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

РОБОЧА ПРОГРАМА
Технології безпеки бездротових і мобільних мереж

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

«__26___» ___08_ 2025 р.

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

Робочу програму навчальної дисципліни обговорено на засіданні кафедри кібербезпеки та математичного моделювання

Протокол від «__26___»___08_____202_5_р. №_6___

Узгоджено з гарантом освітньої програми: _____ Ткач Ю.М.
(підпис) (прізвище та ініціали)

---

1. Загальна інформація про дисципліну

Тип дисципліни	Обов'язкова
Мова викладання	Українська
Рік навчання та семестр	Перший рік, другий семестр. F5 Кібербезпека та захист інформації ОПП Кібербезпека
Викладач (-і)	Семендяй Сергій Матвійович, старший виладач 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 F5 – Кібербезпека та захист інформації:

КЗ1. Здатність застосовувати знання у практичних ситуаціях.

КЗ2. Здатність проводити дослідження на відповідному рівні.

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:

ПРН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв’язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

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.

ПРН12. 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.

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.

Практичні заняття (12 годин):
1. Бездротові стандарти та протоколи – 2 години.
2. Бездротовий збір даних та WiFi MAC-аналіз – 2 години.
3. Дослідження радіочастотного спектра – 4 години.
4. Хакерські радіостанції – 2 години.
5. Дослідження радіочастотного ресурсу Wi-Fi – 2 години.

Розрахунково-графічна робота (РГР)
Тема: Розрахунок дальності роботи бездротового каналу зв’язку.

Самостійна робота:
1. Бездротові стандарти та протоколи.
2. Бездротовий збір даних та WiFi MAC-аналіз.
3. Бездротові засоби інформаційного аналізу.
4. Бездротовий стандарт передачі даних ZigBee.
5. Технології Bluetooth.
6. Бездротові стратегії забезпечення безпеки та їх реалізація.
7. Засоби захисту в мобільних технологіях.

8. Система оцінювання та вимоги

З дисципліни студент може набрати до 60% підсумкової оцінки за виконання всіх видів робіт, що виконуються протягом семестру і до 40% підсумкової оцінки – на заліку.

Умовою допуску до заліку є виконання всіх видів навчальної роботи передбачених даною робочою програмою – захист усіх практичних робіт, які виконувались у поточному семестрі, оформлення звіту по практичних роботах відповідно до стандартів, виконання та захист розрахунково-графічної роботи.

Для захисту практичної роботи студент повинен відповісти на всі контрольні питання з методичних вказівок та на питання, за вибором викладача, з лекційного курсу по темі практичної роботи. За кожну практичну роботу студент отримує певну кількість балів з урахуванням максимальної кількості балів. При цьому враховується якість оформлення звіту та повнота відповідей на питання при захисті практичної роботи.

Для складання письмової компоненти модульного контролю існує перелік питань до модульного контролю. В залежності від повноти відповіді студент отримує певну кількість балів з урахуванням максимальної кількості балів. Студент, який не здає вчасно роботу, одержує оцінку нуль балів. Повторне складання студентом письмової компоненти модульного контролю не допускається.

Розрахунково-графічна робота з дисципліни виконується відповідно до методичних рекомендацій, з метою закріплення та поглиблення теоретичних знань та практичних вмінь, набутих студентом у процесі засвоєння навчального матеріалу дисципліни в області проектування бездротових ліній зв’язку. Для захисту розрахунково-графічної роботи студент повинен відповісти на декілька питань за вибором викладача по розрахункових частинах роботи. В тому випадку, коли студент відповідає на всі питання без помилок (або з несуттєвими помилками), розрахунково-графічна робота вважається захищеною. Якщо при відповіді студент допускає грубі помилки, або питання виконані менш ніж на половину, то розрахунково-графічна робота вважається незахищеною.

Складання заліку є обов’язковим елементом підсумкового контролю знань для студентів, які претендують на оцінку «добре» або «відмінно». Якщо студент виконав всі види робіт протягом семестру та набрав 60% підсумкової оцінки (тобто «задовільно»), то він, за бажанням, може залишити набрану кількість балів як підсумкову оцінку і не складати залік.

З тими ЗВО, які до проведення підсумкового семестрового контролю не встигли виконати всі обов’язкові види робіт та мають підсумкову оцінку від 0 до 19 балів (за шкалою оцінювання), проводяться додаткові індивідуальні заняття, за результатами яких визначається, наскільки глибоко засвоєний матеріал, та чи необхідне повторне вивчення дисципліни. У випадку якщо студент не має необхідних знань, він не допускається до складання заліку під час семестрового контролю, але має право ліквідувати академічну заборгованість у порядку, передбаченому «Положенням про поточне та підсумкове оцінювання знань студентів НУ «Чернігівська політехніка».

Для складання заліку існують білети. Якщо відповідь повна і зміст відповіді студента повністю відповідає сутності поставленого запитання, він може отримати від 33 до 40 балів. В тому випадку, коли студент виконує всі завдання без грубих помилок, він може отримати від 24 до 32 балів. Якщо при відповіді на питання білету студент допускає грубі помилки і всі завдання виконані менш ніж на половину, то він може отримати від 17 до 24 балів. При невиконанні хоча б одного завдання білету, студент не може отримати більше 16 балів.

Повторне складання заліку з метою підвищення позитивної оцінки не дозволяється.

Дисципліну можна вважати такою, що засвоєна, якщо студент:

– має загальне уявлення про архітектуру та принципи роботи бездротових (Wi-Fi, Bluetooth, NFC) і мобільних (3G, 4G, 5G) мереж;

– розуміє основні загрози для безпеки бездротових і мобільних мереж, але може мати труднощі з їхнім глибоким аналізом;

– ознайомлений із основними методами захисту (автентифікація, шифрування, VPN, IDS/IPS), але може потребувати додаткових пояснень щодо їхньої реалізації;

– вміє налаштувати базовий рівень безпеки Wi-Fi-мережі (WPA3, фільтрація MAC-адрес, прихований SSID);

– може використовувати базові інструменти аналізу безпеки (Wireshark, Kismet, NetStumbler) на рівні запуску та перегляду результатів;

– розуміє принципи тестування на проникнення, але може мати труднощі із самостійним проведенням тестів;

– здатен виконати типові завдання, але робота може містити неточності або потребувати додаткових пояснень викладача.

Студент із таким рівнем знань має поверхове розуміння предмета, але може орієнтуватися в основних поняттях і виконувати прості практичні завдання під керівництвом викладача. В цьому випадку студент може отримати підсумкову оцінку «задовільно» – 60 балів – Е (в т.ч. й під час ліквідації академічної заборгованості з дисципліни).

Засобами оцінювання та методами демонстрування результатів навчання з дисципліни є поточний та семестровий контроль. Поточний контроль складається з опитувань, які проводяться під час лекцій та захисту практичних робіт. Запитання для поточного контролю знаходяться у відповідних методичних рекомендаціях. Семестровий контроль проводиться у вигляді диференційованого заліку, запитання до якого на початку семестру розміщується у системі дистанційного навчання. Залікові білети знаходяться в пакеті документації на дисципліну.

Оцінювання знань ЗВО здійснюється відповідно до «Положення про поточне та підсумкове оцінювання знань здобувачів вищої освіти Національного університету «Чернігівська політехніка»», затвердженого Вченою радою Національного університету «Чернігівська політехніка» 31 серпня 2020 р. протокол № 6 та введено в дію наказом ректора від 31 серпня 2020 р. № 26.

Для визначення рівня засвоєння студентами навчального матеріалу використовуються такі методи оцінювання знань:

– поточний контроль на практичних заняттях (усне та письмове опитування, тестування, оцінка правильності та своєчасності виконання практичних робіт);

– оцінка за різні види самостійної роботи (наукові дослідження, реферати, домашні контрольні роботи, презентації);

– проміжний модульний контроль;

– підсумковий контроль (2-й семестр – диференційований залік).

Поточний контроль проводиться шляхом спілкування із студентами під час практичних занять та під час оцінювання виконання самостійної роботи. Бали, які набрані студентом під час поточного контролю, додаються до модульних оцінок.

Підсумковий контроль включає модульний та семестровий контроль. Модульний контроль проводиться у вигляді письмової відповіді на теоретичне запитання та вирішення практичної задачі.

Семестровий контроль за результатами вивчення дисципліни проводиться в останній атестаційний тиждень семестру (сесію) шляхом зваженого додавання результатів модульного контролю та постановки підсумкової оцінки до залікової відомості.

Для діагностики знань використовується модульно-рейтингова система зі 100-бальною шкалою оцінювання.

Розподіл балів, які отримують здобувачі вищої освіти

Модуль за тематичним планом дисципліни та форма контролю		**Кількість балів**
Змістовий модуль 1.		0…15
1	Оцінка виконання практичних робіт (підготовленість, самостійність, своєчасність).	0…10
2	Самостійна робота.	0…2
3	Модульний контроль.	0…3
Змістовий модуль 2.		0…15
1	Оцінка виконання практичних робіт (підготовленість, самостійність, своєчасність).	0…10

2	Самостійна робота.	0…2
3	Модульний контроль.	0…3
Змістовий модуль 3.		0…15
1	Оцінка виконання практичних робіт (підготовленість, самостійність, своєчасність).	0…10
2	Самостійна робота.	0…2
3	Модульний контроль.	0…3
Усього поточний і проміжний модульний контроль		**0…45**
Розрахунково-графічна робота		**0…15**
Семестровий контроль (диференційований залік)		**0…40**
Разом		**0…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.