ЗАТВЕРДЖЕНО

Вченою радою факультету інформаційно-комп'ютерних технологій

28 серпня 2024 р., протокол №8

Голова Вченої ради

_____ Тетяна НІКІТЧУК

РОБОЧА ПРОГРАМА
вибіркової навчальної дисципліни фахової підготовки «Кібероперації»

факультет інформаційно-комп'ютерних технологій

для здобувачів вищої освіти освітнього ступеня «бакалавр»

Схвалено на засіданні кафедри комп'ютерної інженерії та кібербезпеки
26 серпня 2024 р., протокол №6

Завідувач кафедри

_____ Андрій ЄФІМЕНКО

Розробник: к.т.н., доцент, завідувач кафедри комп'ютерної інженерії та кібербезпеки Андрій ЄФІМЕНКО

Житомир
2024 – 2025 н.р.

Робоча програма вибіркової навчальної дисципліни «Кібероперації» затверджена Вченою радою факультету інформаційно-комп’ютерних технологій від 28 серпня 2024 р., протокол № 8.

1. Опис навчальної дисципліни

Найменування показників	Характеристика навчальної дисципліни
	денна форма навчання
Кількість кредитів 4	Вибіркова
Модулів – 1	Лекції
	32 год.
Змістових модулів – 2	Практичні
	-
Загальна кількість годин – 120	Лабораторні
	32 год.
Тижневих годин для денної форми навчання: аудиторних – 64 самостійної роботи – 56	Самостійна робота
	56 год.
	Вид контролю: залік

Частка аудиторних занять і частка самостійної та індивідуальної роботи у загальному обсязі годин з навчальної дисципліни становить:

для денної форми навчання – 53 % аудиторних занять, 47 % 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.

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

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

Тема 5. Мережна інфраструктура сучасного підприємства

2. Змістовий модуль 2.

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

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	8	4	0	4
	Тема 2. Операційні системи Windows. Архітектура, адміністрування, вразливості	10	2	4	4
	Тема 3. Операційні системи Linux. Архітектура, адміністрування, вразливості	10	2	4	4
	Тема 4. Мережні протоколи. Проблеми безпеки та принципи захисту мережних протоколів	12	4	4	4
	Тема 5. Мережна інфраструктура сучасного підприємств	12	4	4	4
	Разом змістовний модуль 1	**52**	**16**	**16**	**20**
	Змістовий модуль 2				
	Тема 6. Принципи, методи та засоби забезпечення безпеки мережної інфраструктури	8	2	2	4
	Тема 7. Поглиблений аналіз мережних атак	8	2	2	4
	Тема 8. Захист мережної інфраструктури	8	2	2	4
	Тема 9. Криптографія та інфраструктура відкритих ключів	8	2	2	4
	Тема 10. Захист та аналіз стану кінцевих пристроїв	8	2	2	4
	Тема 11. Принципи, методи та засоби моніторингу безпеки	8	2	2	4
	Тема 12. Принципи, методи та засоби аналізу даних вторгнень	10	2	2	6
	Тема 13. Реагування на інциденти та їх обробка	10	2	2	6
	Разом змістовний модуль 2	**68**	**16**	**16**	**36**
	ВСЬОГО	**120**	**32**	**32**	**56**

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, UDP, HTTP та HTTPs за допомогою аналізатора трафіку Wireshark	2
4.	Дослідження та аналіз структури шкідливого ПЗ	2
5.	Дослідження та аналіз методів і засобів соціальної інженерії	2
6.	Дослідження функціонування сервісів та процесів передачі трафіку протоколу DNS	2
7.	Дослідження процесів та результатів атак на сервер MySQL	2
8.	Дослідження процесів та результатів атак на журнали	2
9.	Дослідження процесів цифрування та розшифровування даних за допомогою інструментарію хакерів	2
10.	Дослідження процесів перехоплення та підміни трафіку протоколів віддаленого доступу Telnet, SSH	2
11.	Дослідження процесів та інструментів хешування даних	2
12.	Дослідження інструментарію сертифікації ключів	2
13.	Дослідження інструментарію міжмережного екранування на базі Snort	2
14.	Дослідження та робота з інструментарієм оперування з даними безпеки мережі	2
15.	Дослідження процесів та інструментів отримання файлів певних типів з потоків перехопленого трафіку	2
16.	Дослідження методів та процесів ізоляції зламаних вузлів	2
РАЗОМ		**32**

6. Завдання для самостійної роботи

Опрацювання матеріалів навчальних курсів CCNA Cybersecurity Operations, 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;
– контрольні роботи – 40 балів.
Детальний розподіл балів наводиться у рейтинг-листі освітньої компоненти.

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/