ЗАТВЕРДЖЕНО
Вченою радою факультету
інформаційно-комп'ютерних технологій
31 серпня 2023 р., протокол № 5
Голова Вченої ради
Тетяна НІКІТЧУК

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ОК 29 «КІБЕРОПЕРАЦІЇ»

для здобувачів вищої освіти освітнього ступеня «бакалавр»
спеціальності 125 «Кібербезпека та захист інформації»
освітньо-професійна програма «Кібербезпека та захист інформаційя»
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
Андрій ЄФІМЕНКО

Розробник: кандидат технічних наук, завідувач кафедри комп'ютерної інженерії та кібербезпеки Єфіменко Андрій Анатолійович

Житомир
2026-2027 н.р.

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність, освітній ступінь</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td colspan="2">денна форма навчання</td></tr>
<tr><td>Кількість кредитів 7</td><td>Галузь знань
12 «Інформаційні технології»</td><td colspan="2">Нормативна</td></tr>
<tr><td>Модулів – 2</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 colspan="2">4-й</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 210</td><td>7-й</td><td>8-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="11">Тижневих годин для денної форми навчання:
аудиторних –
2 (7-й семестр),
5 (8-й семестр)
самостійної роботи –
1,75 (7-й семестр),
5,625 (8-й семестр)</td><td rowspan="11">Освітній ступінь «бакалавр»</td><td>16 год.</td><td>12 год.</td></tr>
<tr><td colspan="2">Практичні</td></tr>
<tr><td>–</td><td>–</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>16 год.</td><td>48 год.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>28 год.</td><td>90 год.</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td colspan="2">Вид контролю:
7семестр – залік,
8 семестр – екзамен ,
курсовий проект</td></tr>
</table>

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

для денної форми навчання – 44% аудиторних занять, 56% самостійної та індивідуальної роботи;

2. Мета та завдання навчальної дисципліни

Метою навчальної дисципліни є формування теоретичних знань та практичних навичок для моніторингу, аналізу, проведення кібероперацій.

Завданнями вивчення дисципліни є:

- оволодіння знаннями щодо принципів побудови центрів моніторингу та управління кібербезпекою;
- опанування додаткових понять та узагальнення знань ОС Windows в контексті безпечності архітектури ОС, принципів та схем безпечного адміністрування, наявності вразливостей, використання засобів захисту в контексті організації моніторингу та управління кібербезпекою інформаційних систем;
- опанування додаткових понять та узагальнення знань ОС Linux в контексті безпечності архітектури ОС, принципів та схем безпечного адміністрування, наявності вразливостей, використання засобів захисту в контексті організації моніторингу та управління кібербезпекою інформаційних систем;;
- опанування додаткових понять та узагальнення знань про мережні протоколи в контексті проблем безпеки та принципів захисту протоколів;
- оволодіння поняттями та знаннями складних мережних інфраструктур сучасних підприємств в контексті організації моніторингу та управління кібербезпекою інформаційних систем;;
- опанування принципів та набуття навичок забезпечення безпеки мережної інфраструктури в контексті організації моніторингу та управління кібербезпекою інформаційних систем;;
- набуття знань та умінь поглибленого аналізу мережних атак;
- набуття навичок для захисту мережних інфраструктур різного роду;
- узагальнення знань та набуття навичок застосування засобів криптографії та інфраструктури відкритих ключів;
- опанування знань та набуття навичок аналізу захищеності та забезпечення захисту кінцевих точок;
- опанування знань щодо принципів, методів та отримання вмінь використання засобів моніторингу безпеки;
- опанування знань щодо принципів, методів за набуття вмінь використання засобів аналізу даних вторгнень;
- опанування знань та набуття навичок для реагування на інциденти кібербезпеки та їх оброблення.

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

Загальні компетентності:

КЗ 2. Знання та розуміння предметної області та розуміння професії.

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.

Фахові компетентності:

КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)

КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.

КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

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

РН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;

РН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;

РН 4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;

РН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;

РН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки;

РН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки;

РН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;

РН 10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем;

РН 11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах;

РН 12. Розробляти моделі загроз та порушника;

РН 13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних;

РН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій;

РН 16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів;

РН 17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент;

РН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;

РН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;

РН 21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;

РН 25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту;

РН 27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;

РН 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;

РН 33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;

РН 35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки;

РН 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;

РН 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;

РН 43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів;

РН 44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами;

РН 45. Застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;

РН 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;

РН 48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;

РН 50. Забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);

РН 51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах;

РН 53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.

3. Програма навчальної дисципліни

Модуль 1
1. Змістовий модуль 1.

Тема 1. Кібербезпека, центри моніторингу та управління кібербезпекою.

Тема 2. Операційні системи Windows. Архітектура, адміністрування, вразливості.

Тема 3. Операційні системи Windows. Архітектура, адміністрування, вразливості.

2. Змістовий модуль 2.

Тема 4. Мережні протоколи. Проблеми безпеки та принципи захисту мережних протоколів.

Тема 5. Мережна інфраструктура сучасного підприємства.

Модуль 2
3. Змістовий модуль 3.

Тема 6. Принципи, методи та засоби забезпечення безпеки мережної інфраструктури.

Тема 7. Поглиблений аналіз мережних атак.

Тема 8. Захист мережної інфраструктури.

Тема 9. Криптографія та інфраструктура відкритих ключів.

4. Змістовий модуль 4.

Тема 10. Захист та аналіз стану кінцевих пристроїв.

Тема 11. Принципи, методи та засоби моніторингу безпеки.

Тема 12. Принципи, методи та засоби аналізу даних вторгнень.

Тема 13. Реагування на інциденти та їх обробка.

4. Структура (тематичний план) навчальної дисципліни

Кредитні модулі	Змістовні модулі	Кількість годин			
		Всього	Лекції	Лабораторні	Самостійна робота
1	2	3	4	5	6
№1, 2	**Модуль 1**				
	Змістовий модуль 1				
	Тема 1. Кібербезпека, центри моніторингу та управління кібербезпекою	10	4	0	6
	Тема 2. Операційні системи Windows. Архітектура, адміністрування, вразливості	12	2	4	6
	Тема 3. Операційні системи Linux. Архітектура, адміністрування, вразливості	12	2	4	6
	Змістовий модуль 2				
	Тема 4. Мережні протоколи. Проблеми безпеки та принципи захисту мережних протоколів	12	4	4	4
	Тема 5. Мережна інфраструктура сучасного підприємств	14	4	4	6
	Разом модуль 1	**60**	**16**	**16**	**28**
	Модуль 2				
	Змістовий модуль 3				
	Тема 6. Принципи, методи та засоби забезпечення безпеки мережної інфраструктури	15	2	6	7
	Тема 7. Поглиблений аналіз мережних атак	15	1	6	8
	Тема 8. Захист мережної інфраструктури	15	1	6	8
	Тема 9. Криптографія та інфраструктура відкритих ключів	15	2	6	7
	Змістовий модуль 4				
	Тема 10. Захист та аналіз стану кінцевих пристроїв	15	1	6	8
	Тема 11. Принципи, методи та засоби моніторингу безпеки	15	1	6	8
	Тема 12. Принципи, методи та засоби аналізу даних вторгнень	15	2	6	7
	Тема 13. Реагування на інциденти та їх обробка	15	2	6	7
	Разом модуль 2	**120**	**12**	**48**	**60**
	Курсовий проект	**30**	**–**	**–**	30
	ВСЬОГО	**210**	**28**	**64**	**118**

5. Теми лабораторних занять

№	Назва теми	Кількість годин
1.	Встановлення та налагодження мережі віртуальних машин CyberOps Workstation, Kali Linux, Security Onion	2
2.	Перехоплення та аналіз мережних повідомлень за допомогою аналізатора трафіку Wireshark	2
3.	Дослідження перехоплених повідомлень протоколів DNS та UDP за допомогою аналізатора трафіку Wireshark	4
4.	Дослідження перехоплених повідомлень протоколів HTTP та HTTPs за допомогою аналізатора трафіку Wireshark	4
5.	Дослідження та аналіз структури шкідливого ПЗ	4
6.	Дослідження та аналіз методів і засобів соціальної інженерії	4
7.	Дослідження функціонування сервісів та процесів передачі трафіку протоколу DNS	4
8.	Дослідження процесів та результатів атак на сервер MySQL	4
9.	Дослідження процесів та результатів атак на журнали	4
10.	Дослідження процесів цифрування та розшифровування даних за допомогою інструментарію хакерів	4
11.	Дослідження процесів перехоплення та підміни трафіку протоколів віддаленого доступу Telnet, SSH	4
12.	Дослідження процесів та інструментів хешування даних	4
13.	Дослідження інструментарію сертифікації ключів	4
14.	Дослідження інструментарію міжмережного екранування на базі Snort	4
15.	Дослідження та робота з інструментарієм оперування з даними безпеки мережі	4
16.	Дослідження процесів та інструментів отримання файлів певних типів з потоків перехопленого трафіку	4
17.	Дослідження методів та процесів ізоляції зламаних вузлів	4
РАЗОМ		**64**

6. Завдання для самостійної роботи

Опрацювання матеріалів навчального курсу Cybersecurity Operations.

7. Індивідуальні завдання

Не передбачені (можуть надаватися за запитом здобувача вищої освіти як додаткові завдання).

8. Методи навчання

Під час викладання освітньої компоненти використовуються наступні методи навчання:

МН1 – вербальні (лекція, пояснення, розповідь, бесіда, інструктаж);

МН2 – наочні (спостереження, ілюстрація, демонстрація);

МН3 – практичні (різні види вправ та завдань, виконання розрахунків, практики);

МН4 – пояснювально-ілюстративний (передбачає надання готової інформації викладачем та її засвоєння студентами);

МН5 – репродуктивний, в основу якого покладено виконання різного роду завдань за зразком;

МН6 – метод проблемного викладу;

МН7 – частково-пошуковий (евристичний);

МН9 – дискусійний метод;

МН10 – метод активного навчання (проведення ділових ігор, ігрового проектування);

МН11 – ситуаційний метод, рішення кейсових завдань.

9. Методи контролю

Оцінювання рівня опанування компетентностей та досягнення програмних результатів навчання, передбачених для освітньої компоненти здійснюється з використанням наступних методів:

МО1 – оцінювання роботи під час аудиторних занять;

МО2 – виконання практичних завдань;

МО3 – поточне тестування;

МО4 – виконання аудиторної контрольної роботи;

МО5 – захист індивідуального завдання;

МО6 – залік/іспит.

10. Розподіл балів

Семестровий розподіл балів:
– відвідування та робота на лекціях – 4 бали.
– робота на лабораторних заняттях (зокрема і поточні контролі) – 24 бали;
– виконання та захист звітів з лабораторних робіт – 24 бали;
– самостійна робота студентів – 8 балів;
– модульні контролі – 40 балів.
Детальний розподіл балів наводиться у рейтинг-листі освітньої компоненти.
Розподіл балів за курсовий проект/роботу:
– виконання курсового проекту (проект системи/мережі) – 60 балів;
– прилюдний захист курсового проекту – 40 балів.

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. Omar Santos, Joseph Muniz CCNA Cyber Ops SECOPS 210-255 Official Cert Guide (Certification Guide) 1st Edition, Cisco Press, 2017.
2. Omar Santos/ Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide (Certification Guide) 1st Edition, Cisco Press, 2017.
3. CCNA Cybersecurity Operations. Companion Guide. 1st Edition, Cisco Press, 2018.
4. Omar Santos, Joseph Muniz, Stefano De Crescenzo CCNA Cyber Ops (SECFND #210-250 and SECOPS #210-255). Official Cert Guide Library. 1st Edition, 2018
5. Навчальний курс CCNA Cybersecurity Operations [Електронний ресурс] – Режим доступу: www.netacad.com.
6. Навчальний курс Cybersecurity Operations [Електронний ресурс] – Режим доступу: www.netacad.com.
7. Навчальний курс Ntwork Security [Електронний ресурс] – Режим доступу: www.netacad.com.
8. Навчальний курс CCNP Enterprise: Core Networking [Електронний ресурс] – Режим доступу: www.netacad.com.

Допоміжна література

1. Бирюков А. А. Информационная безопасность. Защита и нападение. 2-е изд., перераб. и доп. / А. А. Бирюков. – М. : ДМК-Пресс, 2017. – 434 с.
2. Олифер В. Г. Безопасность компьютерных сетей / В. Г. Олифер, Н. А. Олифер. – М. : Горячая линия-Телеком, 2016. – 644 с.
3. Paquet, Catherine. Implementing Cisco IOS Network Security (IINS) / Catherine Paquet. – Cisco Press, 2009. – 600 p.
4. Conlan J., Patrik. Cisco Network Professional. Advanced Internetworking Guide. / Patrik J. Conlan. – Wiley Publishing, 2009. – 854 p.
5. Vyncke, Eric. LAN Switch Security: What Hackers Know about Your Switches / Eric Vyncke, Christopher Paggen. – Cisco Press, 2007. – 340 p.
6. Wilkins, Sean. CCNP Security. SECURE 642-637. Official Cert Guide / Sean Wilkins, Franklin H. Smith III. – Cisco Press, 2011. – 738 p.
1. Watkins, Michael. CCNA Security. Official Exam Certification Guide / Michael Watkins, Kevin Wallace. – Cisco Press, 2008. – 638 p.
2. Santos, Omar. CCNA Security 210-260. Official Cert Guide / Omar Santos, John Stuppi. – Cisco Press, 2015. – 658 p.
3. Barker, Keith. CCNA Security 640-554. Official Cert Guide / Keith Barker, Scott Morris.– Cisco Press, 2013. – 740 p.

12. Інформаційні ресурси в Інтернеті

1. www.netacad.com
2. www.wireshark.org
3. www.gns3.net
4. www.eve-ng.net
5. www.kali.org
6. https://securityonionsolutions.com/
7. https://www.snort.org/