	Кам’янець-Подільський національний університет імені Івана Огієнка Фізико-математичний факультет Кафедра комп’ютерних наук **СИЛАБУС** **навчальної дисципліни** **«КІБЕРБЕЗПЕКА ІОТ ТА ВБУДОВАНИХ СИСТЕМ»**

1. Загальна інформація про курс

Назва курсу, мова викладання	**КІБЕРБЕЗПЕКА ІОТ ТА ВБУДОВАНИХ СИСТЕМ** мова викладання – українська
Викладачі	Моцик Ростислав Васильович, доцент кафедри комп’ютерних наук
Профайл викладача	https://cs.kpnu.edu.ua/2019/11/04/motsyk-rostyslav-vasylovych/
E-mail:	motsyk@kpnu.edu.ua
Сторінка курсу в MOODLE	
Консультації	Розклад проведення консультацій: щочетверга з 16-00 до 17-00 в ауд. №11 корпусу №4; формат консультацій – групові та індивідуальні у вигляді співбесіди

2. Анотація до курсу

Навчальна дисципліна «кібербезпека IoT та вбудованих систем» призначена для здобувачів вищої освіти. Він охоплює специфічні загрози, які виникають у ресурсно-обмежених середовищах Інтернету речей (IoT), вбудованих систем та критичної промислової інфраструктури (IIoT/SCADA). На відміну від традиційної мережевої безпеки, дисципліна зосереджується на проблемах, пов'язаних із захистом на апаратному рівні, особливостях низькорівневого програмування та архітектурах, які не підтримують стандартні засоби захисту. Здобувачі ВО детально вивчатимуть моделі захисту, такі як

Trusted Execution Environment (TEE) та Secure Boot, а також принципи легковагової криптографії.

3. Мета і завдання курсу

Надати магістрам глибоке розуміння унікальних архітектурних, апаратних та програмних загроз, що стосуються пристроїв Інтернету речей (IoT), вбудованих систем та критичної інфраструктури (IIoT), а також навчити розробці та впровадженню комплексних стратегій захисту (Security by Design).

Завдання:

1. Опанувати архітектурні моделі захисту (TEE, Secure Boot) та моделювання загроз для ресурсно-обмежених систем.
2. Навчитися виконувати реверс-інжиніринг прошивок (Firmware) та ідентифікувати низькорівневі вразливості.
3. Вивчити методи захисту протоколів зв'язку IoT (MQTT, CoAP) та особливості легковагової криптографії.
4. Здобути практичні навички аудиту безпеки та планування реагування на інциденти у мережах IoT.

4. Результати навчання

Після завершення курсу здобувачі ВО зможуть:

- вміти використовувати інструменти реверс-інжинірингу (наприклад, Binwalk, Ghidra) для аналізу вбудованого ПЗ та ідентифікувати апаратні інтерфейси (JTAG, UART) для аудиту.
- вміти проводити оцінку вразливостей мережевих IoT-протоколів та застосовувати принципи безпеки за замовчуванням (Security by Design) у проєктах.
- вміти розробляти політику управління безпекою, використовувати стандарти (ETSI EN 303 645) та формувати стратегію реагування на інциденти у складних IoT-системах.

5. Формат курсу

Стандартний курс (очний).

6. Обсяг і ознаки курсу

Інформація з робочої програми навчальної дисципліни:

Найменування показників	**Характеристика навчального курсу**
	денна форма навчання
Освітня програма, спеціальність	Освітньо-професійна програма: *Комп'ютерні*

	науки спеціальність: F3 *Комп'ютерні науки*
Рік навчання/ рік викладання	перший, або другий
Семестр вивчення	1-ий, 2-ий, 3-ій
нормативна/вибіркова	вибіркова
Кількість кредитів ЄКТС	4
Загальний обсяг годин	120
Кількість годин навчальних занять	40
Лекційні заняття	12 год.
Практичні заняття	-
Семінарські заняття	-
Лабораторні заняття	28 год
Самостійна та індивідуальна робота	80 год.
Форма підсумкового контролю	залік

7. Пререквізити курсу

Освітні компоненти, які мають бути вивчені раніше на першому (бакалаврському) рівні вищої освіти.

8. Технічне й програмне забезпечення /обладнання

Для проведення лекцій необхідним є мультимедійне забезпечення. Для проведення лабораторних робіт – навчальна лабораторія обчислювальної техніки з доступом до мережі Інтернет.

9. Політика курсу (правила та вимоги)

Увесь навчальний контент розміщено в модульному середовищі навчання К-ПНУ імені Івана Огієнка – moodle. Підготовка до лабораторних занять, виконання завдань лабораторних робіт є обов'язковими для кожного здобувача вищої освіти.

Академічна доброчесність. Очікується, що роботи здобувачів ВО будуть їх оригінальними дослідженнями чи міркуваннями. Відсутність покликань на використані джерела, фабрикування джерел, списування, втручання в роботу інших здобувачів ВО становлять приклади можливої академічної недоброчесності. Виявлення ознак академічної недоброчесності в роботі

здобувача ВО є підставою для її незарахування викладачем, незалежно від масштабів плагіату чи обману.

Відвідання занять. Очікується, що всі студенти відвідають усі лекції та лабораторні заняття курсу. Здобувачі ВО мають інформувати викладача про неможливість відвідати заняття. Для того, щоб опрацювати питання пропущеної лекції, достатньо скласти і продемонструвати викладачу конспект. Студенти зобов'язані дотримуватися термінів виконання усіх видів робіт, передбачених курсом.

Форми поточного та підсумкового контролю. Поточний контроль реалізується на лабораторних заняттях.

Підсумковий контроль з навчальної дисципліни – залік, який виставляється за результатами поточного контролю.

10. Схема курсу

Денна форма здобуття вищої освіти

Тема 1: Архітектурна безпека та моделі загроз IoT/IIoT

1.1. Архітектура та моделі загроз IoT. Структура пристрою (MCU, шлюз, хмара). Специфічні вектори атак. OWASP IoT Top 10.

1.2. Безпека на апаратному рівні. Концепції Trusted Execution Environment (TEE) та Hardware Root of Trust.

1.3. Безпека завантажувального ланцюга. Реалізація механізму Secure Boot та підписання прошивки (Firmware Signing).

1.4. Легковагова криптографія. Вибір криптоалгоритмів для ресурсно-обмежених пристроїв. Управління життєвим циклом ключів.

Тема 2: Аналіз вразливостей вбудованих систем

2.1. Реверс-інжиніринг прошивки (Firmware). Інструменти для аналізу: Binwalk, Ghidra/IDA Pro. Емуляція прошивки за допомогою QEMU.

2.2. Низькорівневі вразливості. Вразливості переповнення буфера (Buffer Overflows) у C/C++ коді вбудованих систем.

2.3. Апаратний аудит та інтерфейси. Методи фізичного доступу. Робота з діагностичними інтерфейсами: JTAG, UART, SWD.

2.4. Методи несанкціонованого доступу (Огляд). Side-Channel Attacks (аналіз енергоспоживання), Fault Injection (загальний огляд).

Тема 3: Безпека мережевих протоколів та інтеграція з хмарою

3.1. Безпека бездротових протоколівю Аналіз вразливостей Wi-Fi, Bluetooth Low Energy (BLE), ZigBee.

3.2. Протоколи застосувального рівня IoT. Захист MQTT (TLS/SSL) та CoAP (DTLS). Аутентифікація та авторизація у мережах IoT.

3.3. Безпека промислових систем (ICS/SCADA). Архітектура Purdue. Протоколи Modbus/OPC UA. Відмінності IT/OT-безпеки.

3.4. Роль хмарних IoT-платформ. Безпека AWS IoT/Azure IoT Hub. Модель спільних обов'язків у контексті IoT-Cloud.

Тема 4: Безпечне проєктування та управління інцидентами

4.1. Security by Design та моделювання загроз. Інтеграція безпеки на ранніх етапах (SDLC). Методології Threat Modeling для IoT.

4.2. Secure Coding та стандарти. Найкращі практики безпечного кодування для вбудованих систем. Стандарт ETSI EN 303 645.

4.3. Моніторинг та логування. Централізований збір логів (Syslog). Моніторинг поведінки пристроїв для виявлення аномалій.

4.4. Реагування на інциденти та аудит. Планування IRP (Incident Response Plan) для мережі IoT. Проведення аудиту безпеки IoT-продуктів.

11. Система оцінювання та вимоги

Оцінювання здобувачів вищої освіти здійснюється відповідно до Положення про рейтингову систему оцінювання навчальних досягнень здобувачів вищої освіти. Поточний контроль передбачає оцінювання роботи (знань і вмінь) здобувачів освіти впродовж практичних занять за 12-бальною шкалою.

Таблиця 1. Розподіл балів за поточний і модульний контроль відповідно до робочої програми навчальної дисципліни

Поточний і модульний контроль (100 балів)	**Сума**
Поточний контроль	100
100 балів	

Підсумковий семестровий контроль з навчальної дисципліни передбачений у формі заліку.

Відповідно до Положення про організацію освітнього процесу в Кам'янець-Подільському національному університеті імені Івана Огієнка (від 03.07.2024 р. за № 79-ОД) здобувач вищої освіти, який не має академічної заборгованості за результатами поточного контролю з освітнього компонента, підсумковою формою контролю за яким встановлено залік, отримує підсумкову рейтингову оцінку з цього освітнього компонента відповідно до Таблиці 3:

Здобувач вищої освіти, знання, уміння і навички якого на навчальних заняттях оцінено від 1 до 3 балів, вважається таким, що недостатньо підготувався до цих занять і має академічну заборгованість за результатами поточного контролю. Поточну заборгованість, пов’язану з непідготовленістю

або недостатньою підготовленістю до навчальних занять, здобувач вищої освіти повинен ліквідувати. За відпрацьовані лекційні заняття оцінки не ставляться, за практичні та лабораторні заняття нараховуються бали середнього (4, 5, 6), достатнього (7, 8, 9) та високого рівня (10, 11, 12).

Таблиця 2. Критерії оцінювання знань, умінь, навичок здобувачів вищої освіти

Рівень навчальних досягнень	**Оцінка в балах**	**Критерії оцінювання**
Початковий	1	Студент не демонструє жодних знань з матеріалу курсу, не володіє базовою термінологією (TEE, Secure Boot, IIoT) і не здатний визначити навіть основні архітектурні компоненти чи моделі загроз для вбудованих систем, а також повністю ігнорує практичні завдання, що свідчить про повну відсутність роботи з дисципліною.
	2	Студент демонструє лише фрагментарне, поверхове знання окремих термінів, не розуміючи їхньої суті та зв'язку, допускає грубі помилки у визначенні базових концепцій кібербезпеки IoT (наприклад, плутає JTAG із UART), не здатен відтворити основні принципи роботи низькорівневих протоколів і не може застосувати отримані знання для найпростіших практичних завдань чи аудиту, що вимагає значної допомоги викладача.
	3	Студент має несистематичні знання, здатний частково відтворити лише близько 30% навчального матеріалу, відповідає на питання з помилками, невпевнено володіє термінологією та не може логічно і послідовно викласти матеріал (наприклад, описуючи принципи Secure Boot), а також не виконує або виконує з критичними помилками практичні завдання, що стосуються роботи з інструментами аналізу прошивок (Binwalk) чи налаштування захисту протоколів.
Середній	4	Студент володіє знаннями на рівні відтворення основного матеріалу, але допускає значні неточності та має труднощі з обґрунтуванням, не розуміє архітектурних відмінностей, які є ключовими для магістерського рівня (наприклад, між IIoT та SCADA), виконує лабораторні роботи лише за чіткими покроковими інструкціями та не здатний до самостійного аналізу безпеки чи моделювання загроз.
	5	Студент має загальні знання, може відповісти на більшість питань, але демонструє поверховість розуміння та нездатність до аналізу, пояснює концепції без глибокої деталізації (наприклад, знає про TEE, але не

Рівень навчальних досягнень	Оцінка в балах	Критерії оцінювання
		про його практичну реалізацію), допускає помилки в застосуванні термінології та не здатний самостійно впоратися з комплексною частиною практичних робіт (наприклад, проведенням базового реверс-інжинірингу чи впровадженням легкої криптографії), що вимагає додаткових пояснень.
	6	Студент має досить повні знання основних розділів курсу, вміє пояснити ключові поняття (TEE, Secure Boot, OWASP IoT Top 10) і виконати більшість практичних завдань на базовому рівні, але демонструє брак систематичності та логічної послідовності у відповідях, має труднощі із синтезом знань із різних розділів (наприклад, інтеграція безпеки на різних рівнях IoT-архітектури) та допускає невеликі, але суттєві помилки у теоретичних та практичних аспектах.
Достатній	7	Студент демонструє впевнене, систематичне розуміння більшості навчального матеріалу, самостійно виконує більшість практичних завдань (включаючи моделювання загроз та базовий реверс-інжиніринг прошивок), здатен аналізувати типові вразливості, але допускає несуттєві помилки у складних теоретичних питаннях (наприклад, у деталях роботи Side-Channel Attacks) та не завжди може швидко знайти оптимальне рішення у нетипових практичних ситуаціях.
	8	Студент має гарні, глибокі знання, вільно оперує термінологією, здатен аргументовано пояснювати архітектурні рішення (наприклад, вибір між MQTT та CoAP), успішно виконує всі лабораторні роботи, включаючи розробку повноцінного захисту протоколів та аудит безпеки, але його відповіді можуть бути недостатньо вичерпними або мати невеликі логічні порушення при викладі складного матеріалу, а також є потреба у додатковому стимулюванні для ґрунтовного обґрунтування прийнятих рішень.
	9	Студент демонструє повні та міцні знання, логічно та послідовно викладає матеріал, здатен якісно проводити аудит безпеки та пропонувати ефективні рішення, має глибоке розуміння специфіки кібербезпеки вбудованих систем, самостійно виконує всі завдання курсу, а його відповіді є майже вичерпними, хоча можливі незначні недоліки у деталізації або обґрунтуванні вибору певних

Рівень навчальних досягнень	Оцінка в балах	Критерії оцінювання
		інструментів (наприклад, Ghidra vs IDA Pro) чи міжнародних стандартів.
Високий	10	Студент демонструє вичерпні знання, вміло застосовує теоретичний матеріал для розв'язання практичних завдань, здатен до критичного аналізу та порівняння архітектурних рішень, успішно захищає проєкт, що демонструє комплексне застосування знань, а також самостійно знаходить додаткову інформацію, але його рішення можуть бути не завжди оптимальними або йому бракує глибини в обґрунтуванні науково-дослідних аспектів та найновіших трендів у галузі.
	11	Студент має глибокі, міцні та творчі знання, вільно оперує всіма інструментами та методологіями, здатен розробляти та обґрунтовувати нестандартні рішення для складних проблем безпеки IoT/IIoT, демонструє відмінні навички проєктування відмовостійких систем, а його проєкт є високоякісним, інноваційним та містить елементи самостійного дослідження, що відповідає високим магістерським вимогам.
	12	Студент демонструє винятковий, оригінальний та творчий підхід до розв'язання усіх завдань курсу, має повні, глибокі, системні знання, здатний до професійної оцінки та проєктування комплексних систем кіберзахисту критичної інфраструктури, вільно використовує спеціалізовані інструменти на експертному рівні, а його фінальний проєкт не лише ідеально виконаний, але й має високу наукову або практичну цінність, пропонуючи новітні рішення, що виходять за межі стандартних вимог.

Таблиця 3. Підсумковий рейтинг з кредитного модуля (дисципліни)

Рейтингова оцінка з кредитного модуля	Оцінка за шкалою ECTS	Оцінка за національною шкалою
90-100	A (відмінно)	зараховано
82-89	B (добре)	
75-81	C (добре)	
67-74	D (задовільно)	
60-66	E (достатньо)	
35-59	FX (незадовільно з можливістю повторного складання)	не зараховано

34 і менше	F (незадовільно з обов'язковим проведенням додаткової роботи щодо вивчення навчального матеріалу кредитного модуля)	

Здобувач вищої освіти, який має академічну заборгованість за результатами поточного контролю з навчальної дисципліни, підсумковою формою контролю за яким встановлено залік, отримує оцінку F за шкалою ЄКТС та «не зараховано» за національною шкалою.

Здобувач вищої освіти, який має академічну заборгованість за результатами підсумкового контролю з освітнього компонента у формі заліку, зобов'язаний ліквідувати її в терміни, визначені графіком ліквідації академічної заборгованості.

Частина кредитів може бути перезарахована за умови успішного проходження масового відкритого онлайн курсу з підтвердженням персоніфікованим сертифікатом освітньої платформи. Перелік масових відкритих онлайн курсів та обсяг кредитів для перезарахування визначає викладач. Наприклад, https://prometheus.org.ua/, https://www.coursera.org/, https://www.udemy.com та ін.

12. Рекомендована література.

Основна література

1. O'Flynn, B., Chen, S., & Shaked, E. Practical IoT Hacking: The Definitive Guide to Hacking and Securing the Internet of Things. 2020. P. 600.
2. Yau, K. The Firmware Reverse Engineering Handbook. 2020. P. 400.
3. Chowdhury, M. S. (). Security and Privacy in the Internet of Things: Architecture and Solutions. 2023. P. 350.
4. Mousa, F. Hardware Security and Trust: Design and Implementation. 2021. P. 420.
5. NIST SP 800-193. Platform Firmware Resilience (PFR) Guidelines. 2018. P. 150.

Допоміжна література

1. OWASP IoT Top 10 та OWASP Firmware Security Testing Methodology. Електронний ресурс. https://x-phy.com/blog/
2. MITRE ATT&CK for ICS (Industrial Control Systems) Framework. Електронний ресурс. https://www.aosphere.com/
3. ETSI EN 303 645. Електронний ресурс. https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf
4. Allen, L. (). Advanced Security for Industrial Control Systems. 2021. P. 380.
5. Singh, S. D. Hands-On Embedded Programming with C++. 2022. P. 450.

6. Проєкти та документація з інструментів: Ghidra, Binwalk, QEMU. Електронний ресурс. https://infosec-kpi.in.ua/assets/files/re_slides.pdf
7. Documentation on MQTT and CoAP Security (TLS/DTLS). Електронний ресурс. https://www.cloud.studio/coap-vs-mqtt/?srsltid=AfmBOoqmdyR9hFjI8eYQsTOXeuv5T0wB9J_-6GLaD03f7ZEiEe7sH3rh
8. Stallings, W. (). Cryptography and Network Security: Principles and Practice. 2020. P. 700.