій (WEP, WPA, WPA2, WPA3, EAP, IPSec, TLS);
- методи автентифікації та шифрування даних у бездротових і мобільних мережах;
- принципи безпечної конфігурації точок доступу та мобільних пристроїв;
- інструменти аналізу та тестування безпеки бездротових мереж (Wireshark, Aircrack-ng, Kismet, Kali Linux);
- методи виявлення та запобігання атакам (IDS/IPS, VPN, firewall-рішення, захист мобільних додатків).

вміти :

- аналізувати архітектуру та протоколи безпеки бездротових і мобільних мереж (Wi-Fi, Bluetooth, NFC, 3G, 4G, 5G);
- виявляти вразливості у бездротових і мобільних мережах, застосовуючи методи тестування на проникнення;
- перехоплювати та аналізувати трафік за допомогою інструментів Wireshark, Aircrack-ng, Kismet;
- захищати бездротові мережі шляхом налаштування безпечного з’єднання, автентифікації та шифрування;
- конфігурувати захищені точки доступу та мобільні пристрої відповідно до сучасних стандартів безпеки;
- використовувати інструменти захисту: VPN, брандмауери, IDS/IPS-системи для запобігання атакам;
- проводити аудит безпеки бездротових і мобільних мереж та розробляти рекомендації щодо їх захисту;
- реагувати на інциденти безпеки у бездротових і мобільних мережах, застосовуючи відповідні методи захисту та відновлення.

5. Пререквізити

Для успішного опанування курсу “Технології безпеки бездротових і мобільних мереж”, студент повинен мати такі базові знання та навички:

- принципи побудови та функціонування мереж OSI та TCP/IP;
- протоколи маршрутизації та адресації (IPv4, IPv6, DHCP, DNS);
- основи роботи локальних (LAN) і глобальних (WAN) мереж;

- основи криптографії (симетричне та асиметричне шифрування, хешування);
- загальні принципи забезпечення безпеки інформаційних систем;
- основні методи атак на інформаційні системи (MITM, DoS, фішинг тощо);
- основи роботи в Linux і Windows (налаштування мереж, командний рядок);
- використання вбудованих засобів безпеки (брандмауери, VPN, журналювання подій);
- базове розуміння Python або Bash для автоматизації мережевого аналізу;
- використання скриптів для аналізу логів та тестування безпеки.

6. Обсяг курсу.

Вид заняття	Загальна кількість годин (очна/заочна форма навчання)
Лекції	12/6
Практичні заняття	12/4
Самостійна робота	66/80
Індивідуальне завдання – *розрахунково-графічна робота*	
Всього кредитів – *3*	90

Лекційні заняття – дистанційно в MS Teams.

Практичні заняття – очно в лабораторії кафедри та дистанційно в MS Teams.

Самостійна робота – з використанням системи дистанційного навчання університету, рекомендованих інформаційних джерел, презентацій, нормативно-правових актів тощо.

7. Тематика курсу

Змістовий модуль 1. Загрози для бездротових технологій та їх аналіз

Тема 1. ***Бездротові стандарти та протоколи***

Предмет дисципліни, її цілі та задачі. Структура, завдання і форми контролю, основна література. Основні положення. Термінологія бездротових мереж.

Розуміння незалежних органів стандартів, роль Wi-Fi Alliance для тестування сумісності, можливості та особливості WPA та WPA2, стандарти IETF, розуміння протоколів RADIUS та EAP. Визначення та розуміння впливу корпоративних стандартів безпеки, включаючи: 802.11z, 802.11ac, 802.11af. Отримання інформації про роботу органів стандартів та ресурсів робочої групи.

Тема 2. ***Бездротовий збір даних та WiFi MAC-аналіз***

Використання бездротового сніфінгу як механізму аналізу, розуміння режиму роботи WLAN-картки, сніфінг у керованому режимі, сніфінг в режимі монітора, переваги RFMON-сніфінгу, реалізація RFMON. Аналіз бездротового трафіку за допомогою tcpdump, Wireshark та Kismet. Вилучення даних бездротового зв’язку за допомогою Wireshark, визначення бездротових мереж за допомогою Kismet, відображення бездротових мереж за допомогою gpsmap, Google Maps, Google Earth.

Тема 3. ***Бездротові засоби інформаційного аналізу***

Побудова GPS-карт для точок бездротового доступу (airodump-ng). Загальні можливості IEEE 802.11 MAC, розуміння архітектури та експлуатації мереж ad hoc та інфраструктури, етапи автентифікації та асоціації станцій, розуміння операцій та поведінки автентифікації IEEE 802.1X. Визначення можливостей та особливостей типів EAP, включаючи PEAP, EAP/TLS, TTLS, EAP-

FAST. Пакетне оформлення в бездротових мережах, розуміння формату та полів заголовка 802.11.

Змістовий модуль 2. Атаки на комерційні бездротові протоколи

Тема 4. ***Бездротовий стандарт передачі даних ZigBee***

Введення в ZigBee, випадках використання ZigBee та розгортання. Атаки на системи ZigBee та інші бездротові промислові системи. Архітектура ZigBee і IEEE 802.15.4 фізичної та MAC-рівня. Механізми захисту ZigBee та IEEE 802.15.4; автентифікація та криптографічний контроль. Слабкі сторони у механізмах надання та керування ключовими інструментами ZigBee. Інструменти для підслуховування та керування мережами ZigBee. Використання резервування ключів ZigBee Over-the-Air (OTA). Пошук ZigBee-пристроїв за допомогою інструментів аналізу сигналу.

Тема 5. ***Технології Bluetooth***

Введення технології Bluetooth, оцінка стек протоколу Bluetooth. Аналіз пристрою Bluetooth Classic, процедура приєднання Bluetooth-піконета, компонентів фізичного рівня. Аналіз технології Bluetooth Low Energy (4.0), випадки використання, моделі та структура розгортання. Профілі Bluetooth та можливості програми, параметри безпеки Bluetooth, використання автентифікації посилань Bluetooth та шифрування. Методи аудиту та ідентифікації пристроїв Bluetooth, методи визначення місцезнаходження передавачів Bluetooth на платформах Windows і Android. Найкращі методи роботи з політикою безпеки Bluetooth та налаштування пристроїв.

Змістовий модуль 3. Забезпечення безпеки бездротових систем і мереж

Тема 6. ***Бездротові стратегії забезпечення безпеки та їх реалізація***

Введення в концепції IDS, диференціювання справжніх позитивних фактів з помилкових спрацьовувань, оцінка подій, що становлять інтерес. Моделі розгортання WIDS, включаючи оверлейні, інтегровані та гібридні розгортання. Методи виявлення атак, включаючи аналіз сигнатур, аналіз тенденцій та аналіз аномалій. Оцінювання атак за допомогою аналізу трафіку.

Тема 7. ***Засоби захисту в мобільних технологіях***

Оцінка WIDS-систем, агрегації подій, розгортання світлових ламп, захищених протоколів зв’язку, служб захисту від вторгнення, інтеграції з сторонніми системами IDS. Розгортання WIDS, включаючи охоплення об’єкта, час затримки, вірність реєстрації, зберігання подій, аналіз тенденцій. Управління політикою довіри клієнтів сертифіката. Способи розгортання нового кореневого сертифіката. Керування налаштуваннями клієнтської конфігурації бездротової інфраструктури.

8. Система оцінювання та вимоги

Загальна система оцінювання курсу	Оцінювання курсу базується на накопичувальній системі та включає: поточний контроль (оцінювання практичних занять) – 30 балів, проміжний модульний контроль – 15 балів, виконання індивідуального завдання (РГР) – 15 балів та підсумковий контроль – 40 балів. Оцінювання кожного виду діяльності здійснюється окремо відповідно до досягнення навчальних цілей.
Вимоги до РГР	Критерії оцінювання РГР: 1) виконання завдання – 10 балів; 2) якість виконання завдання – 2 бали; 4) оформлення роботи, відповідність методичним рекомендаціям – 2 бали; 5) своєчасність здачі роботи – 1 бал.

Практичні заняття	Оцінка кожного практичного заняття здійснюється за наступними критеріями: 1) виконання практичного завдання – 3 бали; 2) аналіз отриманих результатів – 1 бал; 3) належне оформлення звіту – 1 бал.
Умови допуску до підсумкового контролю	1. Виконання та захист усіх практичних робіт. 2. Проходження проміжного модульного контролю. 3. Виконання розрахунково-графічної роботи.

Розподіл балів, які отримують здобувачі вищої освіти

Модуль за тематичним планом дисципліни та форма контролю		**Кількість балів**
Змістовий модуль 1.		0…15/15
1	Оцінка виконання практичних робіт (підготовленість, самостійність, своєчасність).	0…10/10
2	Проміжний модульний контроль	0…5/5
Змістовий модуль 2.		0…15/15
1	Оцінка виконання практичних робіт (підготовленість, самостійність, своєчасність).	0…10/10
2	Проміжний модульний контроль	0…5/5
Змістовий модуль 3.		0…15/15
1	Оцінка виконання практичних робіт (підготовленість, самостійність, своєчасність).	0…10/10
2	Проміжний модульний контроль	0…5/5
Усього поточний і проміжний модульний контроль		**0…45/45**
Розрахунково-графічна робота		**0…15/15**
Семестровий контроль (диференційований залік)		**0…40/40**
Разом		**0…100/100**

Шкала оцінювання результатів навчання

Оцінка в балах	**Оцінка ECTS**	**Оцінка за національною шкалою (диференційований залік)**	
		для екзамену (диференційованого заліку), курсового проєкту (роботи), практики, атестації	для заліку
90 – 100	**A** (*відмінно*)	відмінно	зараховано
82-89	**B** (*дуже добре*)	добре	
75-81	**C** (*добре*)		
66-74	**D** (*задовільно*)	задовільно	
60-65	**E** (*достатньо*)		
0-59	**FX** (*незадовільно*)	незадовільно з можливістю повторного складання	незараховано з можливістю повторного складання

9. Обладнання та програмне забезпечення

При вивченні даного курсу використовується типове та специфічне обладнання та програмне забезпечення, а саме:

- системний блок Intel Core i3 8100/ RAM 8 GB/ SSD 120 Gb/ HDD 1 Tb з монітором LG 22MP58VQ – 12 компл.;
- мікрокомп'ютер Raspberry Pi 4 Model 4 Gb – 3 компл.;
- адаптер Wi-Fi ALFA AWUS 036AC – 2 од.;
- бездротовий маршрутизатор Mikrotik hAP ac lite tower (RB952Ui-5ac2nD);
- комутатор Cisco catalyst 2960-S;
- SDR-радіо HackRF One PortaPack H2;
- багатофункціональний пошуковий прилад ANDRE;
- багатоканальний детектор бездротових протоколів PROTECT 1207i;
- тестер радіокомунікаційний Rohde&Schwartz CMD55;
- аналізатор спектра;
- ПЗ Windows 11 Pro Ukrainian DVD, 12 ліцензій;
- ПЗ Microsoft Office Home and Student 2021 ESD, 12 ліцензій;
- ПЗ ОС Ubuntu Server 24.04.2 LTS, ліцензія GNU;
- ПЗ ОС Kali-Linux 2024.4-Kernel 6.11.0, Xfce 4.18.6, ліцензія GNU;
- ПЗ VirtualBox v. 7.1.6, ліцензія GNU.

10. Політики курсу.

До загальної політики курсу відноситься дотримання принципів відвідування занять у відповідності до затвердженого розкладу, а також вільного відвідування лекційних занять для осіб, які отримали на це дозвіл відповідно до «Порядку надання дозволу на вільне відвідування занять здобувачам вищої освіти НУ «Чернігівська політехніка»». Запорукою успішного вивчення дисципліни є активність та залучення під час проведення практичних та лекційних занять – відповіді на запитання викладача (як один з елементів поточного контролю), задавання питань для уточнення незрозумілих моментів, вирішення практичних завдань. Консультації відбуваються в аудиторіях університету у відповідності до затвердженого розкладу або ж особистих чи групових консультацій на платформі Microsoft Teams та (через вбудований форум) на сторінці курсу в системі дистанційного навчання НУ «Чернігівська політехніка».

Політика дедлайнів

Своєчасність здачі практичної роботи оцінюється в 1 бал за кожну практичну роботу. Відповідно, максимальна оцінка за невчасно здані роботи зменшується на зазначену кількість балів. Виключенням може бути наявність поважних причин несвоєчасної здачі зазначених робіт (хвороба, участь в зазначений час в інших видах навчальної, наукової чи організаційної роботи, офіційна робота за фахом тощо).

Політика користування ноутбуками / смартфонами

Прохання до здобувачів тримати смартфони переведеними у беззвучний режим протягом лекційних та практичних занять, так як дзвінки, переписки та спілкування у соціальних мережах відволікають від проведення занять як викладача, так й інших здобувачів. Ноутбуки, планшети та смартфони не можуть використовуватися в аудиторіях під час занять та під час проведення підсумкового контролю (за виключенням проходження тестового контролю в системі Moodle).

Політика заохочень та стягнень

За результатами навчальної, наукової або організаційної діяльності здобувачів вищої освіти за курсом їм можуть нараховуватися додаткові бали – до 10 балів, у залежності від вагомості досягнень. Види позанавчальної діяльності, за якими здобувачі вищої освіти заохочуються додатковою кількістю балів: участь у міжнародних проектах, наукові дослідження, тези, участь у науково-практичних конференціях, винаходи, патенти, авторські свідоцтва за напрямами курсу.

Політика академічної доброчесності

Академічна доброчесність повинна бути забезпечена під час проходження даного курсу (принципи описані у Кодексі академічної доброчесності НУ «Чернігівська політехніка»). Списування під час проміжного та підсумкового контролів, виконання практичних завдань на замовлення, підказки вважаються проявами академічної недоброчесності. Від усіх слухачів курсу очікується дотримання академічної доброчесності у зазначених вище моментах. До здобувачів вищої освіти, у яких було виявлено порушення академічної доброчесності, застосовуються різноманітні дисциплінарні заходи (включаючи повторне проходження певних етапів).

Правила перезарахування кредитів

Кредити, отримані в інших закладах вищої освіти, а також результати навчання у неформальній та/або інформальній освіті, можуть бути перезараховані викладачем у відповідності до положення «Порядок визначення академічної різниці та перезарахування навчальних дисциплін у НУ «Чернігівська політехніка»». Визнання результатів навчання у неформальній освіті розповсюджується на окремі змістові модулі (теми) навчальної дисципліни.

11. Рекомендована література та інформаційні джерела

1. Ставрінудіс, К. Безпека бездротових мереж: Захист Wi-Fi, Bluetooth, NFC і мобільних мереж / К. Ставрінудіс. – 2-ге вид. – Лондон: Packt Publishing, 2022. – 428 с.
2. Густафсон, Е. Захист мобільних мереж 5G і IoT / Е. Густафсон. – Нью-Йорк: Wiley, 2021. – 384 с.
3. Камарілло, Г. IP-захист у мобільних і бездротових мережах / Г. Камарілло, Х. Гарсія-Мартін. – Бостон: Addison-Wesley, 2020. – 352 с.
4. Перкінс, Ч. Мобільні та бездротові мережі: Технології та безпека / Ч. Перкінс. – Лондон: Pearson, 2021. – 420 с.
5. NIST 800-187: Guide to LTE Security / National Institute of Standards and Technology. – Вашингтон: NIST, 2021. – 142 с.
6. OWASP Mobile Security Testing Guide / OWASP Foundation. – 2022. – 280 с.
7. IEEE 802.11 Security Handbook / Institute of Electrical and Electronics Engineers (IEEE). – Нью-Йорк: IEEE Press, 2020. – 210 с.
8. PTK, M. Wi-Fi Security & Penetration Testing / M. PTK. – Лондон: Springer, 2022. – 368 с.
9. Фарук, А. Безпека мереж 4G та 5G: Загрози, атаки, методи захисту / А. Фарук. – Амстердам: Elsevier, 2021. – 325 с.
10. OWASP Foundation. Mobile Security Testing Guide [Електронний ресурс]. – Режим доступу: https://owasp.org/www-project-mobile-security-testing-guide/. – Дата звернення: 31.03.2024.
11. NIST. LTE Security Guide [Електронний ресурс]. – Режим доступу: https://csrc.nist.gov/publications/detail/sp/800-187/final. – Дата звернення: 31.03.2024.
12. Wi-Fi Alliance. Безпека Wi-Fi 6 та WPA3 [Електронний ресурс]. – Режим доступу: https://www.wi-fi.org/discover-wi-fi/security. – Дата звернення: 31.03.2024.
13. 5G Americas. Загрози та захист мобільних мереж 5G [Електронний ресурс]. – Режим доступу: https://www.5gamericas.org/. – Дата звернення: 31.03.2024.
14. Bluetooth SIG. Офіційна документація Bluetooth Security [Електронний ресурс]. – Режим доступу: https://www.bluetooth.com/security/. – Дата звернення: 31.03.2024.