ЗАТВЕРДЖЕНО

Вченою радою
факультету інформаційно-
комп'ютерних технологій
31 серпня 2023 р., протокол № 5

Голова Вченої ради
Тетяна НІКІТЧУК

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ОК 11 «ТЕСТУВАННЯ НА ПРОНИКНЕННЯ, ЕТИЧНИЙ ХАКІНГ ТА ЦИФРОВА КРИМІНАЛІСТИКА»

для здобувачів вищої освіти освітнього ступеня «магістр»
спеціальності 125 «Кібербезпека та захист інформації»
освітньо-професійна програма «Кібербезпека»
факультет інформаційно-комп'ютерних технологій
кафедра комп'ютерної інженерії та кібербезпеки

Схвалено на засіданні
кафедри комп'ютерної
інженерії та кібербезпеки
28 серпня 2023 р., протокол № 7

Завідувач кафедри
Андрій ЄФІМЕНКО

Гарант освітньо-
професійної програми
Володимир ВОРОТНІКОВ

Розробник: кандидат технічних наук, доцент, завідувач кафедри комп'ютерної інженерії та кібербезпеки Андрій ЄФІМЕНКО

Житомир
2023 – 2024 н.р.

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань,
освітній ступінь</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td>Кількість кредитів – 3</td><td>Галузь знань:
12 Інформаційні технології</td><td colspan="2">нормативна
(нормативна, за вибором)</td></tr>
<tr><td>Модулів – 1</td><td rowspan="5">Спеціальність
125 Кібербезпека та захист інформації</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td rowspan="2">Змістових модулів – 4</td><td>1-й</td><td>-</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 90</td><td>2-й</td><td>-</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="10">Тижневих годин для денної форми навчання:
аудиторних – 4
самостійної роботи – 2</td><td rowspan="10">Освітній ступінь «Магістр»</td><td>16 год.</td><td>4</td></tr>
<tr><td colspan="2">Практичні</td></tr>
<tr><td>–</td><td>–</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>32 год.</td><td>6</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>42 год.</td><td>80</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td colspan="2">Вид контролю: екзамен</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної та індивідуальної роботи становить:

для денної форми навчання – 53 % аудиторних занять, 47 % самостійної та індивідуальної роботи;

для заочної форми навчання − 11 % аудиторних занять, 89 % самостійної та індивідуальної роботи.

2. Мета та завдання навчальної дисципліни

Метою навчальної дисципліни «Тестування на проникнення, етичний хакінг та цифрова криміналістика» є формування комплексу знань, які необхідні для проведення тестування комп'ютерних систем на проникнення, уміння застосовувати нормативно-правові, організаційні та технічні процедури етичного хакінгу, ознайомлення з теоретичними положеннями криміналістичної науки, оволодіння криміналістичними засобами, прийомами та методами збирання, дослідження, оцінки та використання доказів під час розслідування та попередження злочинів у цифровому середовищі.

Завданнями вивчення навчальної дисципліни «Тестування на проникнення, етичний хакінг та цифрова криміналістика» є набуття знань, умінь та навичок (компетентностей), спрямованих на:

- знання та уміння виявляти випадки порушення кібербезпеки;
- знання та вміння здійснювати аналіз цифрової інформації;
- знання та вміння виконувати тестування на проникнення;
- знання та вміння застосовувати нові методи в дослідницькій і прикладній діяльності в сучасній системі цифрової криміналістики;
- знання та вміння здійснювати аналіз ризиків функціонування комп'ютерних систем;
- знання та вміння порівнювати і зіставляти цифрові докази і традиційні докази для встановлення відмінностей між ними; використовувати і критично аналізувати моделі процесів цифрової криміналістики;
- знання та вміння визначати послідовність аналізу, формувати моделі порушника та загроз, використовувати сучасні методи та методики аналізу ризиків, оцінювати управління ризиками;
- знання та вміння здійснювати систематичний збір і обробку інформації, яка може бути використана для підвищення захищеності мережі, процесу ухвалення рішення, оцінки програм або вироблення політики безпеки;
- знання та вміння застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки для розслідування внутрішніх та зовнішніх інцидентів в сфері кібербезпеки.
- знання та вміння використовувати інструменти для етичного злому;
- знання та вміння підготовки звіту із висновками та рекомендаціями щодо рівня захищеності інформаційно-комунікаційних систем.

Зміст навчальної дисципліни направлений на формування наступних **компетентностей**, визначених стандартом вищої освіти зі спеціальності 125 спеціальності «Кібербезпека та захист інформації»:

КЗ-1. Здатність застосовувати знання у практичних ситуаціях.

КЗ-2. Здатність проводити дослідження на відповідному рівні.

КФ-2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.

КФ-3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.

КФ-5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ-7. 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.

КФ-8. 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.

Отримані знання з навчальної дисципліни стануть складовими наступних програмних результатів навчання за спеціальністю 125 «Кібербезпека та захист інформації»:

РН-2. Інтегрувати фундаментальні та спеціальні знання для розв’язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.

РН-3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

РН-4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

РН-5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.

РН-6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

РН-7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв’язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

РН-8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.

РН-10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

РН-12. 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.

РН-13. 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.

РН-16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.

РН-19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.

РН-20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.

РН-21. Використовувати методи натурного, фізичного і комп’ютерного

моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

РН-22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.

РН-23. 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.

3. Програма навчальної дисципліни

Змістовий модуль 1. Основи етичного хакінгу

Тема 1. Введення в етичний хакінг. Основи етичного хакінгу

1. Знайомство з термінологією безпеки.
2. Основні загрози інформаційної безпеки.
3. Хакінг та його концепція.
5. Основні стадії хакінгу.
6. Види хакерських атак.

Тема 2. Види тестування на проникнення. Класифікація та цілі проникнення.

1. Тестування на проникнення – чорний, білий, сірий ящик.
2. Області тестування на проникнення.
3. Стартові точки иа канали доступу для тестів на проникнення.
4. Цілі проникнення. Межі тестування на проникнення. Класифікація.

Тема 3. Методологія тестування на проникнення

1. Вимоги до методики випробування на проникнення.
2. П’ять фаз тесту на проникнення.
3. Модулі для процедур тестування.
4. Принцип виключення.
5. Методології тестування на проникнення: OSTMM та ISSAF.

Тема 4. Юридичні питання тестування на проникнення

1. Правові рамки тестування на проникнення.
2. Важливі умови договору між тестером на проникнення та клієнтом.

3. Обов'язки тестера.
4. Обмеження відповідальності.

Змістовий модуль 2. Спеціалізоване програмне забезпечення для тестування на проникнення

Тема 5. Виконання тестів на проникнення. Сканування портів та вразливостей. IDS

1. Підготовка. Розвідка. Аналіз інформації.
2. Утиліти сканування. Використання AngryIP
3. Виконання сканування портів. Типи сканування портів.
4. Сканери вразливості. Типи сканування вразливостей.
5. Характеристика систем виявлення вторгнень. Огляд видів систем.

Тема 6. Тестування на проникнення інфраструктури. Ін’єкції SQL

1. Види тестування на проникнення інфраструктури .
2. Тестування зовнішньої та внутрішньої інфраструктури.
3. Кваліфікація тестерів на проникнення.
4. Ін’єкції SQL, їх види.
5. Методи проникнення через ін’єкції SQL.

Тема 7. Мобільні пристрої та тестування на проникнення. Характеристика тестування на проникнення в бездротові мережі.

1. Роль мобільних пристроїв у процесі тестування.
2. Огляд тестування бездротових мереж.
3. RFID-тестування, NFC-тестування, IoT-тестування.

Тема 8. Збір інформації та написання звітів.

1. Класифікація типів інформації.
2. Класифікація методів збору даних.
3. Етапи написання звітів. Планування звіту.
4. Зміст звіту про тестування на проникнення.

Змістовий модуль 3. Основи цифрової криміналістики

Тема 9. Електронні (цифрові) докази

1. Цифрові дані як докази: визначення, роль, типи, характеристика, законодавчі вимоги.
2. Характеристика криміналістичних досліджень.
3. Типи кіберзлочинів, проблеми розслідувань, загальні правила криміналістичних досліджень.

5. Типи електронних доказів.

6. Ролі та обов'язки осіб, що проводять криміналістичні дослідження.

Тема 10. Процес первинних цифрових криміналістичних досліджень

1. Загальний огляд процесу первинних цифрових криміналістичних досліджень..

2. Ключові компоненти ідентифікації, збирання, здобуття та збереження цифрових доказів.

3. Процес первинних цифрових криміналістичних досліджень: комп'ютерів, периферійних пристроїв та носіїв для збереження цифрових даних, які не під'єднані до мережі; мережних пристроїв.

Тема 11. Структура жорсткого диску та файлових систем

1. Типи жорстких дисків зберігання даних, їх характеристики.

2. Фізична та логічна структура жорстких дисків.

3. Розділи жорстких дисків.

4. Завантаження з диску ОС Windows, Linux, Mac, їх файлові системи.

5. Відмінності різноманітних RAID систем зберігання.

6. Порядок аналізу файлових систем.

Тема 12. Отримання даних та створення дублікатів носіїв даних

1. Загальний опис процесу вилучення даних.

2. Отримання динамічних (live data) та статичних (static data) даних.

3. Порядок дій під час отримання та дублювання даних.

4. Забезпечення незмінності оригінальних носіїв даних.

5. Визначення ефективних методів і засобів отримання даних з комп'ютерів із встановленими ОС Windows і ОС Linux.

Змістовий модуль 4. Технічні засоби цифрової криміналістики

Тема 13. Засоби стирання, видалення даних та інформації. Обладнання для блокування запису.

1. Пристрої для знищення цифрової інформації, їх типи.

2. Обладнання для віддаленого і екстреного знищення інформації на жорстких дисках.

3. Принципи функціонування апаратних та програмних блокаторів запису.

Тема 14. Аналіз зібраної інформації та відновлення даних. Захищені модульні системи зберігання даних

1. Аналізатори протоколів.

2. Пристрої для аналізу протоколів інтерфейсу ATA.

3. Захищені модульні системи зберігання даних .
4. Засоби шифрування інформації на накопичувачах.
5. Дублікатори та перетворювачі інтерфейсів.

Тема 15. Криміналістичні дослідження мобільних пристроїв . Апаратно-програмні засоби шифрування мобільного зв'язку.

1. Роль апаратних і програмних платформ у криміналістичному дослідження мобільних пристроїв.
2. Стек архітектури Android і процеси завантаження системи.
3. Стек архітектури iOS і процеси завантаження системи.
4. Визначення місць збереження доказових даних.
5. Засоби шифрування мобільного зв'язку: дзвінків, повідомлень SMS та електронної пошти (Secusmart GmbH).

Тема 16. Складання звіту і представлення результатів криміналістичних досліджень

1. Узагальнений шаблон звіту криміналістичних досліджень.
2. Види звітів та методика їх складання.
3. Порівняння ролей експертів і технічних спеціалістів.

4. Структура (тематичний план) навчальної дисципліни

Змістові модулі і теми	Кількість годин							
	денна форма				заочна форма			
	усього	лекції	лабораторні	самостійна робота	усього	лекції	лабораторні	самостійна робота
Змістовий модуль 1. Основи етичного хакінгу								
Тема 1. Введення в етичний хакінг. Основи етичного хакінгу	5	1	2	2	5	1	2	2
Тема 2. Види тестування на проникнення. Класифікація та цілі проникнення.	5	1	2	2	5			5
Тема 3. Методологія тестування на проникнення	6	1	2	3	6			6
Тема 4. Юридичні питання тестування на проникнення	6	1	2	3	6			6
Разом за змістовий модуль 1	22	4	8	10	22	1	2	19
Змістовий модуль 2. Спеціалізоване програмне забезпечення для тестування на проникнення								
Тема 5. Виконання тестів на проникнення. Сканування портів та вразливостей. IDS	5	1	2	2	5	1	2	2

Тема 6. Тестування на проникнення веб-додатків. Ін'єкції SQL	5	1	2	2	5			5
Тема 7. Мобільні пристрої та тестування на проникнення. Характеристика тестування на проникнення в бездротові мережі.	6	1	2	3	6			6
Тема 8. Збір інформації та написання звітів.	6	1	2	3	6			6
Разом за змістовий модуль 2	22	4	8	10	22	1	2	19
Змістовий модуль 3. Основи цифрової криміналістики								
Тема 9. Електронні (цифрові) докази	5	1	2	2	5	1	2	2
Тема 10. Процес первинних цифрових криміналістичних досліджень	5	1	2	2	5			5
Тема 11. Структура жорсткого диску та файлових систем	6	1	2	3	6			6
Тема 12. Отримання даних та створення дублікатів носіїв даних	6	1	2	3	6			6
Разом за змістовий модуль 3	22	4	8	10	22	1	2	19
Змістовий модуль 4. Технічні засоби цифрової криміналістики								
Тема 13. Засоби стирання, видалення даних та інформації. Обладнання для блокування запису.	6	1	2	3	6	1		5
Тема 14. Аналіз зібраної інформації та відновлення даних. Захищені модульні системи зберігання даних	6	1	2	3	6			6
Тема 15. Криміналістичні дослідження мобільних пристроїв . Апаратно-програмні засоби шифрування мобільного зв'язку.	6	1	2	3	6			6
Тема 16. Складання звіту і представлення результатів криміналістичних досліджень	6	1	2	3	6			6
Разом за змістовий модуль 4	24	4	8	12	24	1	0	23
ВСЬОГО	90	16	32	42	90	4	6	80

5. Теми практичних (лабораторних) занять

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	ОС Kali Linux. Встановлення Kali Linux	2	-
2	Встановлення Metasploitable	2	-
3	Налаштування мережі для тестування на проникнення	2	-
4	Створення та запуск веб-сервера	2	-
5	Тестування на проникнення бездротових мереж	2	-
6	Сканування вразливостей з OpenVAS 8.0	2	-
7	Автоматичний пошук і перевірка експлойтів в Kali Linux за допомогою Armitage	2	-
8	Сканування мереж. Перехоплення даних в мережах	2	-
9	Збір та аналіз цифрової криміналістичної інформаці в ОС Windows	2	-
10	Збір та аналіз цифрової криміналістичної інформаці в ОС Linux. Аналіз журналів подій Linux.	2	-
11	Архітектура Apache веб-сервера і криміналістичний аналіз його логфайлів.	2	-
12	Розмежування доступу, застосування різних програм шифрування при збереженні інформації на дисках	2	-
13	Архівування та резервне копіювання даних	2	-
14	Криміналістичне дослідження хмарних сховищ Dropbox та Google Drive	2	-
15	Інструменти й техніки мережевої криміналістики: Wireshark, NetWitness, NetIntercept	2	-
16	Дослідження електронної пошти за допомогою MXToolbox Email Header Analyzer	2	-
РАЗОМ		32	-

6. Завдання для самостійної роботи

Тема 1. Безпека ІТ та тестування на проникнення

1. Що таке тестування на проникнення?
2. Чому потрібне тестування на проникнення?
3. Коли виконувати тестування на проникнення?
4. Основні обмеження тестування на проникнення.

Тема 2. Загальні вимоги до тестування на проникнення

1. Організаційні вимоги.
2. Вимоги до персоналу.
3. Технічні вимоги.
4. Етичні питання.

Тема 3. Атаки на паролі

1. Хеші паролів.
2. Мистецтво ручного вгадування паролів.
3. Атаки на хеш.

Тема 4. Експлуатація з використанням атак на стороні клієнта:

1. Експлуатація клієнтів.
2. Огляд можливостей експлуатації браузера.

Тема 5. Технічні особливості огляду засобів комп'ютерної техніки, виявлених на місці події.

1. Огляд стандартних засобів комп'ютерної техніки.
2. Огляд мобільних засобів комп'ютерної техніки із функцією телефону.
3. Огляд автомобільних засобів комп'ютерної техніки.

Тема 6. Обробка цифрової криміналістики в програмному забезпеченні.

1. Аналіз реєстру Windows.
2. Використання Hex-редактора.
3. Отримання та збереження доказів.
4. Імпорт доказів.
5. Пошук і фільтрація

Тема 7. Типові випадки і рекомендації по їх дослідженню

1. Типові випадки інцидентів, пов'язаних з витоком даних.
2. Типовий випадок інциденту з компрометації клієнтського пристрою / системи.
3. Типовий випадок інциденту, причиною якого є шкідливий код.

Тема 8. Звітність і труднощі застосування цифрової криміналістики

1. Як ефективно вести звітність по роботі цифрового криміналіста.
2. Хмарні технології.
3. Віртуалізація.
4. Мобільні пристрої та принцип BYOD (Bring Your Own Device).

7. Індивідуальні завдання

Індивідуальні завдання з дисципліни «Тестування на проникнення, етичний хакінг та цифрова криміналістика» полягають у виконанні лабораторних робіт згідно варіанту по списку в журналі та відпрацюванні матеріалу навчальних курсів мережевої академії Cisco NetAcad (проходження онлайн навчання, виконання тестових контрольних робіт, виконання тестових проміжних оцінювань).

8. Методи навчання

В ході вивчення дисципліни використовуються наступні методи навчання: мультимедійні презентації, аналіз інформації з відкритих джерел, комп'ютерне моделювання, статистичний аналіз.

Основними видами занять, які проводяться під керівництвом викладача, є лекції, лабораторні роботи та самостійна робота.

На лекціях розглядаються загальні теоретичні положення дисципліни. Під час проведення лекцій використовуються мультимедійні засоби для інтерактивної демонстрації прикладів та графічного матеріали. До кожної лекції студентам додається презентація основних положень.

При виконанні лабораторних робіт зміцнюються знання, отримані на лекціях, набуваються первинні навички з проведення розрахунків міцності захисту, створення моделі загроз та моделі порушника, комп'ютерного моделювання загроз за допомогою різного програмного забезпечення, реалізації моделей контролю доступу до інформації з обмеженим доступом.

При самостійній роботі студенти набувають навички самостійного освоєння матеріалу, який не використаний в навчальному процесі.

9. Методи контролю

Контрольні заходи включають поточний та підсумковий модульний контроль. Поточний контроль здійснюється під час проведення лабораторних занять для перевірки рівня підготовки студента до виконання конкретного завдання. Форма проведення поточного контролю: усне опитування, вирішення ситуаційних задач, тестовий контроль. Оцінюється вхідний, проміжний, кінцевий рівень знань студента. Підсумковий контроль проводиться у вигляді комп'ютерних тестів та/або виконання практичних завдань.

10. Розподіл балів

Поточне оцінювання та самостійна робота								РАЗОМ
Змістовий модуль 1				Змістовий модуль 2				
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	
6,25	6,25	6,25	6,25	6,25	6,25	6,25	6,25	
Поточне оцінювання та самостійна робота								
Змістовий модуль 3				Змістовий модуль 4				
Т9	Т10	Т11	Т12	Т13	Т14	Т15	Т16	
6,25	6,25	6,25	6,25	6,25	6,25	6,25	6,25	
							РАЗОМ	100

Шкала оцінювання

За шкалою	Екзамен	Залік	Бали
A	Відмінно	Зараховано	90-100
B	Добре	Зараховано	82-89
C			74-81
D	Задовільно	Зараховано	64-73
E			60-63
FX	Незадовільно	Не зараховано	35-59
F		Не зараховано	0-34

11. Рекомендована література

Основна література

1. Цифрова криміналістика : консп. лекцій / уклад. І. З. Якименко. - Тернопіль : ТНЕУ, 2019. – 109 с.

2. Ethical Hacking and Penetration Testing Guide/ Rafay Baloch. - Auerbach Publications, 2014. – 531 p.

3. Georgia Weidman. Penetration testing. A Hands-On Introduction to Hacking/ Georgia Weidman. – San Francisco, 2014. – 501 p.

4. Навчальний курс Ethical Hacking. [Електронний ресурс] – skillsforall.com

5. Навчальний курс Junior Penetration Tester. [Електронний ресурс] – rangeforce.com

6. Навчальний курс Web Application Security. [Електронний ресурс] – rangeforce.com

Допоміжна література

1. Полотай О.І. «Роль комп'ютерної криміналістики у забезпеченні інформаційної безпеки. Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення» : матеріали Міжнародної наукової інтернет-конференції. – Тернопіль. вип. 67. 2022. – с. 41-43

2. Інноваційні методи та цифрові технології в криміналістиці, судовій експертизі та юридичній практиці : матеріали міжнар. «круглого столу» (Харків, 12 груд. 2019 р.) / редкол.: В. Ю. Шепітько (голов. ред.), В. А. Журавель, В. М. Шевчук, Г. К. Авдєєва. – Харків : Право, 2019. – 164 с.

3. Karie, Nickson M. and H. S. Venter (2015). Taxonomy of Challenges for Digital Forensics. Journal of Forensic Sciences, Vol. 60(4), 885–893 p.

12. Інформаційні ресурси в Інтернеті

1. https://securityonline.info/category/forensics/
2. http://www.dfrws.org/
3. https://www.forensicmethods.com
4. https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools
5. http://www.pentest-standard.org/index.php/Exploitation