Міжнародний гуманітарний університет
Факультет кібербезпеки, програмної інженерії та комп'ютерних наук
Кафедра комп'ютерної інженерії та інноваційних технологій

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
Безпека бездротових мереж Інтернету речей (IoT)

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

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

1. АНОТАЦІЯ ДО КУРСУ

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. Передумовами є знання, уміння та навички, отримані при вивченні «Комп'ютерних мереж» (ОК 13), «Захисту інформації в інфокомунікаційних системах та мережах» (ОК 12), «Програмування мікроконтролерів та пристроїв Інтернету речей» (ОК 28), «Систем технічного захисту інформації» (ОК 31) та «Комплексних систем захисту інформації» (ОК 24).

ПОСТРЕКВІЗИТИ. Знання та навички із забезпечення безпеки бездротових мереж та IoT-пристроїв є корисними при паралельному вивченні «Етичного хакінгу та тестування на проникнення» (ОК 18), а також при проходженні переддипломної практики (ОК 35) і підготовці та захисті кваліфікаційної роботи (ОК 36).

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

У процесі реалізації програми дисципліни «Безпека бездротових мереж Інтернету речей (IoT)» 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.

3. ОБСЯГ ТА ОЗНАКИ КУРСУ

Загалом		**Вид заняття** (денне відділення / заочне відділення)				**Ознаки курсу**		
ЄКТС	**годин**	**Лекційні заняття**	**Лабораторні заняття**	**Практичні заняття**	**Самостійна робота**	**Курс, (рік навчання)**	**Семестр**	**Обов'язкова / вибіркова**
6	180	40/8	20/4	6/2	114/166	4	8	Обов'язкова

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. ТЕХНІЧНЕ Й ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ / ОБЛАДНАННЯ

Студенти отримують теми та питання курсу, методичні рекомендації, перелік основної й додаткової літератури, індивідуальні та практичні завдання, а також результати оцінювання як традиційним шляхом, так і з використанням університетської платформи дистанційного навчання

на базі Moodle. Для формування практичних компетентностей з безпеки IoT та бездротових мереж використовується спеціалізоване лабораторне середовище, розгорнуте у віртуалізованій інфраструктурі. Практичні заняття проводяться із застосуванням операційних систем для тестування безпеки (наприклад, Kali Linux), інструментів сканування та аналізу вразливостей IoT-пристроїв, експлуатації бездротових протоколів (Wi-Fi, BLE, ZigBee, LoRaWAN), а також навчальних середовищ і симуляторів IoT-пристроїв для відпрацювання атак та заходів захисту на різних рівнях складності.

6. САМОСТІЙНА РОБОТА

До самостійної роботи студентів щодо вивчення дисципліни «Безпека бездротових мереж Інтернету речей (IoT)» 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 в рамках лабораторних робіт.
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, помехоустойчивість 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 багатолучевості, 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**	
	Для екзамену	**Для заліку**
поточний контроль, який здійснюється у ході: проведення практичних та лабораторних занять, виконання самостійної роботи, індивідуальних завдань, дослідна робота здобувача тощо.	**50%**	**100%**
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

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, підготовка реферату (есе) 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 балів за пдготовку 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;

[1] Індивідуально-консультативна робота викладача зі здобувачами

- «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 ІСПИТ
(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 при формі контролю **залік** (максимум 100 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 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
(для екзамену / заліку)

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. ДОТРИМАННЯ ВИМОГ АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ

Викладання та засвоєння навчальної дисципліни передбачає неухильне дотримання вимог академічної доброчесності, яка регулюється Законом України "Про освіту" (Відомості Верховної Ради (ВВР), 2014, № 37-38, ст.2004), «Методичними рекомендаціями для закладів вищої освіти з підтримки принципів академічної доброчесності» (Лист МОН № 1/9-650 від 23.10.18 року), іншими нормативними документами. Зокрема, основні засади дотримання академічної доброчесності визначено у «Положенні про академічну доброчесність у Міжнародному гуманітарному університеті», «Кодексі академічної доброчесності Міжнародного гуманітарного університету» та «Інструкції щодо процедури технічної перевірки на наявність текстових запозичень (академічного плагіату)», затвердженої наказом МГУ від 03.05.2024 р., № 708а.

Відповідно до ст.42 Закону України "Про освіту" академічна доброчесність - це сукупність етичних принципів та визначених законом правил, якими мають керуватися учасники освітнього процесу під час навчання, викладання та провадження наукової (творчої) діяльності з метою забезпечення довіри до результатів навчання та/або наукових (творчих) досягнень.

Дотримання академічної доброчесності передбачає:

- самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання (для осіб з особливими освітніми потребами ця вимога застосовується з урахуванням їхніх індивідуальних потреб і можливостей);
- посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей;
- дотримання норм законодавства про авторське право і суміжні права;
- надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації.

11. 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