МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

Кафедра інформаційних технологій та кібербезпеки факультету №4

МЕТОДИЧНІ МАТЕРІАЛИ
ДО ПРАКТИЧНИХ ЗАНЯТЬ

з навчальної дисципліни "Кібербезпека"
обов'язкових компонент
освітньої програми першого рівня вищої освіти

125 "Кібербезпека" (Протидія кіберзлочинності)

Харків 2020

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 23.09.2020 № 9

СХВАЛЕНО
Вченою радою факультету №4
Протокол від 16.09.2020 № 5

ПОГОДЖЕНО
Секцією науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 18.09.2020 № 5

Розглянуто на засіданні кафедри інформаційних технологій та кібербезпеки (протокол від 15.09.2020 № 16)

Розробник: професор кафедри інформаційних технологій та кібербезпеки ХНУВС, к.т.н. доцент Носов В.В.

Рецензенти:

доцент кафедри інформаційних технологій та кібербезпеки факультету №4 Харківського національного університету внутрішніх справ к.т.н. доцент Тулупов В.В.

завідувач кафедри інформаційних управляючих систем Харківського національного університету радіоелектроніки, д.т.н. професор Петров К.Е.

1. Розподіл часу навчальної дисципліни за темами

Номер та назва навчальної теми	Кількість годин відведених на вивчення навчальної дисципліни					Вид контролю
	Всього	з них:				
		лекції	Практичні заняття	Лабораторні заняття	Самостійна робота	
Семестр №6						
Тема №1. Основні відомості про кібербезпеку	16	6	2		8	залік
Тема №2. Пасивний збір інформації	36	8	4	6	18	
Тема №3. Активний збір інформації про мережу	36	8	4	6	18	
Тема №4. Механізми захисту мережі від збору інформації, сканування та проникнення	32	8	4	6	16	
Тема №5. Застосування криптографічних сервісів	36	8	4	6	18	
Тема №6. Аналіз трафіку в комп'ютерних мережах	32	8	4	6	16	
Тема №7. Перехоплення сесій передачі даних в комп'ютерних мережах	36	8		6	18	
Тема №8. Безпека в безпровідних мережах	36	8	4	6	18	
Тема №9. Безпека в операційних системах	40	10	4	6	20	
Всього за семестр №6	**300**	**72**	**30**	**48**	**150**	
Семестр №7						
Тема №10. Шкідливе програмне забезпечення	24	6	4	4	12	екзамен
Тема №11. Переповнення буферу	24	6		4	12	
Тема №12. Безпека веб-серверів та веб-застосувань	32	6	6	6	16	
Тема №13. Атака «відмова в обслуговуванні»	24	6		4	12	
Тема №14. SQL-ін'єкції	32	6	4	6	16	
Тема №15. Соціальна інженерія	24	6	4	4	12	
Тема №16. Тестування на вразливість до атак	20	4		4	10	
Всього за семестр №7	**180**	**40**	**18**	**32**	**90**	
Всього за дисципліною	**480**	**112**	**48**	**80**	**240**	

2. Методичні вказівки до практичних занять

Тема №1. Основні відомості про кібербезпеку

Практичне заняття 1. Встановлення Kali Linux

Навчальна мета заняття: навчитися інсталювати спеціалізовану ОС, що використовується для тестування безпеки

Кількість годин: 2 год.

Навчальні питання

1. Встановлення Kali Linux
2. Основні команди Linux
3. Налаштування мережі
4. Встановлення оновлень
5. Підключення клієнта віддаленого керування по ssh протоколу

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.
Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Дати коротку характеристику ОС Kali Linux. Надати посилання до місця розміщення дистрибутиву ОС.

Охарактеризувати засіб віртуалізації – VirtualBox. Надати посилання до місця розміщення дистрибутиву.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №2. Пасивний збір інформації

Практичне заняття 2. Аналіз результатів пасивного збору інформації

Навчальна мета заняття: навчитися аналізувати результати пасивного збору інформації
Кількість годин: 2 год.

Навчальні питання

1. Побудова та аналіз зв'язків за результатами пасивного збору інформації
2. Збір інформації за заголовками електронної пошти

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.
Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Дати коротку характеристику сервісів і засобів аналізу результатів пасивного збору інформації. Надати посилання на відповідні засоби.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Практичне заняття 3. Засоби та сервіси OSINT

Навчальна мета заняття: навчитися користуватися засобами і наявними сервісами OSINT
Кількість годин: 2 год.

Навчальні питання

1. Наявні OSINT сервіси.
2. Відомі OSINT утиліти

Література: пошукові сервіси глобальної мережі.
Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Дати коротку характеристику актуальних OSINT сервісів і засобів. Надати посилання на відповідні засоби.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №3. Активний збір інформації про мережу

Практичне заняття 4. Засоби активного отримання інформації за певними протоколами

Навчальна мета заняття: навчитися користуватися засобами активного отримання інформації за протоколами NetBIOS, SNMP, LDAP, SMTP, DNS.

Кількість годин: 2 год.

Навчальні питання

1. Засоби отримання інформації зпротоколів NetBIOS, SNMP, LDAP.
2. Засоби отримання інформації зпротоколів SMTP, DNS

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.
Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Дати коротку характеристику засобам активного отримання інформації за протоколами NetBIOS, SNMP, LDAP, SMTP, DNS. Надати посилання на відповідні засоби.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Практичне заняття 5. Засоби пошуку вразливостей

Навчальна мета заняття: навчитися користуватися засобами пошуку вразливостей віддалених ресурсів.

Кількість годин: 2 год.

Навчальні питання

1. Сканер вразливостей OpenVAS.
2. Налаштування SSH-тунелю

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Дати коротку характеристику сканеру вразливостей. Надати посилання на порядок встановлення і використання сканеру вразливостей.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №4. Механізми захисту мережі від збору інформації, сканування та проникнення

Практичне заняття 6. Пастки Honeypot

Навчальна мета заняття: навчитися користуватися засобами імітування цілей атаки.

Кількість годин: 4 год.

Навчальні питання

1. Пастка IoT-Honeypot.
2. Пастка Heralding.
3. Пастка Kippo.

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Дати коротку характеристику засобам імітування цілей атаки. Вказати порядок встановлення і використання засобів.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №5. Застосування криптографічних сервісів
Практичне заняття 7. Засоби криптографії і криптоаналізу

Навчальна мета заняття: навчитися користуватися засобами криптографії і криптоаналізу
Кількість годин: 4 год.

Навчальні питання

1. Симетричні алгоритми
2. Асиметричні алгоритми
3. Геші
4. Колізії
5. Інструменти та методи для підбору гешів

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.
Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Дати коротку характеристику набору OpenSSL та напрямам застосування криптографії. Вказати спосіб встановлення додаткових застосунків в ОС.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №6. Аналіз трафіку в комп'ютерних мережах
Практичне заняття 8. MITM атаки

Навчальна мета заняття: ознайомитися із засобами проведення MITM атак
Кількість годин: 4 год.

Навчальні питання

1. Xerosploit.
2. Evilginx2.
3. Morpheus Framework.

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.
Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Дати коротку характеристику MITM атакам. Вказати порядок встановлення і використання засобів проведення MITM атак.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №8. Безпека в безпровідних мережах

Практичне заняття 9. Втручання у роботу WiFi мереж

Навчальна мета заняття: ознайомитися із засобами проведення DoS атак і створення підроблених точок доступу WiFi мереж

Кількість годин: 4 год.

Навчальні питання

1. DoS атака на безпровідні мережі.
2. Створення підроблених точок доступу.

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Вказати порядок встановлення і використання засобів проведення активного втручання у роботу WiFi мереж.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №9. Безпека в операційних системах

Практичне заняття 10. Атаки на парольний захист

Навчальна мета заняття: ознайомитися із засобами атак на парольний захист

Кількість годин: 4 год.

Навчальні питання

1. Утиліта John the ripper.
2. Утиліта Hashcat.
3. Генерація словників Crunch і Mentalist.

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Вказати порядок встановлення і використання засобів атак на парольний захист.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №10. Шкідливе програмне забезпечення

Практичне заняття 11. Шкідливе програмне забезпечення ОС Android

Навчальна мета заняття: ознайомитися із засобами створення шкідливого програмного забезпечення для ОС Android

Кількість годин: 4 год.

Навчальні питання

1. Утиліта MSFvenom.
2. Утиліта SpyNoteShell.

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Вказати порядок встановлення і використання засобів створення шкідливого програмного забезпечення для ОС Android.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №12. Безпека веб-серверів та веб-застосувань

Практичне заняття 12. Міжсайтові підробка запиту і скриптинг

Навчальна мета заняття: ознайомитися із техніками атак Cross Site Request Forgery і Cross Site Scripting

Кількість годин: 6 год.

Навчальні питання

1. Міжсайтова підробка запиту (Cross Site Request Forgery).
2. Stored XSS.
3. Reflected XSS.
4. XSStrike.

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Дати коротку характеристику техніками атак Cross Site Request Forgery і Cross Site Scripting. Вказати порядок встановлення і використання тестового веб-додатку DVWA.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №14. SQL-ін'єкції

Практичне заняття 13. Засоби тестування SQL-ін'єкцій

Навчальна мета заняття: ознайомитися інструментами тестування SQL-ін'єкцій

Кількість годин: 4 год.

Навчальні питання

1. Використання SleuthQL.
2. Використання LazySQLMap.

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Дати коротку характеристику інструментам тестування SQL-ін'єкцій. Вказати порядок встановлення і їх використання на тестовому веб-додатку.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №15. Соціальна інженерія

Практичне заняття 14. Засоби забезпечення соціальної інженерії

Навчальна мета заняття: ознайомитися із засобами забезпечення соціальної інженерії

Кількість годин: 4 год.

Навчальні питання

1. QRLJacking.

2. Camelishing.
3. Gophish.

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.
Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Дати коротку характеристику засобами забезпечення соціальної інженерії. Вказати порядок їх встановлення і використання.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №16. Тестування на вразливість до атак
Практичне заняття 15. Тестування на вразливість до атак

Навчальна мета заняття: навчитися проводити тестування на вразливість до атак комп'ютерних систем

Кількість годин: 4 год.

Навчальні питання

1. Тестування на вразливість до атак

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.
Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Intertnet; медіа проектор.

План проведення заняття

І. Порядок проведення вступу до заняття.

Дати коротку характеристику процедурі тестування на вразливість до атак. Вказати спосіб встановлення потрібних застосунків в ОС.

ІІ. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

ІІІ. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

3. Рекомендована література (основна, допоміжна), інформаційні ресурси в Інтернеті

Основна

1. Кібербезпека для спеціальних агентів кіберполіції (лекції). OSCE. 2016.

2. Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.
3. Matt Walker. CEH Certified Ethical Hacker All-in-One Exam Guide. McGraw-Hill, 2012.
4. ITU-T Rec. X.805. Security architecture for systems providing end-to-end communications. / ITU-T Recommendation X.805, 10/2003. URL: https://www.itu.int/rec/T-REC-X.805-200310-I/en (дата звернення: 20.09.2016).

Допоміжна

5. ITU-T Rec. X.800. Security architecture for Open Systems Interconnection for CCITT applications. / Recommendation X.800, Geneva, 1991. URL: http://www.itu.int/rec/T-REC-X.800-199103-I (дата звернення: 20.09.2016).
6. ITU-T E.408. Telecommunication networks security requirements. / ITU-T Recommenda-tion E.408, 05/2004. URL: https://www.itu.int/rec/T-REC-E.408-200405-I/en (дата звер-нення: 20.09.2016).
7. NIST Special Publication 800-33. Underlying Technical Models for Information Technol-ogy Security. / Gary Stoneburner. CODEN: NSPUE2, December 2001. URL: http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf (дата звернення: 20.09.2016).

Інформаційні ресурси

1. http://www.hackerhighschool.org/
2. https://securityonline.info/
3. https://kali.tools/
4. https://tools.kali.org/
5. https://hackersonlineclub.com/
6. https://hakin9.org/
7. https://gbhackers.com/
8. https://securityonline.info/
9. https://www.hackingarticles.in/