Силабус курсу

БЕЗПЕКА ІНТЕРНЕТ-РЕЧЕЙ

Ступінь вищої освіти – магістр
Галузь знань – F Інформаційні технології
Спеціальність - F5 Кібербезпека та захист інформації
Освітньо-професійна програма – «Кібербезпека»
Дисципліна циклу: вибіркова
Рік навчання: 1
Семестр: 2
Кількість кредитів: 5
Мова викладання: українська

Керівник курсу

ПІП	Наталія ЯЦКІВ
Контактна інформація	n.yatskiv@wunu.edu.ua

Опис дисципліни

Метою дисципліни є сформувати у здобувачів системне розуміння загроз і механізмів захисту екосистем Інтернету речей на всіх рівнях – від архітектури та протоколів до прошивки, хмарних платформ і OT/IIoT – та навчити застосовувати перевірені практики безпеки з урахуванням реальних інцидентів і сучасних трендів (AI/5G/Edge).

Структура курсу

Години лек/пр	Тема	Результати навчання	Завдання
2/-	Вступ до IoT і основи безпеки	Здобувач розрізняє архітектури IoT (пристрій–шлюз–хмара/edge), моделі загроз і базові принципи безпеки (CIA, zero trust), пояснює життєвий цикл пристрою та визначає поверхню атаки.	Поточне опитування
2/2	Уразливості та загрози IoT	Ідентифікує типові уразливості (weak creds, hard-coded keys, відкриті порти, небезпечні OTA), класифікує загрози за STRIDE/ATT&CK і пріоритезує ризики за впливом та ймовірністю.	Поточне опитування
2/2	Основи криптографії для IoT	Пояснювати відмінності між симетричною/асиметричною криптографією, вибирає алгоритми з урахуванням ресурсних обмежень, коректно застосовує режими шифрування та MAC/AEAD.	Поточне опитування
2/2	Аутентифікація та авторизація	Порівнювати схеми аутентифікації пристрій↔служба (сертифікати,	Поточне опитування

		токени), налаштовує рольову модель доступу (RBAC/ABAC), безпечно зберігає секрети та керує ротацією ключів.	
2/2	Безпечні протоколи IoT	Обґрунтовано обирати протоколи (TLS/DTLS, MQTT(S), CoAP, HTTP(S)), конфігурує шифр-набори і перевірку сертифікатів, мінімізує метадані та запобігає downgrade-атакам.	Поточне опитування
2/2	Оновлення ПЗ та безпечне завантаження	Проектувати ланцюг довіри (secure boot, measured boot), впроваджує підписані OTA-оновлення з перевіркою цілісності/походження та планом roll-back/roll-forward.	Поточне опитування
2/-	Мережева безпека та сегментація в IoT	Виконувати мікросегментацію (VLAN/VXLAN, ACL), застосовувати принцип найменших привілеїв для трафіку, налаштовувати фільтрацію/IDS.	Поточне опитування
2/-	Захист кінцевих пристроїв і апаратна безпека IoT	Застосовувати TPM/TEE/SE для зберігання ключів, захищати від JTAG/UART-доступу та атаки на живлення/побічні канали.	Поточне опитування
4/2	Аналіз прошивки та реверс-інжиніринг IoT-пристроїв	Аналізувати прошивки, ідентифікувати компоненти (init-скрипти, busybox, бібліотеки), знаходити уразливості в конфігах/бінарях і готує PoC.	Поточне опитування
2/-	Захист даних та приватність	Класифікувати дані, впроваджує шифрування at-rest/in-transit, анонімізацію/псевдонімізацію, формувати політики мінімізації збору та вимоги до згоди/ретенції.	Поточне опитування
2/-	Хмарні та мобільні IoT-платформи	Оцінювати безпеку брокерів/шлюзів і хмарних сервісів, правильно керує ідентичностями/секретами, налаштовувати журнали/моніторинг і реагування на інциденти.	Поточне опитування
2/-	Реальні атаки та інциденти	Розбирати кейси (botnets, supply-chain, ransomware в IoT), виконувати базовий пошук багів, формувати план реагування та інциденти для підвищення стійкості.	Поточне опитування
2/2	Промисловий IoT та OT-безпека	Інтегрувати IIoT з PLC/SCADA, застосовувати сегментацію та моніторинг протоколів OT.	Поточне опитування
2/-	Дослідження та розробки в області IoT	Планувати експеримент безпеки, будувати тестові стенди, коректно вимірює метрики (латентність, споживання, криптопрофілі) і оформляти наукові результати.	Поточне опитування

2/-	Майбутнє безпеки IoT та нові виклики	Оцінювати тенденції (PQC, SBOM, AI/ML-атаки/захист), формувати дорожню карту покращень, пропонувати архітектурні рішення для підвищення кіберстійкості.	Поточне опитування

Рекомендовані джерела інформації

1. Architecture of Internet of Things (IoT). https://www.geeksforgeeks.org/computer-networks/architecture-of-internet-of-things-iot/
2. NIST SP 800-183. Networks of 'Things'.
3. https://csrc.nist.gov/pubs/sp/800/183/final#:~:text=possible%20nefarious%20intent,all%20distributed%20systems%20that%20employ
4. OWASP Internet of Things. https://owasp.org/www-project-internet-of-things/
5. NIST SP 800-213. IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements. https://csrc.nist.gov/pubs/sp/800/213/final#:~:text=Organizations%20will%20increasingly%20use%20Internet,actions%20an%20organization%20will%20expect
6. IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-213.pdf
7. MQTT Message Data Integrity - MQTT Security Fundamentals. https://www.hivemq.com/blog/mqtt-security-fundamentals-mqtt-message-data-integrity/
8. Heightened DDoS Threat Posed by Mirai and Other Botnets | CISA. https://www.cisa.gov/news-events/alerts/2016/10/14/heightened-ddos-threat-posed-mirai-and-other-botnets
9. RFC 9200: Authentication and Authorization for Constrained Environments Using the OAuth 2.0 Framework (ACE-OAuth). https://www.rfc-editor.org/rfc/rfc9200.html.
10. IoT Protocols and Standards Worth Exploring in 2024 | EMQ. https://www.emqx.com/en/blog/iot-protocols-mqtt-coap-lwm2m
11. MQTT vs CoAP: Comparing Protocols for IoT Connectivity | EMQ. https://www.emqx.com/en/blog/mqtt-vs-coap
12. OTA IoT Breakdown: What OTA Is and How It Works in IoT. https://memfault.com/blog/ota-for-iot/
13. Network Firewalls vs. Application Firewalls | Linode Docs. https://www.linode.com/docs/guides/network-firewalls-vs-application-firewalls/
14. Enabling a Fast and Secure VPN for IoT devices using WireGuard. https://www.netmaker.io/resources/vpn-for-iot-devices
15. Hardware-Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases. https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8320-draft.pdf
16. A Review of IoT Firmware Vulnerabilities and Auditing Techniques. https://www.mdpi.com/1424-8220/24/2/708
17. OWASP IoTGoat – Deliberately Insecure IoT Firmware. https://www.oneconsult.com/en/blog/iot-ot-security/owasp-iotgoat-deliberately-insecure-iot-firmware/
18. NIST Special Publication 800-57 Part 1 Revision 5. Recommendation for Key Management: Part 1 – General . https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-57pt1r5.pdf
19. The Top Internet of Things (IoT) Cybersecurity Breaches in 2025 – Asimily. https://asimily.com/blog/the-top-internet-of-things-iot-cybersecurity-breaches-in-2025/
20. The Top Internet of Things (IoT) Cybersecurity Breaches in 2025 https://asimily.com/blog/the-top-internet-of-things-iot-cybersecurity-breaches-in-2025/
21. IoT SECURITY GUIDE. https://www.dsci.in/files/content/knowledge-centre/2023/IoT-Security-Guide.pdf

22. Guide to Attribute Based Access Control (ABAC) Definition and Considerations https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf
23. GSMA 5G Security Guide v3.0 (2024). https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2024/07/FS.40-v3.0-002-19-July.pdf?utm_source=chatgpt.com
24. FIPS 203. Module-Lattice-Based Key-Encapsulation Mechanism Standard. https://csrc.nist.gov/pubs/fips/203/final?utm_source=chatgpt.com.

Політика оцінювання

Політика щодо дедлайнів і перескладання. Для виконання усіх видів завдань здобувачами і проведення контрольних заходів встановлюються конкретні терміни. Перескладання модулів проводиться в установленому порядку.

Політика щодо академічної доброчесності. Списування під час проведення контрольних заходів заборонені. Під час контрольного заходу здобувач може користуватися лише дозволеними допоміжними матеріалами або засобами, йому забороняється в будь-якій формі обмінюватися інформацією з іншими здобувачами, використовувати, розповсюджувати, збирати варіанти контрольних завдань.

Політика щодо відвідування. За об'єктивних причин (наприклад, карантин, воєнний стан, хвороба, закордонне стажування) навчання може відбуватись в дистанційній формі за погодженням із керівником курсу з дозволу дирекції факультету.

Оцінювання

Підсумковий бал (за 100-бальною шкалою) з дисципліни «Безпека Інтернет- речей» визначається як середньозважена величина, в залежності від питомої ваги кожної складової залікового кредиту:

Модуль 1		Модуль 2	Модуль 3	Модуль 4
20%	20%	5%	15%	40%
Поточне оцінювання	Модульний контроль	Тренінги	Самостійна робота	Екзамен
Визначається як середнє арифметичне з оцінок отриманих на заняттях.	Модульна робота.	Оцінка за виконання та презентацію завдання тренінгу.	Оцінка за виконане завдання самостійної роботи.	Теоретичні питання: 2 питання по 30 балів - max 60 балів. Практичне завдання - max 40 балів

Шкала оцінювання:

За шкалою ЗУНУ	**За національною шкалою**	**За шкалою ECT8**
90-100	відмінно	A (відмінно)
85-89	добре	B (дуже добре)
75-84		C (добре)
65-74	задовільно	D (задовільно)
60-64		E (достатньо)
35-59	незадовільно	FX (незадовільно з можливістю повторного складання)
1-34		F (незадовільно з обов'язковим повторним курсом)