Міністерство освіти і науки України
Сумський національний аграрний університет
Факультет економіки і менеджменту
Кафедра кібернетики та інформатики

Робоча програма (силабус) освітнього компонента

Управління кібербезпекою

Спеціальність	F6 Інформаційні системи і технології
Освітня програма	Інформаційні системи та технології
Рівень вищої освіти	Другий (магістерський)

СУМИ – 2024

Розробник: Олександр В’ЮНЕНКО доц., к.е.н., доц. кафедри кібернетики та інформатики

(прізвище, ініціали) (вчений ступінь та звання, посада)

Розглянуто, схвалено та затверджено на засіданні кафедри Кібернетики та інформатики протокол від 12 червня 2024 р. № 16

(назва кафедри)

Завідувач кафедри Світлана АГАДЖАНОВА

(підпис) (прізвище, ініціали)

Погоджено:

Гарант освітньої програми Надія ПАСЬКО

(підпис) (ПІБ)

Декан факультету, де реалізується освітня програма Маргарита ЛИШЕНКО

(підпис) (ПІБ)

Рецензія на робочу програму(додається) надана: Світлана АГАДЖАНОВА

(підпис) (ПІБ)

Юлія РУДЕНКО

(підпис) (ПІБ)

Методист відділу якості освіти, ліцензування та акредитації

(підпис) (ПІБ)

Зареєстровано в електронній базі: 12.08.2024 р.

(дата)

Інформація про перегляд робочої програми (силабусу):

Навчальний рік, в якому вносяться зміни	Номер додатку до робочої програми з описом змін	Зміни розглянуто і схвалено		
		Дата та номер протоколу засідання кафедри	Завідувач кафедри	Гарант освітньої програми

1. ЗАГАЛЬНА ІНФОРМАЦІЯ ПРО ОСВІТНІЙ КОМПОНЕНТ

1.	Назва ОК	Управління кібербезпекою			
2.	Факультет/кафедра	Факультет економіки та менеджменту / Кафедра кібернетики та інформатики			
3.	Статус ОК	Обов'язковий			
4.	Програма/Спеціальність (програми), складовою яких є ОК *(заповнюється для обов'язкових ОК)*	ОП - Інформаційні системи та технології Спеціальність – 126 «Інформаційні системи та технології»			
5.	ОК може бути запропонований для *(заповнюється для вибіркових ОК)*				
6.	Семестр та тривалість вивчення	Дисципліна викладається протягом 1 навчального року в 1-му семестрі			
7.	Кількість кредитів ЄКТС	5 кредитів (150 годин)			
8.	Загальний обсяг годин та їх розподіл	Контактна робота(заняття)			Самостійна робота
		Лекційні	Практичні /семінарські	Лабораторні	
	І семестр	30	30	–	90
9.	Мова навчання	українська			
10.	Викладач / Координатор освітнього компонента	Доцент кафедри кібернетики та інформатики, кандидат економічних наук (PhD) В'юненко Олександр Борисович			
11.1	Контактна інформація	oleksandr.viunenko@snau.edu.ua; ауд. 308е			
11.	Загальний опис освітнього компонента	Дисципліна «Управління кібербезпекою» охоплює теоретичні та практичні аспекти забезпечення безпеки інформаційних систем, управління ризиками та протидії кіберзагрозам у сучасному цифровому середовищі. У рамках курсу розглядаються ключові принципи кіберзахисту, архітектура систем безпеки, моделі управління ризиками, а також сучасні методи і технології – від етичного хакінгу та цифрової криміналістики до аналізу шкідливого ПЗ, забезпечення безпеки web-додатків, мобільних і хмарних сервісів. Особлива увага приділяється міжнародним стандартам та практикам (ISO/IEC 27001, NIST, CIS), принципам Zero Trust, управлінню інцидентами й безперервністю бізнесу, а також використанню штучного інтелекту і машинного навчання для виявлення та запобігання кібератакам. Курс знайомить здобувачів з інструментами SOC/SIEM, методами аудитів і тестувань на проникнення, а також розробкою політик і стратегій кіберзахисту. Академічне значення дисципліни полягає в інтеграції знань із різних галузей ІТ, професійне – у формуванні компетентностей для ефективного управління інформаційною безпекою, а особистісне – у розвитку відповідального ставлення до захисту даних і цифрової стійкості. Таким чином, дисципліна сприяє формуванню професійних компетентностей, необхідних для ефективного управління інформаційною безпекою та забезпечення стійкості організацій до сучасних кіберзагроз..			
12.	Мета освітнього компонента	Метою вивчення дисципліни є досягнення здобувачами сучасного конструктивного, фундаментального мислення та комплексу спеціальних знань щодо аналізу, проєктування, впровадження та удосконалення систем кібербезпеки в сучасних інформаційних системах і технологіях, сприяння формуванню здатності розв'язувати задачі дослідницького та інноваційного характеру у сфері управління кіберризиками, забезпечення захисту інформації, виявлення, реагування та запобігання кіберзагрозам шляхом використання сучасних методів, стандартів і засобів інформаційної безпеки.			

13.	Передумови вивчення ОК, зв'язок з іншими освітніми компонентами ОП	1. Передумови відсутні 2. Освітній компонент є основою для: ОК 9 ІТ інфраструктура ОК11 «Фахове стажування та переддипломна практика»
14.	Політика академічної доброчесності	При виконання практичних робіт та при написання проміжних контрольних та атестаційних робіт здобувач вищої освіти обов'язково має дотримуватись правил академічної доброчесності. При виявленні фактів списування або академічної не доброчесності робота виконана здобувачем вищої освіти робота анулюється.
15.	Посилання на курс у Moodle	https://cdn.snau.edu.ua/moodle/course/view.php?id=6047

2. РЕЗУЛЬТАТИ НАВЧАННЯ ЗА ОСВІТНІМ КОМПОНЕНТОМ ТА ЇХ ЗВ'ЯЗОК З ПРОГРАМНИМИ РЕЗУЛЬТАТАМИ НАВЧАННЯ

Результати навчання за ОК: Після вивчення освітнього компонента здобувач вищої освіти очікувано буде здатен…»	Програмні результати навчання, на досягнення яких спрямований ОК (зазначити номер згідно з нумерацією, наведеною в ОП) **РН10** Здатність забезпечувати якісний кіберзахист ІСТ, планувати, організовувати, впроваджувати та контролювати функціонування систем захисту інформації.	Як оцінюється ДРН
ДРН 1 Аналізувати сучасні кіберзагрози та архітектури захисту інформаційних систем, порівнювати міжнародні моделі та фреймворки та розробляти фрагменти планів реагування і забезпечення безперервності бізнесу.	×	Звіт за результатами виконання практичних робіт №1 та №2 Проміжний контроль №1: тести множинного вибору
ДРН 2 Застосовувати методи цифрової криміналістики для вилучення та аналізу цифрових доказів, забезпечувати ланцюг їх збереження відповідно до міжнародних стандартів та формувати криміналістичні звіти за результатами розслідування інцидентів.	×	Звіт за результатами виконання практичної роботи №3 та №4 Проміжний контроль№1: тести множинного вибору
ДРН 3 Здійснювати етичне тестування на проникнення, використовувати сучасні інструменти та методології (OWASP, PTES, NIST SP 800-115) для виявлення вразливостей і пропонувати обґрунтовані заходи їх усунення.	×	Звіт за результатами виконання практичної роботи №5 Проміжний контроль №1: тести множинного вибору
ДРН 4 Застосовувати методи статичного та динамічного аналізу для дослідження шкідливого програмного забезпечення, класифікувати зразки ПЗ за життєвим циклом і робити висновки щодо заходів протидії кіберінцидентам.	×	Звіт за результатами виконання практичної роботи №6 Проміжний контроль №1: тести множинного вибору
ДРН 5 Оцінювати захищеність веб-додатків, бездротових мереж та мобільних пристроїв, виявляти типові загрози (OWASP Top 10, WPA2) і застосовувати практики підвищення безпеки (WAF, MFA, BYOD-контроль).	×	Звіт за результатами виконання практичної роботи №7-8 Проміжний контроль №1-2: тести множинного вибору

ДРН 6 аналізувати архітектури та ризики хмарних технологій (IaaS, PaaS, SaaS), впроваджувати засоби захисту даних (шифрування, токенізація) та застосовувати принципи Zero Trust у хмарному середовищі.	×	Звіт за результатами виконання практичних робіт №9-10 Проміжний контроль №2: тести множинного вибору Підсумковий контроль: іспит
ДРН 7 Розробляти безпечне програмне забезпечення із застосуванням Secure SDLC та Threat Modeling, виконувати статичний і динамічний аналіз коду, а також формувати запити й кореляційні правила для виявлення інцидентів у SOC/SIEM.	×	Звіт за результатами виконання практичної роботи №11-12 Проміжний контроль №2: тести множинного вибору
ДРН 8 Моделювати архітектуру Zero Trust із використанням мікросегментації, MFA та IAM, застосовувати методи машинного навчання для виявлення аномалій, а також аргументовано презентувати результати аудитів та кейсів із урахуванням професійної етики й стандартів.	×	Звіт за результатами виконання практичної роботи №13-14 Проміжний контроль №2: тести множинного вибору

3. ЗМІСТ ОСВІТНЬОГО КОМПОНЕНТА (ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ)

Тема. Перелік питань, що будуть розглянуті в межах теми	Розподіл в межах загального бюджету часу				Рекомендована література
	Аудиторна робота			Самостійна робота	
	Лекції	Практ. з. / семін. з.	Лаб. з.		
Тема 1. Вступ до управління кібербезпекою. Архітектура безпеки сучасних інформаційних систем та технологій 1.1. Кіберзагрози XXI століття 1.2. Основи управління кіберризиками 1.3. Стандарти, нормативи та моделі захисту (ISO/IEC 27001, NIST, CIS)	2	2	–	6	1, 14, 16, 17, 18, 65, 70, 89
Тема 2. Організація системи кіберзахисту в іст: політики, плани та процедури 2.1. Стратегія забезпечення безпеки 2.2. Планування заходів реагування та неперервності бізнесу 2.3. Ролі та відповідальність персоналу	2	2	–	6	1, 15, 17, 18, 26, 27, 31, 55
Тема 3. Цифрова криміналістика (Частина 1): принципи та інструменти 3.1. Методологія цифрових розслідувань 3.2. Ланцюг збереження доказів 3.3. Інструменти цифрової криміналістики	2	2	–	6	1, 7, 11, 17, 18, 38, 41, 44, 47, 82, 98
Тема 4. Цифрова криміналістика (Частина 2): практичні кейси та аналіз інцидентів 4.1. Аналіз файлових систем та логів 4.2. Розбір атак типу APT, Insider Threat 4.3. Створення криміналістичних звітів	2	2	–	6	1, 3, 8, 17, 18, 53, 54, 59, 61, 67, 78, 95
Тема 5. Етичний хакінг та тестування на проникнення 5.1. Різновиди хакерів та правова база 5.2. Методології тестування (OWASP, PTES, NIST SP 800-115)	2	2	–	6	1, 4, 17, 18, 57, 63, 66, 85, 86, 87

5.3. Практика використання Metasploit, Burp Suite					
Тема 6. Аналіз шкідливого програмного забезпечення 6.1. Класифікація та життєвий цикл шкідливого ПЗ 6.2. Статичний та динамічний аналіз 6.3. Інструменти: IDA Pro, Ghidra, Cuckoo Sandbox	2	2	–	6	1, 2, 6, 17, 18, 60, 71, 76, 84
Тема 7. Безпека web-додатків: атаки та захист 7.1. Загрози OWASP Top 10 7.2. Захист автентифікації, сесій, введення даних 7.3. Розгортання WAF, HTTPS, CSP	2	2	–	6	1, 17, 18,24, 42, 58, 63, 90, 91
Тема 8. Безпека бездротових мереж та мобільних пристроїв 8.1. Протоколи бездротової передачі (Wi-Fi, Bluetooth) 8.2. Методи атак: Evil Twin, Packet Sniffing 8.3. Захист BYOD-середовищ	2	2	–	6	1, 17, 18,51, 52, 62, 68, 69, 100
Тема 9. Безпека хмарних технологій (Частина 1): моделі та ризики 9.1. Хмарні архітектури (IaaS, PaaS, SaaS) 9.2. Ризики багатокористувацького середовища 9.3. Відповідальність CSP та користувача	2	2	–	6	1, 17, 18,19, 56, 64, 72, 74, 80
Тема 10. безпека хмарних технологій (Частина 2): практичні аспекти 10.1. Захист даних у хмарі (шифрування, токенізація) 10.2. Контейнери, Kubernetes, DevSecOps 10.3. Розгортання Zero Trust у хмарі	2	2	–	6	1, 17, 18, 20, 34, 37, 73, 75, 81, 83
Тема 11. Розробка безпечного програмного забезпечення 11.1. Secure SDLC, Threat Modeling 11.2. Аналіз вихідного коду, статичне/динамічне тестування 11.3. Інструменти: SonarQube, Checkmarx	2	2	–	6	1, 10, 12, 17, 18, 46, 63, 77, 99
Тема 12. Інструменти моніторингу, SIEM, та управління подіями безпеки 12.1. Архітектура та функції SOC 12.2. Логи, кореляція, реагування на інциденти 12.3. Популярні SIEM-рішення: Splunk, ELK, IBM QRadar	2	2	–	6	1, 17, 18, 29, 33, 40, 43, 45, 79, 92, 96, 97
Тема 13. Zero Trust архітектура: сучасна парадигма захисту 13.1. Принципи Zero Trust 13.2. Мікросегментація, MFA, IAM 13.3. Роль у побудові адаптивної безпеки	2	2	–	6	1, 17, 18, 23, 28, 30, 39, 65
Тема 14. Штучний інтелект і машинне навчання в управлінні кіберзагрозами 14.1. Виявлення аномалій, поведінковий аналіз 14.2. Використання штучного інтелекту для прогнозування атак 14.3. Ризики: Adversarial ML, Bias in models	2	2	–	6	1, 5, 9, 13, 17, 18, 28, 48, 50, 54, 88, 93, 94, 95, 100

Тема 15. Комплексне управління кібербезпекою в іст: кейси, аудит, сертифікація 15.1. Аудит та перевірка безпеки 15.2. Кейс-стаді: атака на SolarWinds, Uber, Colonial Pipeline 15.3. Сертифікація фахівців: CISSP, CISM, CEH	2	2	–	6	1, 17, 18, 21, 22, 25, 32, 35, 36, 49
Всього годин	**30**	**30**	**0**	**90**	

4. МЕТОДИ ВИКЛАДАННЯ ТА НАВЧАННЯ

ДРН	**Методи викладання** (робота, що буде проведена викладачем під час аудиторних занять, консультацій)	**Кількість годин**	**Методи навчання** (які види навчальної діяльності має виконати студент самостійно)	**Кількість годин**
ДРН 1 Аналізувати сучасні кіберзагрози та архітектури захисту інформаційних систем, порівнювати міжнародні моделі та фреймворки та розробляти фрагменти планів реагування і забезпечення безперервності бізнесу.	- проведення лекційних та практичних занять з мультимедійними презентаціями, - практикоорієнтоване навчання шляхом колективного розбору архітектурних моделей безпеки (TOGAF, SABSA, NIST) та симуляції сценаріїв реагування на інциденти.	4	- додаткове опрацювання лекційного матеріалу; - підготовка до захисту звітів практичних робіт; - самостійне вивчення теоретичних підходів до моделювання архітектур безпеки: TOGAF, SABSA, NIST та порівняння фреймворків реагування на інциденти: NIST CSF, ISO 27035, SANS	12
ДРН 2 Застосовувати методи цифрової криміналістики для вилучення та аналізу цифрових доказів, забезпечувати ланцюг їх збереження відповідно до міжнародних стандартів та формувати криміналістичні звіти за результатами розслідування інцидентів.	- проведення лекційних та практичних занять з мультимедійними презентаціями, - практикоорієнтоване навчання шляхом відпрацювання прийомів вилучення цифрових доказів, аналізу логів та створення криміналістичних звітів.	4	- додаткове опрацювання лекційного матеріалу; - підготовка до захисту звітів практичних робіт; - самостійне вивчення міжнародних стандартів цифрової криміналістики та електронних доказів, методів аналізу файлових систем, реєстру та артефактів ОС у цифровій криміналістиці	12
ДРН 3 Здійснювати етичне тестування на проникнення, використовувати сучасні інструменти та методології (OWASP, PTES, NIST SP 800-115) для виявлення вразливостей і пропонувати обґрунтовані заходи їх усунення.	- проведення лекційних та практичних занять з мультимедійними презентаціями, - практикоорієнтоване навчання шляхом застосування методологій тестування (OWASP, PTES, NIST SP 800-115) у симуляції пентесту	2	- додаткове опрацювання лекційного матеріалу; - підготовка до захисту звітів практичних робіт; - самостійне вивчення питання методів управління вразливостями та практик етичного тестування на проникнення.	6
ДРН 4 Застосовувати методи статичного та динамічного аналізу для дослідження шкідливого програмного забезпечення, класифікувати зразки ПЗ	- проведення лекційних та практичних занять з мультимедійними презентаціями, - практикоорієнтоване навчання шляхом виконання завдань зі	2	- додаткове опрацювання лекційного матеріалу; - підготовка до захисту звітів практичних робіт; - самостійне вивчення особливостей реагування на різні типи	6

за життєвим циклом і робити висновки щодо заходів протидії кіберінцидентам.	статичного й динамічного аналізу шкідливого ПЗ (IDA Pro, Ghidra, Cuckoo Sandbox)		кіберінцидентів: шкідливе ПЗ, фішинг, DDoS-атаки	
ДРН 5 Оцінювати захищеність веб-додатків, бездротових мереж та мобільних пристроїв, виявляти типові загрози (OWASP Top 10, WPA2) і застосовувати практики підвищення безпеки (WAF, MFA, BYOD-контроль).	- проведення лекційних та практичних занять з мультимедійними презентаціями, - практикоорієнтоване навчання шляхом аналізу безпеки веб-додатків і Wi-Fi-мереж, відпрацювання захисту автентифікації, сесій та BYOD-середовища.	4	- додаткове опрацювання лекційного матеріалу; - підготовка до захисту звітів практичних робіт; - самостійне вивчення питання типових атак на web і бездротові мережі та способів їхнього нейтралізування	12
ДРН 6 аналізувати архітектури та ризики хмарних технологій (IaaS, PaaS, SaaS), впроваджувати засоби захисту даних (шифрування, токенізація) та застосовувати принципи Zero Trust у хмарному середовищі.	- проведення лекційних та практичних занять з мультимедійними презентаціями, - практикоорієнтоване навчання шляхом моделювання архітектур хмарних сервісів (IaaS, PaaS, SaaS), впровадження шифрування та Zero Trust у віртуальних середовищах.	4	- додаткове опрацювання лекційного матеріалу; - підготовка до захисту звітів практичних робіт; - самостійне вивчення питання ризиків хмарних технологій і сучасних практик захисту даних.	12
ДРН 7 Розробляти безпечне програмне забезпечення із застосуванням Secure SDLC та Threat Modeling, виконувати статичний і динамічний аналіз коду, а також формувати запити й кореляційні правила для виявлення інцидентів у SOC/SIEM.	- проведення лекційних та практичних занять з мультимедійними презентаціями, - практикоорієнтоване навчання шляхом аналізу вихідного коду з використанням статичних/динамічних інструментів і створення кореляційних правил у SIEM.	4	- додаткове опрацювання лекційного матеріалу; - підготовка до захисту звітів практичних робіт; - самостійне вивчення питання питання безпечного SDLC та принципів функціонування SOC.	12
ДРН 8 Моделювати архітектуру Zero Trust із використанням мікросегментації, MFA та IAM, застосовувати методи машинного навчання для виявлення аномалій, а також аргументовано презентувати результати аудитів та кейсів із урахуванням професійної етики й стандартів.	- проведення лекційних та практичних занять з мультимедійними презентаціями, - практикоорієнтоване навчання шляхом моделювання Zero Trust-архітектури, використання ML для виявлення аномалій і підготовки міні-аудитів.	6	- додаткове опрацювання лекційного матеріалу; - підготовка до захисту звітів практичних робіт; - самостійне вивчення питання питання застосування ML/AI у кібербезпеці, законодавчих і етичних аспектів кіберзахисту	18
	Всього:	**30**		**90**

5. ОЦІНЮВАННЯ ЗА ОСВІТНІМ КОМПОНЕНТОМ

5.1. Сумативне оцінювання

5.1.1 Для оцінювання очікуваних результатів навчання передбачено

№	Методи сумативного оцінювання	Бали / Вага у загальній оцінці	Дата складання
Осінній семестр			
1.	Практична робота 1. Модель архітектури кібербезпеки організації	4 бали / 4%	До 7 тижня
2.	Практична робота 2. Розробка фрагмента плану реагування на інциденти	4 бали / 4%	До 7 тижня
3.	Практична робота 3. Вилучення та аналіз цифрових доказів з образу диска	4 бали / 4%	До 7 тижня
4.	Практична робота 4. Криміналістичний звіт на основі логів	4 бали / 4%	До 7 тижня
5.	Практична робота 5. Пентест тестового сервера: сканування і експлуатація вразливостей	4 бали / 4%	До 7 тижня
6.	Практична робота 6. Динамічний аналіз шкідливого ПЗ	4 бали / 4%	До 7 тижня
7.	Практична робота 7. Аудит аутентифікації/сесій у веб-додатку	4 бали / 4%	До 7 тижня
8.	Проміжний контроль №1 (Тести множинного вибору)	22 балів / 22%	До 7 тижня
9.	Практична робота 8. Аналіз WPA2-мережі: виявлення та виправлення конфігураційних проблем	4 бали / 4%	До 15 тижня
10.	Практична робота 9. Аудит політик керування ідентифікацією та доступом у хмарному середовищі	4 бали / 4%	До 15 тижня
11.	Практична робота 10. Розгортання шифрування даних у хмарному середовищі	4 бали / 4%	До 15 тижня
12.	Практична робота 11. Аналіз вихідного коду та виправлення вразливостей	4 бали / 4%	До 15 тижня
13.	Практична робота 12. Формування запиту для виявлення інциденту	4 бали / 4%	До 15 тижня
14.	Практична робота 13. Моделювання мікросегментації з багатофакторною автентифікацією та керування ідентифікацією та доступом	4 бали / 4%	До 15 тижня
15.	Практична робота 14. Виявлення аномалій у журналі подій за допомогою простої моделі машинного навчання	4 бали / 4%	До 15 тижня
16.	Практична робота 15. Проведення міні-аудиту інформаційної системи	4 бали / 4%	До 15 тижня
17.	Проміжний контроль №2 (Тести множинного вибору)	18 балів / 18%	До 15 тижня

5.1.2 Критерії оцінювання

Компонент	Незадовільно	Задовільно	Добре	Відмінно
Весняний семестр				
Практична робота 1. Модель архітектури кібербезпеки організації	≤1 балу	2 бали	3 бали	4 бали
	Модель не містить основних компонентів системи або побудована з суттєвими логічними помилками. Загрози описані поверхово або відсутні.	Побудовано базову модель, яка охоплює основні компоненти системи, але не всі взаємозв'язки відображені. Загрози описані частково, з неточностями	Модель загалом відображає архітектуру системи, присутні межі довіри, основні загрози класифіковані за STRIDE, є загальні рекомендації.	Модель повністю охоплює всі ключові компоненти системи, чітко ідентифіковані загрози та обґрунтовані заходи захисту. Результати оформлені структуровано, логічно та з використанням рекомендованих інструментів.
Практична робота 2. Розробка фрагмента плану реагування на інциденти	≤1 балу	2 бали	3 бали	4 бали
	Завдання виконано формально або з грубими помилками. Відсутня логіка реагування, не враховано ролі або етапи інциденту. Звіт має фрагментарний або невпорядкований характер. Джерела не використані або відсутні. Можлива наявність плагіату.	Завдання виконано частково. Опис фрагмента плану неповний, бракує важливих елементів (наприклад, конкретних дій або послідовності). Відсутні висновки або вони не відображають рефлексії. Недостатнє обґрунтування вибраного інциденту. Порушено вимоги до структури або формату.	Завдання виконано в основному правильно. План реагування надано, проте окремі компоненти (наприклад, класифікація інциденту чи ролі) подано нечітко або спрощено. Візуалізація або висновки можуть бути поверховими. Незначні недоліки в оформленні або логіці.	Завдання виконано повністю та грамотно. Фрагмент плану реагування структурований, усі етапи інцидент-менеджменту враховано. Чітко визначені ролі та відповідальність, застосовано приклад/сценарій. Оформлення звіту відповідає вимогам, наведено власні висновки, джерела актуальні та релевантні.
Практична робота 3. Вилучення та аналіз цифрових доказів з образу диска	≤1 балу	2 бали	3 бали	4 бали
	Мінімальне виконання завдань, немає аналітики, звіт формальний або не містить доказів практичного виконання.	Завдання виконано частково. Відсутні ключові компоненти (наприклад, аналіз одного з об'єктів), поверхневі висновки.	Виконано основну частину завдань. Присутні незначні неточності у висновках або оформленні, однак аналіз проведено на прийнятному рівні.	Повноцінно виконані всі завдання. Детально задокументований аналіз, надані обґрунтовані висновки, якісні скриншоти, правильне використання інструментів.

Практична робота 4. Криміналістичний звіт на основі логів	≤1 балу	2 бали	3 бали	4 бали
	Звіт фрагментарний; виявлено 1-2 події без пояснення значення; структура не дотримана.	Проведено базовий аналіз логів; часткова реконструкція подій; присутні помилки у висновках або структура неповна.	Виявлено ключові інциденти; звіт логічно структурований, надано докази та висновки, але є дрібні неточності.	Повний, послідовний звіт із доказами, обґрунтованим сценарієм атаки, чіткими висновками та рекомендаціями; дотримано академічної мови.
Практична робота 5. Пентест тестового сервера: сканування і експлуатація вразливостей	≤1 балу	2 бали	3 бали	4 бали
	Мінімальний аналіз, лише перелік відкритих портів. Вразливості не описано. Звіт фрагментарний.	Виявлено вразливості, але немає підтвердження або аналіз поверхневий. Модель атаки відсутня.	Виявлено й частково змодельовано експлуатацію. Звіт містить скріншоти, базовий аналіз наслідків.	Повна реалізація: сканування, перевірка, експлуатація (етична), висновки й рекомендації. Добре структурований звіт із доказами.
Практична робота 6. Динамічний аналіз шкідливого ПЗ	≤1 балу	2 бали	3 бали	4 бали
	Підготовлено середовище, аналіз поверхневий або відсутній. Звіт формальний.	Здійснено запуск і моніторинг, але з частковим описом дій. IoC не виділено.	Докладно описано основні артефакти поведінки, присутні лог-файли, базовий аналіз IoC..	Повний звіт з демонстрацією активності, аналізом шкідливих дій, IoC, сценарієм атаки. Є рекомендації з реагування.
Практична робота 7. Аудит аутентифікації/ сесій у веб-додатку	≤1 балу	2 бали	3 бали	4 бали
	Проведено загальну перевірку, частково описано механізм автентифікації. Вразливості не підтверджені..	Виявлено принаймні 1 типову вразливість, без детального аналізу або доказів..	Проведено системний аудит, знайдено декілька вразливостей, запропоновано базові рекомендації.	Повний аналіз: виявлено вразливості з прикладами, зроблено технічні рекомендації, надано скріни, лог-файли.
Проміжний контроль №1 (Тести множинного вибору)	≤10 балів	11-15 бали	16-19 балів	20-22 балів
	Кількість правильних відповідей на тест, k_v: k_v <=5	Кількість правильних відповідей на тест, k_v: $6 \le k_v \le 8$.	Кількість правильних відповідей на тест, k_v: $8 \le k_v \le 9$	Кількість правильних відповідей на тест, k_v: $k_v \ge 10$
Практична робота 8. Аналіз WPA2-мережі: виявлення та виправлення конфігураційних проблем	≤1 балу	2 бали	3 бали	4 бали
	Виконано базовий збір даних, без детального аналізу; загальні висновки.	Виявлено 1–2 типові проблеми конфігурації, без аналізу впливу.	Проведено аналіз з використанням утиліт, описано декілька проблем, подано пропозиції..	Повний технічний аудит з прикладами конфігураційних помилок, доказами (скріншоти/логи), чіткими рекомендаціями.
Практична робота 9. Аудит політик керування ідентифікацією та доступом у хмарному середовищі	≤1 балу	2 бали	3 бали	4 бали
	Визначено базову структуру доступу, без глибокого аналізу політик.	Виявлено 1–2 критичні проблеми доступу, без пропозицій щодо їх вирішення.	Проведено аналіз, запропоновано раціональні заходи з обмеження доступу.	Повноцінний аудит з прикладами, технічними обґрунтуваннями і рекомендаціями з урахуванням принципу Least Privilege.

Практична робота 10. Розгортання шифрування даних у хмарному середовищі	≤1 балу	2 бали	3 бали	4 бали
	Поверхневе ознайомлення з сервісом шифрування без практичної реалізації..	Виконане базове шифрування, але відсутні перевірки доступу або життєвого циклу ключів.	Реалізовано шифрування з урахуванням налаштувань доступу до ключів, часткова верифікація.	Повноцінна реалізація з тестуванням, аудитом, аналізом життєвого циклу ключів і документованими результатами.
Практична робота 11. Аналіз вихідного коду та виправлення вразливостей	≤1 балу	2 бали	3 бали	4 бали
	Аналіз поверхневий, виправлення часткові або відсутні.	Ідентифіковано частину вразливостей, деякі з них виправлено.	Виявлено основні вразливості, коректно виправлено, але без глибокого обґрунтування.	Повний аналіз, усі вразливості ідентифіковано та виправлено з якісним обґрунтуванням і тестуванням.
Практична робота 12. Формування запиту для виявлення інциденту	≤1 балу	2 бали	3 бали	4 бали
	Запит складено частково або некоректно, інтерпретація поверхнева	Сформовано запит і частково обґрунтовано очікуваний результат.	Запит коректний, інтерпретація результату присутня, але без деталізації.	Запит точний, логічно вмотивований, результат інтерпретовано з безпекової точки зору.
Практична робота 13. Моделювання мікросегментації з багатофакторною автентифікацією та керування ідентифікацією та доступом	≤1 балу	2 бали	3 бали	4 бали
	Побудовано схему без деталізації доступів або IAM/MFA. Сценарій не опрацьовано.	Діаграма присутня, частково описані політики. MFA/IAM згадані, але не реалізовані.	Повноцінне моделювання з основними правилами доступу. Сценарій реалізований частково	Діаграма, політики та сценарій чітко обґрунтовані й відповідають принципам Zero Trust.
Практична робота 14. Виявлення аномалій у журналі подій за допомогою простої моделі машинного навчання	≤1 балу	2 бали	3 бали	4 бали
	Завантажено лог, без попередньої обробки, модель не реалізовано або дає некоректний результат.	Дані оброблено, використано базовий підхід до виявлення аномалій, але немає пояснення результатів.	Побудовано модель, надано інтерпретацію виявлених аномалій, часткова візуалізація.	Реалізовано повний цикл: обробка, модель, аналіз результатів, рекомендації з безпеки.
Практична робота 15. Проведення міні-аудиту інформаційної системи	≤1 балу	2 бали	3 бали	4 бали
	Мінімальний аналіз, звіт має фрагментарний характер, недоліки описані поверхнево, рекомендації не обґрунтовано або відсутні.	Проведено базовий аудит, виявлено кілька ключових недоліків, але аналіз неповний або рекомендації мають обмежену практичну цінність.	Аудит виконано систематично: зібрана основна інформація, виявлено ключові ризики, рекомендації відповідно до стандартів, звіт структурований.	Повний аудит з глибоким аналізом, всі етапи виконані, виявлено широкий спектр ризиків, обґрунтовано та детально сформульовано рекомендації, звіт оформлено відповідно до академічних вимог

Проміжний контроль №2 (Тести множинного вибору)	≤9 балів	10-13 бали	14-16 балів	17-18 балів
	Кількість правильних відповідей на тест, k_v: k_v <=5	Кількість правильних відповідей на тест, k_v: $6 \le k_v \le 8$.	Кількість правильних відповідей на тест, k_v: $8 \le k_v \le 9$	Кількість правильних відповідей на тест, k_v: $k_v \ge 10$

5.2. Формативне оцінювання:

№	Елементи формативного оцінювання	Дата
1	Усне опитування після вивчення кожної теми	Після завершення вивчення теми
2	Проходження тестування з атестації та проміжного контролю зі зворотнім зв’язком з викладачем	Відповідно до графіку навчального процесу
3	Проходження тестування після закінчення вивчення кожної теми для самостійного контролю знань та підготовки до складання заліку (іспиту)	Регулюється здобувачем вищої освіти самостійно
4	Захист практичних робіт	Через тиждень після їх здачі
5	Усний зворотний зв'язок від викладача під час роботи над практичними роботами протягом занять	Протягом всього семестру

6. НАВЧАЛЬНІ РЕСУРСИ (ЛІТЕРАТУРА)

6.1. Основні джерела

6.1.1. Підручники посібники

1. Управління кібербезпекою: конспект лекцій / укл.: І. В. Шелехов. - Суми, 2025 – 210 с.
2. Blunden, B. (2022). The Rootkit Arsenal: Escape and Evasion in the Modern Malware Landscape (3rd ed.). Jones & Bartlett Learning.
3. Chuvakin, A., & Schmidt, K. (2020). Designing and Deploying SIEM Solutions.
4. Cyber Security Basics for Dummies. – Wiley, 2020.
5. Hajdarbashi, A., & Kourtesis, D. (2023). Applied Machine Learning in Cybersecurity: Detecting Malicious Network Behavior. Packt Publishing.
6. Kleymenov, A., Thabet, A. (2022). Mastering Malware Analysis: A malware analyst's practical guide to combating malicious software, APT, cybercrime, and IoT attacks. Packt Publishing. – 572 p.
7. Lee, M. (2021). Learning Windows Forensic Analysis. Packt Publishing.
8. Mandia, K., Prosise, C., & Alperovitch, D. (2022). Incident Response & Computer Forensics (3rd Edition). McGraw-Hill Education.
9. Mathew, E. A. (2020). Cybersecurity Data Science: Best Practices in Data Collection, Processing, and Analysis. Apress
10. Meyers, A., & Spadaro, J. (2020). Secure Software Development: A Guide to Building Secure Systems. Apress.
11. Russinovich, M., Solomon, D., & Ionescu, A. (2020). Windows Internals, Part 2. Microsoft Press.

12. Secure Coding in C and C++. – Addison-Wesley, 2021.
13. Srivastava, G., & Kumar, R. (Eds.). (2020). Machine Learning for Cyber Security: Principles, Algorithms, and Practices. CRC Press.
14. Tarandach. I., Coles M. J. Threat Modeling: A Practical Guide for Development Teams. O'Reilly Media, 2020. – 244 p.
15. Whitman M. E., Mattord H.J. Principles of Incident Response & Disaster Recovery (MindTap Course List). Cengage Learning, 2021. – 624 P.
16. Wong A.Y., Chekole E.G., Ochoa M., Zhou J. Threat Modeling and Security Analysis of Containers: A Survey. – https://arxiv.org/abs/2111.11475

6.1.2. Методичне забезпечення

17. Управління кібербезпекою: Методичні вказівки щодо самостійних робіт для здобувачів вищої освіти за освітньо-професійною програмою «Інформаційні системи та технології» спеціальності F6 «Інформаційні системи і технології» другого (магістерського) рівня вищої освіти всіх форм навчання / укл.: І. В. Шелехов. - Суми, 2025 – 168 с.
18. Управління кібербезпекою: Методичні вказівки щодо проведення практичних занять для здобувачів вищої освіти за освітньо-професійною програмою «Інформаційні системи та технології» спеціальності F6 «Інформаційні системи і технології» другого (магістерського) рівня вищої освіти всіх форм навчання / укл.: І. В. Шелехов. - Суми, 2025 – 65 с
19. CIS Controls v8 – https://www.cisecurity.org/controls/
20. CSA Cloud Controls Matrix (CCM) – https://cloudsecurityalliance.org
21. CISA. (2022). Cyber Security Evaluation Tool (CSET). CISA. https://www.cisa.gov/cset
22. Center for Internet Security (CIS). (2023). The CIS Critical Security Controls for Effective Cyber Defense, Version 8. CIS. https://www.cisecurity.org/controls/v8
23. Forrester. No More Chewy Centers: Introducing The Zero Trust Model Of Information Security. https://www.forrester.com/report/No-More-Chewy-Centers-Introducing-The-Zero-Trust-Model-Of-Information-Security/RES49277
24. ISO/IEC 27034-1:2011. Information technology – Security techniques – Application security. Part 1: Overview and concepts.
25. ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems.
26. ISO/IEC 27035-1:2016. Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management. Geneva: ISO, 2016.
27. Killcrece, G., Kossakowski, K. P., Ruefle, R., Zajicek, M. State of the Practice of Computer Security Incident Response Teams (CSIRTs). CERT Coordination Center, Carnegie Mellon University, 2003. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6365
28. MITRE ATTACK. https://attack.mitre.org
29. MITRE ATTACK Framework. – https://attack.mitre.org/
30. National Institute of Standards and Technology (NIST). (2020). NIST Special Publication 800-207: Zero Trust Architecture. NIST. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800...
31. National Institute of Standards and Technology (NIST). Computer Security Incident Handling Guide (NIST SP 800-61 Rev. 2). Gaithersburg, MD: NIST, 2012. https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
32. NIST. (2014). Cybersecurity Framework. NIST. https://www.nist.gov/cybersecurity
33. NIST SP 800-92: Guide to Computer Security Log Management.
34. NIST SP 800-57 – Recommendation for Key Management

35. NIST Special Publication 800-30, Revision 1: Guide for Conducting Risk Assessments.
36. OWASP. (2023). OWASP Application Security Verification Standard (ASVS) 4.0.3. OWASP. https://owasp.org/www-project-application-security-verification-standard/
37. OWASP: Cloud Security Guidelines

6.1.3. Інші джерела

38. Carrier, B. (2015). The Sleuth Kit (Autopsy) Documentation. https://www.sleuthkit.org
39. Cisco. Zero Trust Security. https://www.cisco.com/c/en/us/products/security/zero-trust.html
40. Cybersecurity Frameworks: A Guide to NIST and ISO 27001. https://www.techtarget.com/
41. Digital Corpora. https://digitalcorpora.org/
42. Google Security Research. – https://security.googleblog.com
43. IBM: What is a SIEM? – https://www.ibm.com/topics/siem
44. SANS Institute. Digital Forensics and Incident Response Courseware. https://www.sans.org/cyber-security-courses/digital-forensics-and-incident-response/
45. SANS Institute: Log Analysis. – https://www.sans.org/cyber-security-courses/log-analysis-monitoring/
46. SANS Institute: Secure Coding. – https://www.sans.org/secure-coding/
47. Zimmerman, E. (2017). The Registry File Format. https://www.digitalforensicscience.com

6.2. Додаткові джерела

48. Shelechov I. Information and Analytical System for Assessing the Compliance of Educational Content Specialties Cyber Security With Modern Requirements / A. Dovbysh, I. Shelechov, J. Khibovska, O. Matiash // Radioelectronic and Computer Systems, 2021. - № 1(97). - P. 70–80. - DOI: 10.32620/reks.2021.1.06
49. Shelehov I. Information-extreme machine learning of a cyber attack detection system / A. Dovbysh, V. Liubchak, I. Shelehov, J. Simonovskiy, A. Tenytska // Radioelectronic and Computer Systems, 2022. - № 2022(3). - pp. 121–131. - doi: 10.32620/reks.2022.3.09
50. Шелехов І. В. Нечітка ієрархічна оцінка якості комплексних систем захисту інформації / І. В. Шелехов [та ін.] // Radioelectronic and computer systems. – 2020. – № 4. – С. 106–115. – DOI: 10.32620/reks.2020.4.10
51. Aircrack-ng documentation – https://aircrack-ng.org/documentation.html
52. Cisco Wireless LAN Security White Paper – https://www.cisco.com/
53. CTFTime.org: https://ctftime.org/
54. Digital Corpora. – https://digitalcorpora.org/
55. ENISA – European Union Agency for Cybersecurity. Reference Incident Classification Taxonomy 2021. https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy
56. Gartner: Identity and Access Management. – https://www.gartner.com/en/information-technology/glossary/identity-and-access-management-iam
57. Hack The Box. – https://www.hackthebox.com
58. Hacking APIs. – https://www.hackingapis.com
59. Журнал подій Windows: https://learn.microsoft.com/uk-ua/windows/security/threat-protection/auditing/basic-security-audit-policy-settings
60. Malware Traffic Analysis – https://www.malware-traffic-analysis.net/
61. OWASP Logging Cheat Sheet. – https://cheatsheetseries.owasp.org/cheatsheets/Logging_Cheat_Sheet.html
62. OWASP Mobile Security Testing Guide, розділ Network Communication.
63. OWASP Top 10. – https://owasp.org/www-project-top-ten/

64. OWASP Top 10 for Serverless Applications. – https://owasp.org/www-project-serverless-security-top-10/
65. Palo Alto Networks. Zero Trust: A Cybersecurity Model. https://www.paloaltonetworks.com/cyberpedia/what-is-zero-trust
66. TryHackMe. – https://tryhackme.com
67. Вступ до журналювання Linux (/var/log/auth.log, /var/log/syslog)
68. WPA2 Enterprise Best Practices – https://www.cisa.gov
69. WPA3 Transition Recommendations – https://www.wi-fi.org
70. Welekwe A. Threat Modeling Guide: Components, Frameworks, Methods & Tools. – https://www.comparitech.com/net-admin/threat-modeling-guide/

6.3. Програмне забезпечення

71. Any.Run Online Sandbox - інтерактивний онлайн-інструмент для динамічного аналізу шкідливого програмного забезпечення. - https://any.run
72. AWS IAM - сервіс Amazon Web Services для управління ідентифікацією та доступом. - https://docs.aws.amazon.com/IAM/latest/UserGuide/
73. AWS KMS - сервіс Amazon Web Services для управління ключами. - https://docs.aws.amazon.com/kms/
74. Azure AD - сервіс Microsoft Azure для управління ідентифікацією та доступом у хмарі. - https://docs.microsoft.com/en-us/azure/active-directory/
75. Azure Key Vault - сховище ключів Microsoft Azure для безпечного зберігання та управління ключами, секретами та сертифікатами. - https://learn.microsoft.com/en-us/azure/key-vault/
76. Cuckoo Sandbox - автоматизований інструмент аналізу шкідливого програмного забезпечення. - https://cuckoosandbox.org
77. CWE - список поширених типів вразливостей програмного забезпечення. - https://cwe.mitre.org/
78. Elastic Common Schema (ECS) - стандарт для нормалізації даних журналів і метрик. - https://github.com/elastic
79. Elasticsearch - пошукова та аналітична система. - https://www.elastic.co/guide/index.html
80. Google Cloud IAM - сервіс Google Cloud для управління ідентифікацією та доступом. - https://cloud.google.com/iam/docs
81. Google Cloud KMS - сервіс Google Cloud для управління ключами. - https://cloud.google.com/kms
82. Guidance Software. EnCase Forensic - інструмент для комп'ютерної криміналістики. - https://www.guidancesoftware.com/forensic-solutions
83. HashiCorp Vault - інструмент для безпечного зберігання та доступу до паролів. - https://www.vaultproject.io
84. Hybrid Analysis - безкоштовний сервіс аналізу шкідливого програмного забезпечення. - https://www.hybrid-analysis.com
85. Kali Linux - дистрибутив Linux для тестування на проникнення та аудиту безпеки. - https://docs.kali.org
86. Metasploit - фреймворк для тестування на проникнення та розробки експлойтів. - https://docs.metasploit.com
87. map Network Scanning - утиліта для дослідження мереж та аудиту безпеки. - https://nmap.org/book/man.html

88. Open Threat Exchange (OTX) - платформа для обміну інформацією про загрози. - https://otx.alienvault.com/
89. OWASP: Web Security Testing Guide – інформаційно-аналітична платформа з тестування безпеки вебдодатків від Open Web Application Security Project. - https://owasp.org/www-project-web-security-testing-guide/latest/
90. OWASP Threat Drago - інструмент для моделювання загроз від OWASP. - https://owasp.org/www-project-threat-dragon/
91. PortSwigger Web Security. Burp Suite - інтегрована платформа для тестування безпеки вебдодатків. - https://portswigger.net/burp/documentation
92. QRadar - SIEM-система від IBM для аналізу журналів подій безпеки. - https://www.ibm.com/products/qradar-siem
93. Scikit-learn - бібліотека для машинного навчання на Python. - https://scikit-learn.org
94. Shodan API - інтерфейс програмування додатків для пошукової системи, що сканує підключені до інтернету пристрої. - https://developer.shodan.io/
95. Splunk BOTS - інструменти та демонстраційні набори даних для аналізу поведінки загроз у Splunk. - https://github.com/splunk
96. Splunk - SIEM-система для аналізу машинних даних. - https://docs.splunk.com/
97. Splunk SOAR - платформа для автоматизації та оркестрування реагування на інциденти безпеки. - https://www.splunk.com/en_us/products/soar.html
98. The Sleuth Kit (TSK) - інструментарій для аналізу файлових систем та цифрової криміналістики. - https://www.sleuthkit.org
99. Web Security Testing Guide - інформаційно-аналітична платформа з тестування безпеки вебдодатків від OWASP. - https://owasp.org/www-project-web-security-testing-guide/
100. Wireshark - аналізатор мережевого трафіку. - https://wireshark.org/docs/wsug_html_chunked/

Рецензія на робочу програму (силабус) ОК Управління кібербезпекою

Розроблену викладачем кафедри кібернетики та інформатики (назва) В'юненком О.Б (ПІБ)

Параметр, за яким оцінюється робоча програма (силабус) освітнього компонента гарантом або членом проєктної групи	**Так**	**Ні**	**Коментар**
Результати навчання за освітнім компонентом (ДРН) відповідають НРК	+		
Результати навчання за освітнім компонентом (ДРН) відповідають передбаченим ПРН (для обов'язкових ОК)	+		
Результати навчання за освітнім компонентом дають можливість виміряти та оцінити рівень їх досягнення	+		

Член проектної групи ОП Інформаційні системи та технології (назва) Пасько Н.Б. (ПІБ) (підпис)

Параметр, за яким оцінюється робоча програма (силабус) освітнього компонента викладачем відповідної кафедри	**Так**	**Ні**	**Коментар**
Загальна інформація про освітній компонент є достатньою	+		
Результати навчання за освітнім компонентом (ДРН) відповідають НРК	+		
Результати навчання за освітнім компонентом (ДРН) дають можливість виміряти та оцінити рівень їх досягнення	+		
Результати навчання (ДРН) стосуються компетентностей студентів, а не змісту дисципліни (містять знання, уміння, навички, а не теми навчальної програми дисципліни)	+		
Зміст ОК сформовано відповідно до структурно-логічної схеми	+		
Навчальна активність (методи викладання та навчання) дає змогу студентам досягти очікуваних результатів навчання (ДРН)	+		
Освітній компонент передбачає навчання через дослідження, що є доцільним та достатнім для відповідного рівня вищої освіти	+		
Стратегія оцінювання в межах освітнього компонента відповідає політиці Університету/факультету	+		
Передбачені методи оцінювання дозволяють оцінити ступінь досягнення результатів навчання за освітнім компонентом	+		
Навантаження студентів є адекватним обсягу освітнього компонента	+		
Рекомендовані навчальні ресурси є достатніми для досягнення результатів навчання (ДРН)	+		
Література є актуальною	+		
Перелік навчальних ресурсів містить необхідні для досягнення ДРН програмні продукти	+		

Рецензент (викладач кафедри) кібернетики та інформатики (назва) доц. Агаджанова С.В. (посада, ПІБ) (підпис)