МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ
Кафедра комп'ютерної інженерії та інноваційних технологій

«ЗАТВЕРДЖУЮ»
Ректор Міжнародного гуманітарного університету д.ю.н., професор
_____ Костянтин ГРОМОВЕНКО
« » 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

БЕЗПЕКА БЕЗДРОТОВИХ МЕРЕЖ ІНТЕРНЕТУ РЕЧЕЙ

Галузь знань	12 «Інформаційні технології»
Спеціальність	125 «Кібербезпека та захист інформації»
Назва освітньої програми	Кібербезпека
Рівень вищої освіти	перший (бакалаврський) рівень

Одеса - 2025 рік

Робоча програма затверджена на засіданні кафедри комп'ютерної інженерії та інноваційних технологій протокол № 1 від 28 серпня 2025 року.

Розробники і викладачі	**Контактний тел.**	**E-mail**
професор кафедри комп'ютерної інженерії та інноваційних технологій, д.т.н., професор **Соколов Артем Вікторович**	050-492-32-57	radiosquid@gmail.com

Завідувач кафедри комп'ютерної інженерії та інноваційних технологій
к.т.н., доцент _____ Лариса ЙОНА

Гарант освітньої програми
к.т.н., доцент _____ Лариса ЙОНА

Узгоджено
Начальник навчального відділу _____ Лілія САЄНКО

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><th rowspan="2">Найменування показників</th><th rowspan="2">Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень</th><th colspan="2">Характеристика навчальної дисципліни</th></tr>
<tr><th>денна форма навчання</th><th>заочна форма навчання</th></tr>
<tr><td rowspan="2">Кількість кредитів – 6

Загальна кількість годин – 180</td><td>Галузь - 12 «Інформаційні технології»</td><td colspan="2">обов’язкова</td></tr>
<tr><td rowspan="9">Спеціальність – 125 «Кібербезпека та захист інформації»</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td colspan="2">4-й</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td>8-й</td><td>8-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="10">Мова навчання – українська

Рівень вищої освіти – перший (бакалаврський) рівень</td><td>40 год.</td><td>8 год.</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>6 год.</td><td>2 год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>20 год.</td><td>4 год.</td></tr>
<tr><td colspan="2">Самостійна робота та індивідуальні завдання</td></tr>
<tr><td>114 год.</td><td>166 год.</td></tr>
<tr><td colspan="2">Вид контролю:</td></tr>
<tr><td>екзамен</td><td>екзамен</td></tr>
</table>

Безпека бездротових мереж Інтернету речей – це дисципліна, яка присвячена вивченню сучасних методів захисту інформації в IoT-системах на всіх рівнях, від фізичного сигналу до прикладних протоколів. Курс поєднує класичні принципи теорії сигналів і радіозв’язку з актуальними підходами кібербезпеки, забезпечуючи системне розуміння загроз, способів їх реалізації та ефективних заходів протидії. Студенти опановують основи бездротової передачі даних, методи підвищення завадостійкості, технології розширеного спектра та сучасні протоколи IoT, а також фізичні та програмні вектори атак, криптографічні методи для ресурсообмежених пристроїв, secure boot, підписання прошивок та управління ключами. Дисципліна формує компетенції з аналізу стійкості IoT-пристроїв і мереж до атак, розробки комплексних стратегій захисту та проведення аудиту безпеки відповідно до міжнародних стандартів, що дозволяє студентам отримати системне бачення безпеки IoT та підготуватися до професійної діяльності у сфері кібербезпеки, телекомунікацій та інженерії IoT-систем.

Метою дисципліни є формування у студентів системного розуміння принципів безпеки бездротових мереж Інтернету речей, включно з фізичними, протокольними та програмними аспектами, та набуття компетенцій з аналізу загроз, оцінки стійкості IoT-систем до атак і розробки ефективних заходів захисту відповідно до сучасних стандартів кібербезпеки.

ПРЕРЕКВІЗИТИ: дисципліни циклу професійної підготовки – «Основи програмування» (ОК 8), «Захист інформації в інфокомунікаційних системах та мережах» (ОК 12), «Комп'ютерні мережі» (ОК 13), «Web-технології» (ОК 14), «Безпека програм та даних» (ОК 16), «Криптографія та криптоаналіз» (ОК 23), «Програмування мікроконтролерів та пристроїв Інтернету речей» (ОК 28) знання з яких є необхідною базою для опанування освітнього компонента.

ПОСТРЕКВІЗИТИ: результати навчання за дисципліною інтегрують та узагальнюють компетентності, сформовані протягом освітньої програми, та застосовуються під час підготовки і

захисту кваліфікаційної роботи, а також у професійній діяльності за спеціальністю.

2. ОЧІКУВАНІ КОМПЕТЕНТНОСТІ, ЯКІ ПЛАНУЄТЬСЯ СФОРМУВАТИ ТА ДОСЯГНЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ

У процесі реалізації програми дисципліни «Безпека бездротових мереж Інтернету речей» формуються наступні компетентності із передбачених освітньою програмою:

Інтегральна компетентність

Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі кібербезпеки та захисту інформації.

Загальні компетентності (ЗК)

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК2. Знання та розуміння предметної області та розуміння професійної діяльності

Спеціальні (фахові) компетентності

СК 2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації

СК 4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.

СК 5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.

СК 10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

Навчальна дисципліна «Безпека бездротових мереж Інтернету речей» забезпечує досягнення програмних результатів навчання (РН), передбачених освітньою програмою:

РН 13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та/або інфраструктури організації в цілому.

РН 15. Збирати, обробляти зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводили аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.

РН 16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.

РН 17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.

РН 21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

Заплановані результати навчання за навчальною дисципліною

Знання:

1. На понятійному рівні – системно розуміти основні категорії, поняття та їх визначення у сфері безпеки бездротових мереж Інтернету речей, структуру та зміст дисципліни, а також принципи побудови та функціонування IoT-систем, включаючи фізичний, мережевий та прикладний рівні, сучасні підходи до забезпечення їх безпеки відповідно до міжнародних стандартів і рекомендацій (OWASP IoT Top 10, NIST, ETSI).

2. Описувати архітектури IoT-систем, особливості бездротових технологій (Wi-Fi, BLE, ZigBee, LoRaWAN, NB-IoT), сучасний ландшафт загроз для IoT (включаючи RF-атаки, мережеві атаки, атаки на прошивки та IoT-платформи), а також методи їх виявлення, аналізу та запобігання

з урахуванням обмежених ресурсів пристроїв.

Уміння:

3. Розуміти процеси функціонування бездротових IoT-систем та якісні зміни у сфері їх безпеки, пов’язані з розвитком інформаційних і телекомунікаційних технологій.

4. Визначати вразливості бездротових мереж і IoT-пристроїв, аналізувати безпеку протоколів передачі даних та взаємодії пристроїв із використанням сучасних підходів до оцінки захищеності.

5. Пояснювати механізми реалізації атак на різних рівнях IoT-систем (фізичному, мережевому, прикладному), включаючи джемінг, spoofing, перехоплення трафіку, атаки на протоколи та IoT-платформи, а також принципи їх запобігання.

6. Застосовувати знання:

a) на рівні відтворення – виконувати базовий аналіз безпеки IoT-систем, досліджувати характеристики бездротових каналів, інтерпретувати результати тестування та оцінювати ризики;

b) на творчому рівні – розробляти комплексні підходи до захисту IoT-систем, моделювати сценарії атак і захисту, формувати рекомендації щодо підвищення стійкості до кіберзагроз.

Навички:

7. Використовувати спеціалізовані інструменти та середовища для аналізу безпеки бездротових мереж та IoT (зокрема Wireshark, Kali Linux, інструменти аналізу Wi-Fi/BLE/ZigBee, симулятори IoT-пристроїв, середовища моделювання).

8. Аргументовано обговорювати результати аналізу безпеки IoT-систем, формувати звіти з оцінки захищеності, обґрунтовувати рекомендації щодо усунення вразливостей та підвищення рівня безпеки бездротових мереж і пристроїв Інтернету речей.

3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Тема 1. Основи бездротових систем передачі даних та IoT

У межах теми розглядаються базові принципи побудови бездротових систем передачі даних та архітектура Інтернету речей. Студенти ознайомлюються з моделями IoT (device–gateway–cloud), класифікацією пристроїв, типами сенсорних мереж та основними сценаріями їх застосування. Особлива увага приділяється ролі бездротового середовища передачі даних, характеристикам каналів зв’язку та впливу зовнішніх факторів на якість передачі інформації.

Також розглядаються базові загрози для IoT-систем, включаючи вразливості, пов’язані з відкритим середовищем передачі, обмеженими ресурсами пристроїв та відсутністю належних механізмів автентифікації. Формується системне уявлення про місце безпеки в життєвому циклі IoT-систем.

Тема 2. Теорія сигналів та методи підвищення завадостійкості

Тема присвячена основам теорії сигналів у контексті бездротового зв’язку, включаючи способи представлення та обробки сигналів, а також принципи передачі інформації у зашумлених каналах. Розглядаються методи модуляції, кодування та оптимального прийому сигналів, що забезпечують підвищення достовірності передачі даних.

Окрему увагу приділено методам підвищення завадостійкості, таким як розширення спектра (DSSS, FHSS), корекція помилок та адаптивні підходи до передачі сигналів. Аналізується їх застосування в IoT-системах з урахуванням обмежених ресурсів та специфіки бездротового середовища.

Тема 3. Протоколи IoT і бездротові технології

У рамках теми вивчаються сучасні протоколи та стандарти, що використовуються в IoT, зокрема MQTT, CoAP, а також бездротові технології Wi-Fi, BLE, ZigBee, LoRaWAN та NB-IoT. Розглядаються особливості їх функціонування, архітектурні рішення та сфери застосування.

Окремо аналізуються вразливості протоколів, проблеми автентифікації, шифрування та управління доступом. Студенти отримують уявлення про типові атаки на рівні протоколів та підходи до забезпечення безпечної передачі даних у гетерогенних IoT-мережах.

Тема 4. Фізичний рівень та RF-атаки в IoT

Тема охоплює особливості фізичного рівня бездротових систем, включаючи явища багатолучевості, затухання сигналу, вплив шуму та перешкод. Розглядаються принципи функціонування радіоканалів та їх вплив на надійність і безпеку передачі даних.

Значна увага приділяється RF-атакам, таким як джемінг, spoofing, перехоплення сигналів та атаки побічних каналів. Аналізуються механізми їх реалізації, наслідки для IoT-систем та можливі методи протидії, включаючи фізичні та програмні засоби захисту.

Тема 5. Криптографія та захист ресурсно-обмежених пристроїв

У темі розглядаються основи криптографічного захисту IoT-пристроїв з урахуванням їх обмежених обчислювальних і енергетичних ресурсів. Вивчаються легковагові криптографічні алгоритми, симетричні та асиметричні методи шифрування, зокрема використання ECC.

Також аналізуються механізми забезпечення цілісності та автентичності даних, secure boot, підписування прошивок, управління ключами та безпечне оновлення програмного забезпечення. Розглядаються практичні підходи до реалізації криптографічного захисту в IoT-системах.

Тема 6. Атаки на IoT-платформи та методи оцінки ризиків

Тема присвячена аналізу атак на рівні IoT-платформ, хмарних сервісів та інфраструктури управління пристроями. Розглядаються типові сценарії атак, включаючи ботнети (наприклад, Mirai), експлуатацію вразливостей API, компрометацію облікових даних та DDoS-атаки.

Окремо вивчаються методи оцінки ризиків, ідентифікації загроз та аналізу вразливостей. Студенти знайомляться з підходами до кількісної та якісної оцінки ризиків, що дозволяє формувати обґрунтовані рішення щодо підвищення рівня безпеки IoT-систем.

Тема 7. Аудит безпеки та стратегія захисту IoT-систем

У межах теми розглядаються методи проведення аудиту безпеки IoT-систем, включаючи тестування на проникнення, аналіз конфігурацій та оцінку відповідності стандартам. Вивчаються підходи до виявлення вразливостей та оцінювання ефективності засобів захисту.

Також розглядається формування комплексної стратегії захисту IoT-систем, що охоплює всі рівні – від фізичного до прикладного. Особлива увага приділяється рекомендаціям OWASP IoT Top 10, інтеграції технічних і організаційних заходів безпеки та підготовці звітної документації за результатами аудиту.

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин									
	денна форма					Заочна форма				
	усього	у тому числі				усього	у тому числі			
		лекц.	лаб.	практ.	сам. роб.		лекц.	лаб.	практ.	сам. роб.
Тема 1. Основи бездротових систем передачі даних та IoT	24	5	3	-	16	23	-	-	-	23
Тема 2. Теорія сигналів та методи підвищення завадостійкості	26	5	3	2	16	27	2	-	2	23
Тема 3. Протоколи IoT і бездротові технології	24	5	3	-	16	25	-	2	-	23
Тема 4. Фізичний рівень та RF-атаки в IoT	24	5	3	-	16	25	2	-	-	23
Тема 5. Криптографія та захист ресурсно-обмежених пристроїв	26	5	3	2	16	27	2	2	-	23
Тема 6. Атаки на IoT-платформи та методи оцінки ризиків	28	7	3	2	16	27	2	-	-	25
Тема 7. Аудит безпеки та стратегія захисту IoT-систем	28	8	2	-	18	26	-	-	-	26
Усього годин	**180**	**40**	**20**	**6**	**114**	***180***	***8***	***4***	***2***	***166***
ПІДСУМКОВИЙ КОНТРОЛЬ - ЕКЗАМЕН										

5. ПИТАННЯ ДО ПРАКТИЧНИХ ЗАНЯТЬ

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	**Тема 1. Основи бездротових систем передачі даних та IoT** 1. Архітектура IoT-систем: рівні device–gateway–cloud 2. Класифікація IoT-пристроїв та сенсорних мереж 3. Основні характеристики бездротових каналів передачі даних 4. Типи бездротових технологій та їх застосування в IoT 5. Базові загрози та вразливості бездротових IoT-систем	1	-
2	**Тема 2. Теорія сигналів та методи підвищення завадостійкості** 1. Основи цифрових сигналів та способи їх представлення 2. Методи модуляції у бездротових системах зв'язку 3. Принципи оптимального прийому сигналів у зашумленому каналі 4. Методи розширення спектра (DSSS, FHSS) 5. Кодування та корекція помилок у системах передачі даних	1	-
3	**Тема 3. Протоколи IoT і бездротові технології** 1. Протоколи прикладного рівня IoT (MQTT, CoAP) 2. Особливості технологій BLE, ZigBee та Wi-Fi 3. Технології далекого радіусу дії (LoRaWAN, NB-IoT) 4. Механізми автентифікації та шифрування в IoT-протоколах 5. Вразливості та загрози на рівні протоколів IoT	1	1
4	**Тема 4. Фізичний рівень та RF-атаки в IoT** 1. Особливості фізичного рівня бездротових систем 2. Вплив шуму, затухання та багатолучевості на сигнал 3. Атаки типу джемінг (jamming) та їх реалізація 4. Spoofing та перехоплення бездротового трафіку 5. Методи виявлення та протидії RF-атакам	1	-
5	**Тема 5. Криптографія та захист ресурсно-обмежених пристроїв** 1. Особливості криптографії для IoT-пристроїв 2. Симетричні та асиметричні алгоритми в IoT 3. Використання ECC у ресурсно-обмежених системах 4. Secure boot та підписування прошивок 5. Управління ключами та автентифікація пристроїв	1	-
6	**Тема 6. Атаки на IoT-платформи та методи оцінки ризиків** 1. Архітектура IoT-платформ та потенційні вектори атак 2. Ботнети в IoT (зокрема Mirai) 3. Вразливості API та хмарних сервісів IoT 4. Методи аналізу загроз та вразливостей 5. Підходи до оцінки ризиків у IoT-системах	1	1
7	**Тема 7. Аудит безпеки та стратегія захисту IoT-систем** 1. Основні етапи аудиту безпеки IoT-систем 2. Методи тестування на проникнення IoT 3. Аналіз відповідності стандартам (OWASP IoT Top 10) 4. Формування комплексної стратегії захисту 5. Підготовка звітів за результатами аудиту безпеки	-	-
	Всього	**6**	**2**

5. ЛАБОРАТОРНІ РОБОТИ

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	**Аналіз архітектури IoT-системи** Мета: вивчити структуру IoT-систем (device–gateway–cloud), дослідити взаємодію компонентів та визначити потенційні вразливості на різних рівнях архітектури.	2	-
2	**Дослідження характеристик бездротового каналу передачі даних** Мета: дослідити вплив шумів, затухання та перешкод на якість передачі сигналу, оцінити основні параметри бездротового каналу та їх вплив на надійність передачі даних.	2	-
3	**Аналіз та моделювання методів підвищення завадостійкості** Мета: вивчити принципи роботи методів розширення спектра (DSSS, FHSS) та корекції помилок, дослідити їх ефективність у зашумлених каналах передачі.	2	2
4	**Дослідження протоколів MQTT та CoAP** Мета: ознайомитися з принципами роботи протоколів IoT, проаналізувати обмін повідомленнями, дослідити особливості їх використання та базові аспекти безпеки.	2	-
5	**Аналіз безпеки бездротових технологій (Wi-Fi, BLE, ZigBee)** Мета: дослідити механізми передачі даних у різних бездротових технологіях, виявити потенційні вразливості та оцінити рівень їх захищеності.	2	-
6	**Перехоплення та аналіз бездротового трафіку** Мета: навчитися здійснювати аналіз мережевого трафіку, дослідити структуру переданих даних, виявляти аномалії та потенційні загрози безпеці.	2	2
7	**Дослідження RF-атак (джемінг та spoofing)** Мета: ознайомитися з принципами реалізації атак на фізичному рівні, дослідити їх вплив на роботу бездротових систем та оцінити можливі методи протидії.	2	-
8	**Реалізація криптографічного захисту в IoT** Мета: вивчити принципи застосування криптографічних алгоритмів у IoT, реалізувати базові механізми шифрування, автентифікації та забезпечення цілісності даних.	2	-
9	**Аналіз вразливостей IoT-платформи** Мета: дослідити типові вразливості IoT-платформ і сервісів, виконати базовий аналіз безпеки та визначити потенційні ризики.	2	-
10	**Проведення аудиту безпеки IoT-системи** Мета: сформувати навички комплексного аналізу безпеки IoT-системи, оцінити рівень захищеності, розробити рекомендації щодо усунення вразливостей та підвищення кіберстійкості.	2	-
	Всього	**20**	**4**

6. САМОСТІЙНА РОБОТА

До самостійної роботи студентів щодо вивчення дисципліни «Безпека бездротових мереж Інтернету речей» включаються:

1. Знайомство з науковою та навчальною літературою відповідно зазначених у програмі тем.
2. Опрацювання лекційного матеріалу.
3. Підготовка до практичних занять.
4. Консультації з викладачем протягом семестру.
5. Самостійне опрацювання окремих питань навчальної дисципліни.
6. Підготовка та виконання індивідуальних завдань.
7. Підготовка до підсумкового контролю.

Тематика та питання до самостійної підготовки та індивідуальних завдань

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	**Тема 1. Основи бездротових систем передачі даних та IoT** Вступ до IoT, архітектури мереж, типи бездротових технологій, моделі загроз, базові принципи передачі та прийому сигналів, завадостійкість і роль фізичного рівня у безпеці.	16	23
2	**Тема 2. Теорія сигналів та методи підвищення завадостійкості** Двійкові та багаторівневі системи зв'язку, алгоритми оптимального прийому сигналів, Spread Spectrum, DSSS та FHSS, критерії ефективності та застосування в IoT.	16	23
3	**Тема 3. Протоколи IoT і бездротові технології** MQTT, CoAP, BLE, ZigBee, LoRaWAN, NB-IoT, аналіз вразливостей протоколів, безпека мережевого рівня, криптографічні аспекти передачі даних.	16	23
4	**Тема 4. Фізичний рівень та RF-атаки в IoT** Механізми багатопроменевості, вплив шумоподібних сигналів, джемінг, spoofing, перехоплення бездротового трафіку, Side-channel та інші атаки на фізичному рівні.	16	23
5	**Тема 5. Криптографія та захист ресурсно-обмежених пристроїв** Легковагові криптографічні алгоритми, ECC, симетричні та асиметричні методи, secure boot, підписування прошивок, управління ключами та аутентифікація.	16	23
6	**Тема 6. Атаки на IoT-платформи та методи оцінки ризиків** Botnet-атаки типу Mirai, уразливості хмарних IoT-сервісів, експлуатація API, аналіз стійкості систем до DDoS та інші практичні сценарії атак.	16	25
7	**Тема 7. Аудит безпеки та стратегія захисту IoT-систем** Методики тестування безпеки, інтеграція фізичного та програмного захисту, оцінка ризиків, рекомендації OWASP IoT Top 10, формування комплексної стратегії захисту та звіту про аудит.	18	26
	Всього	**114**	**166**

7. ВИДИ ТА МЕТОДИ КОНТРОЛЮ

Види контролю	Складові оцінювання
поточний контроль, який здійснюється у ході: проведення практичних (лабораторних) занять, виконання самостійної роботи, індивідуальних завдань, дослідна робота здобувача тощо.	**50%**
підсумковий контроль	**50%**

Методи діагностики знань (контролю)	**фронтальне опитування; наукова доповідь, реферати, усне повідомлення, індивідуальне опитування; робота у групах; ділова гра, розв`язання ситуаційних завдань, кейсів, практичних завдань, екзамен**

Питання до екзамену

1. Поясніть архітектуру IoT-системи (device–gateway–cloud) та функції кожного рівня.
2. Охарактеризуйте типи IoT-пристроїв і їх роль у побудові кіберфізичних систем.
3. Проаналізуйте основні моделі взаємодії в IoT (device-to-device, device-to-cloud тощо).
4. Поясніть особливості бездротового середовища передачі даних та його вплив на безпеку.
5. Охарактеризуйте основні параметри бездротового каналу (SNR, BER, пропускна здатність).
6. Проаналізуйте вплив обмежених ресурсів IoT-пристроїв на забезпечення безпеки.
7. Розкрийте поняття життєвого циклу IoT-пристрою та пов’язані з ним ризики.
8. Охарактеризуйте основні класи загроз у IoT-системах.
9. Поясніть роль фізичного рівня у забезпеченні безпеки IoT.
10. Поясніть основні типи сигналів у цифрових системах зв’язку.
11. Розкрийте принципи модуляції сигналів у бездротових системах.
12. Охарактеризуйте поняття шуму та його вплив на передачу інформації.
13. Поясніть критерії оптимального прийому сигналів.
14. Проаналізуйте співвідношення сигнал/шум (SNR) та його значення для якості зв’язку.
15. Розкрийте принципи роботи DSSS та FHSS.
16. Порівняйте методи розширення спектра за ефективністю та стійкістю.
17. Поясніть методи виявлення та корекції помилок.
18. Охарактеризуйте компроміс між завадостійкістю та пропускною здатністю.
19. Поясніть принципи роботи MQTT та його модель publish/subscribe.
20. Порівняйте MQTT та CoAP за архітектурою і сферою застосування.
21. Охарактеризуйте стек протоколів IoT та його особливості.
22. Поясніть принципи роботи BLE та його обмеження.
23. Охарактеризуйте ZigBee та його роль у сенсорних мережах.
24. Проаналізуйте особливості LoRaWAN і NB-IoT.
25. Розкрийте механізми безпеки в IoT-протоколах.
26. Охарактеризуйте типові вразливості протоколів IoT.
27. Поясніть проблеми автентифікації та управління доступом у IoT.
28. Поясніть явище багатопроменевості та його вплив на передачу сигналу.
29. Охарактеризуйте процес затухання сигналу в бездротових каналах.
30. Поясніть принципи виникнення шумів у радіоканалах.
31. Розкрийте механізм реалізації джемінгу (jamming).
32. Охарактеризуйте види джемінг-атак та їх вплив.
33. Поясніть принципи spoofing-атак у бездротових мережах.
34. Проаналізуйте методи перехоплення бездротового трафіку.
35. Розкрийте поняття side-channel атак на фізичному рівні.
36. Охарактеризуйте методи виявлення та протидії RF-атакам.
37. Поясніть особливості криптографії в IoT-системах.
38. Порівняйте симетричні та асиметричні методи шифрування.

39. Охарактеризуйте принципи роботи ECC.
40. Поясніть переваги ECC для IoT-пристроїв.
41. Розкрийте поняття автентичності, цілісності та конфіденційності даних.
42. Поясніть механізм secure boot.
43. Охарактеризуйте процес підписування прошивок.
44. Розкрийте підходи до управління криптографічними ключами.
45. Проаналізуйте проблеми безпечного оновлення IoT-пристроїв.
46. Охарактеризуйте архітектуру IoT-платформ та їх вразливості.
47. Поясніть принципи функціонування ботнетів (на прикладі Mirai).
48. Проаналізуйте DDoS-атаки в IoT-середовищі.
49. Розкрийте вразливості API IoT-систем.
50. Поясніть поняття загрози, вразливості та ризику.
51. Охарактеризуйте основні підходи до оцінки ризиків.
52. Поясніть методи ідентифікації загроз.
53. Проаналізуйте підходи до кількісної та якісної оцінки ризиків.
54. Розкрийте роль моніторингу та реагування на інциденти в IoT.
55. Охарактеризуйте етапи аудиту безпеки IoT-систем.
56. Поясніть методи тестування на проникнення для IoT.
57. Розкрийте підхід OWASP IoT Top 10.
58. Охарактеризуйте принципи побудови комплексної стратегії захисту.
59. Поясніть інтеграцію фізичного та програмного рівнів безпеки.
60. Охарактеризуйте структуру звіту за результатами аудиту безпеки.

8. ОЦІНЮВАННЯ ЗДОБУВАЧІВ ВИЩОЇ ТА ФАХОВОЇ ПЕРДВИЩОЇ ОСВІТИ ЗА НАВЧАЛЬНУ ДИСЦИПЛІНУ У МІЖНАРОДНОМУ ГУМАНІТАРНОМУ УНІВЕРСИТЕТІ

(*поточний контроль, підсумковий контроль, загальний результат оцінювання)*

ЕКЗАМЕН

Поточний контроль			
Види роботи	**Планові терміни виконання**	**Форми контролю та звітності**	**Максимальний відсоток оцінювання**
Систематичність і активність роботи на практичних (лабораторних) заняттях			
1.1. Підготовка до практичних, лабораторних занять	Відповідно до робочої програми та розкладу занять	Перевірка обсягу та якості засвоєного матеріалу під час практичних (лабораторних) занять	**30**
Виконання завдань для самостійного опрацювання			
1.2. Індивідуальне тестування, завдання за заданою тематикою	Відповідно до робочої програми та розкладу занять	Розгляд відповідного матеріалу під час аудиторних занять або ІКР[1], перевірка конспектів навчальних текстів тощо	**10**
Виконання індивідуальних завдань, дослідна робота здобувача			
1.3. Інші види індивідуальних завдань, в т.ч.підготовка наукових публікацій, участь у роботі круглих столів, конференцій тощо.	Відповідно до робочої програми та розкладу занять	Обговорення результатів проведеної роботи під час аудиторних занять, наукових конференцій та круглих столів.	**10**
Разом балів за поточний контроль			**50**
Підсумковий контроль екзамен			**50**
Загальний результат оцінювання			**100**

Поточний контроль знань здобувачів освіти при формі контролю **екзамен** (максимум 50 балів) оцінюється за шкалою *(«2», «3», «4», «5»)*, з обов'язковим переведенням балів за кожний вид роботи таким чином:

- за підготовку до аудиторних занять (максимум 30 балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості практичних (лабораторних) занять, для переводу балів за підготовку до аудиторних занять середньоарифметична оцінка множиться на коефіцієнт 6;
- за виконання завдань для самостійного опрацювання (тестування, завдання, підготовка реферату (есе) за заданою тематикою) (максимум 10 балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості програмного матеріалу, що виноситься на самостійне вивчення, для переводу зазначених балів середньоарифметична оцінка множиться на коефіцієнт 2;
- за інші види індивідуальних завдань, в т.ч. підготовку наукових публікацій, участь у роботі круглих столів, конференцій тощо (максимум 10- балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості інших видів індивідуальних завдань, для переводу

[1] Індивідуально-консультативна робота викладача зі здобувачами

балів за підготовку до аудиторних занять середньоарифметична оцінка множиться на коефіцієнт 2.

КРИТЕРІЇ ОЦІНЮВАННЯ ЗА ПОТОЧНИЙ КОНТРОЛЬ

- «2»- виставляється за неправильну відповідь (письмову роботу), яка не відповідає змісту теми та свідчить про нерозуміння її основних положень;
- «3» -виставляється за відповідь (письмову роботу), яка відповідає змісту теми, але є неповною і неточною у визначенні понять, свідчить про неповне розуміння основних положень навчального матеріалу, свідчить про те, що знання студента мають фрагментарний, поверховий характер;
- «4» - оцінюється правильна і обґрунтована відповідь (письмова робота), з якої видно, що студент знає й розуміє теоретичний матеріал в обсязі навчальної теми, володіє необхідними навичками, не допускає суттєвих помилок.
- «5» - оцінюється повна, правильна, ґрунтовна відповідь (письмова робота) на запитання теми, що передбачає логічність і послідовність викладу матеріалу, володіння термінологією, показує вміння повно й глибоко використовувати теоретичні знання в практичній площині.

КРИТЕРІЇ ОЦІНЮВАННЯ ПІДСУМКОВОГО КОНТРОЛЮ ЗНАНЬ ЗДОБУВАЧІВ ЗА ЕКЗАМЕН
(максимум 50 балів)

Рівень знань оцінюється:

- від 40 до 50 балів - студент виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, демонструє знання матеріалу, проводить узагальнення і висновки;
- 30 до 40 балів - студент володіє знаннями матеріалу, але допускає незначні помилки у формуванні термінів, категорій, проте за допомогою викладача швидко орієнтується і знаходить правильні відповіді;
- 20 - 30 балів - студент відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень, з допомогою викладача може аналізувати навчальний матеріал, але дає недостатньо обґрунтовані, невичерпні відповіді, допускає помилки.
- 10 - 20 балів - володіє навчальним матеріалом на середньому рівні, допускає помилки, серед яких є значна кількість суттєвих;
- 0 10 балів - володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні, на всі запитання дає необґрунтовані, невичерпні відповіді, допускає помилки.

Поточний контроль знань здобувачів освіти оцінюється за шкалою *(«2», «3», «4», «5»)*, з обов'язковим переведенням балів за кожний вид роботи таким чином:

- за підготовку до аудиторних занять (максимум 60 балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості практичних (лабораторних) занять, для переводу балів за підготовку до аудиторних занять середньоарифметична оцінка множиться на коефіцієнт 12;
- за виконання завдань для самостійного опрацювання (тестування, завдання, підготовка реферату (есе) за заданою тематикою) (максимум 20 балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості програмного матеріалу, що виноситься на самостійне вивчення, для переводу зазначених балів середньоарифметична оцінка множиться на коефіцієнт 4;
- за інші види індивідуальних завдань, в т.ч. підготовку наукових публікацій, участь у роботі круглих столів, конференцій тощо (максимум 20- балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості інших видів індивідуальних завдань, для переводу балів за підготовку до аудиторних занять середньоарифметична оцінка множиться на коефіцієнт 4.

9. КРИТЕРІЇ ЗАГАЛЬНИХ РЕЗУЛЬТАТІВ ОЦІНЮВАННЯ ЗНАНЬ ЗДОБУВАЧІВ

Рівень знань оцінюється:

- «відмінно» / «зараховано» A - від 90 до 100 балів. Студент виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, демонструє знання матеріалу, проводить узагальнення і висновки. Був присутній на лекціях та семінарських заняттях, під час яких давав вичерпні, обґрунтовані, теоретично і практично правильні відповіді, має конспект з виконаними завданнями до самостійної роботи, презентував реферат (есе) за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;
- «добре» / «зараховано» B - від 82 до 89 балів. Студент володіє знаннями матеріалу, але допускає незначні помилки у формуванні термінів, категорій, проте за допомогою викладача швидко орієнтується і знаходить правильні відповіді. Був присутній на лекціях та семінарських заняттях, має конспект з виконаними завданнями до самостійної роботи, презентував реферат (есе) за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;
- «добре» / «зараховано» C - від 74 до 81 балів. Студент відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень, з допомогою викладача може аналізувати навчальний матеріал, але дає недостатньо обґрунтовані, невичерпні відповіді, допускає помилки. При цьому враховується наявність конспекту з виконаними завданнями до самостійної роботи, реферату та активність у науково-дослідній роботі;
- «задовільно» / «зараховано» D - від 64 до 73 балів. Студент був присутній не на всіх лекціях та семінарських заняттях, володіє навчальним матеріалом на середньому рівні, допускає помилки, серед яких є значна кількість суттєвих. При цьому враховується наявність конспекту з виконаними завданнями до самостійної роботи, рефератів (есе);
- «задовільно» / «зараховано» E - від 60 до 63 балів. Студент був присутній не на всіх лекціях та семінарських заняттях, володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні, на всі запитання дає необґрунтовані, невичерпні відповіді, допускає помилки, має неповний конспект з завданнями до самостійної роботи.
- «незадовільно з можливістю повторного складання» / «не зараховано» FX – від 35 до 59 балів. Студент володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу.
- «незадовільно з обов'язковим повторним вивченням дисципліни» / «не зараховано» F – від 0 до 34 балів. Студент не володіє навчальним матеріалом.

ТАБЛИЦЯ ВІДПОВІДНОСТІ ЗАГАЛЬНИХ РЕЗУЛЬТАТІВ ОЦІНЮВАННЯ ЗНАНЬ ЗА РІЗНИМИ ШКАЛАМИ

100-бальною шкалою	Шкала за ECTS	За національною шкалою	
		екзамен	залік
90-100	A	Відмінно	Зараховано
82-89	B	Добре	
74-81	C		
64-73	D	Задовільно	
60-63	E		
35-59	Fx	Незадовільно	Не зараховано
1-34	F		

10. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Stravos Z. IoT Network Security: Penetration Testing and Exploitation Techniques (IoT Red Teaming: Offensive and Defensive Strategies Book 4). Independently published, 2025. 231 p.
2. Syed A. Supply Chain Software Security: AI, IoT, and Application Security. Apress, 2024. 592 p.
3. Shewring N. IoT Security (IoT Smart Bites). Independently published, 2024. 48 p.
4. Qureshi B. IoT Hacking: The Complete Guide to IoT Hacking and Security. Independently published, 2025. 301 p.
5. Reynold G. IOT SECURITY ENGINEERING: Complete Guide | Build 50 Security Systems. Independently published, 2025. 173 p.

Допоміжна

6. Maleki A., Nguyen H. H., Barton R. Outage probability analysis of LR-FHSS in satellite IoT networks. IEEE Communications Letters. 2022. Vol. 27, No. 3. P. 946-950.
7. Schiller E. et al. Landscape of IoT security. Computer Science Review. 2022. Vol. 44. P. 100467.
8. Alwahedi F. et al. Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models. Internet of Things and Cyber-Physical Systems. 2024. Vol. 4. P. 167-185.
9. Mazhar T. et al. Analysis of IoT security challenges and its solutions using artificial intelligence. Brain sciences. 2023. Vol. 13, No. 4. P. 683.
10. Kaur B. et al. Internet of Things (IoT) security dataset evolution: Challenges and future directions. Internet of Things. 2023. Vol. 22. P. 100780.

Інформаційні ресурси

11. Національна бібліотека України ім. В.І. Вернадського : веб-сайт. URL: http://www.nbuv.gov.ua.
12. Он-лайн бібліотека. URL: http://www.lib.com.ua
13. http://www.info-library.com.ua/books-book-149.html
14. https://owasp.org – OWASP
15. https://portswigger.net – Portswigger