МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Волинський національний університет імені Лесі Українки
Факультет інформаційних технологій і математики
Кафедра комп'ютерних наук та кібербезпеки

СИЛАБУС
вибіркового освітнього компонента
Системний та мережевий моніторинг в кібербезпеці
першого (бакалаврського) рівня

Луцьк – 2026

Силабус вибіркового освітнього компонента «Системний та мережевий моніторинг в кібербезпеці**»** для підготовки першого (бакалаврського) рівня вищої освіти**.**

Розробник: доцент, кандидат технічних наук Онищук Оксана Олександрівна

Погоджено

Гарант освітньо-професійної програми: Чернящук Н.Л.

Силабус освітнього компонента затверджено на засіданні кафедри комп'ютерних наук та кібербезпеки

протокол № 6 від 15.01.2026 р.

Завідувач кафедри: Гришанович Т. О.

І. Опис освітнього компонента

Найменування показників	Характеристика освітнього компонента
	Вибірковий
Денна форма навчання	Рік підготовки 4
150/5 кредитів	Семестр 8
	Лекції 10 год.
	Лабораторні 20 год.
	Самостійна робота 110 год.
ІНДЗ: немає	Консультації 10 год.
	Форма контролю: залік

ІІ. Інформація про викладача

ПІП – Онищук Оксана Олександрівна
Науковий ступінь – кандидат технічних наук
Вчене звання – доцент
Посада – доцент комп'ютерних наук та кібербезпеки
Контактна інформація: +38-0966943585, Onyshchuk.oksana@vnu.edu.ua

ІІІ. Опис освітнього компонента

1. **Мета освітнього компонента** полягає у наданні здобувачам теоретичних та практичних знань про основні принципи, методи та інструменти моніторингу систем та мереж. Це дозволяє їм розуміти, впроваджувати та управляти системами моніторингу з метою забезпечення надійності, безпеки та ефективності інформаційних технологій.
2. **Завданнями вивчення освітнього компонента** є: надання здобувачам необхідних теоретичних знань про види, методи моніторингу та функціонування сучасних моніторингових систем; вироблення в здобувачів навичок побудови систем моніторингу на прикладі Linux і Windows з особливою увагою безпековим налаштуванням цих систем.
3. **Soft Skills.** У результаті вивчення освітнього компонента «Системний та мережевий моніторинг в кібербезпеці» у здобувачів формуються такі **(soft)** компетентності: аналітичне та системне мислення – здатність обирати оптимальні хмарні рішення для розв’язання прикладних задач, оцінювати ефективність різних моделей (IaaS, PaaS, SaaS) та сервісів; критичне мислення – вміння аналізувати переваги й ризики використання хмарних технологій, приймати обґрунтовані рішення щодо вибору платформ і сервісів; цифрова грамотність та інформаційна культура – впевнене використання сучасних хмарних сервісів, зокрема Amazon Web Services, Microsoft Azure, Google Cloud та сервісу Google Colab для професійної діяльності; навички командної роботи – здатність організовувати та координувати спільну роботу в хмарному середовищі, ефективно розподіляти ролі та відповідальність у команді; комунікаційні навички – вміння презентувати результати проєктів, готувати технічну документацію та пояснювати принципи роботи хмарних платформ; управління часом – планування етапів розробки та впровадження прикладних рішень у хмарному середовищі; самоорганізація та відповідальність – дотримання

принципів безпеки даних, академічної доброчесності та ефективне використання хмарних ресурсів; адаптивність та здатність до самонавчання – готовність опановувати нові сервіси, інструменти й технології у сфері хмарних обчислень.

4. Структура освітнього компонента

Назви змістових модулів і тем	Кількість годин					Форма контролю / Бали
	Усього	у тому числі				
		Лекції	Лабораторні заняття	Консультації	Самостійна робота	
Змістовий модуль 1. Основи системного моніторингу.						
Тема 1. Вступ до системного моніторингу.	20	2	3	1	11	МКР
Тема 2. Архітектура системного моніторингу	15	1	2	2	22	Зах. ЛР
Разом за змістовим модулем 1	**35**	**3**	**5**	**3**	**33**	**25 б.**
Змістовий модуль 2. Основи мережевого моніторингу.						
Тема 3. Вступ до мережевого моніторингу.	20	1	3	1	11	Зах. ЛР
Тема 4. Протоколи NetFlow та sFlow.	20	1	2	1	11	Зах. ЛР
Разом за змістовим модулем 2	**40**	**2**	**5**	**2**	**22**	**25 б.**
Змістовий модуль 3. Інструменти моніторингу та аналізу даних.						
Тема 5. Інструменти та технології системного моніторингу.	15	2	3	2	11	Зах. ЛР
Тема 6. Аналіз та візуалізація даних мережевого моніторингу.	15	1	3	1	11	Зах. ЛР
Тема 7. Впровадження системи моніторингу на основі Wazuh та MS SCOM.	**15**	**1**	**2**	**1**	**11**	Зах. ЛР
Тема 8. Застосування моніторингу для виявлення загроз безпеці	**30**	**1**	**2**	**1**	**22**	Зах. ЛР
Разом за змістовим модулем 3	**75**	**5**	**10**	**5**	**55**	**50 б.**
Всього годин	**150**	**10**	**20**	**10**	**110**	**100 б.**
Види підсумкових робіт						**Бали**

Форма контролю: Д – дебати, Т – тести, ТР – тренінг, РЗ/К – розв'язування задач/кейсів, ІНДЗ/ІРС – індивідуальне завдання/індивідуальна робота здобувача освіти, РМГ – робота в малих групах, МКР/КР – модульна контрольна робота/ контрольна робота, Р – реферат, а також аналітична записка, аналітичне есе, аналіз твору тощо.

Теми лабораторних робіт

№ з/п	Назва теми	

1	Налаштування віртуального середовища: Встановлення та конфігурування Oracle VirtualBox на локальному комп'ютері. Створення віртуальних машини для моніторингу. Інсталяція GNS3	2
2	Встановлення системи моніторингу: Встановлення та налаштування популярних систем моніторингу, таких як Nagios або Zabbix, на віртуальній машині. Дослідження їх основних можливостей та налаштування моніторингу різних системних ресурсів.	2
3	Використання NetFlow та sFlow: Налаштування мережевого обладнання на віртуальній машині, для генерації даних NetFlow та sFlow. Налаштування системи моніторингу для збору та аналізу цих даних. Вивчення та порівняння результатів моніторингу з використанням різних протоколів.	1
4	Аналіз мережевого трафіку: Збір та аналіз мережевого трафіку на віртуальній машині. Використання інструментів, таких як Wireshark, для аналізу пакетів та виявлення проблем в мережі. Розуміння принципів потокового аналізу та використання відповідних інструментів.	1
5	Моніторинг безпеки: Налаштування системи моніторингу для виявлення загроз безпеці в мережі. Аналіз подій безпеки та використання індикаторів компрометації для виявлення аномалій. Розробка та впровадження стратегій відповіді на інциденти безпеки.	1
6	Візуалізація та аналіз даних моніторингу: Використання інструментів візуалізації, таких як Grafana або Kibana, для створення графіків, діаграм та звітів на основі даних моніторингу.	1
7	Встановлення та налаштування WAZUH: створення віртуального серверу WAZUH, налаштування агентів моніторингу, конфігурація правил моніторингу, налаштування моніторингу вразливостей та виявлення індикаторів компрометації.	1
8	Основи роботи з WAZUH: аналіз подій безпеки та вжиття заходів у разі виявлення загроз, створення власних правил моніторингу для специфічних сценаріїв, проведення симуляції атак та аналіз відповіді системи моніторингу на ці атаки.	1
РАЗОМ		10

IV. Політика оцінювання

Політика викладача щодо здобувача освіти. Здобувачі освіти повинні відвідувати лабораторні заняття та вчасно складати відповідні завдання до роботи на комп’ютерах. Оцінювання робіт здійснюється з урахуванням вірно виконаного обсягу у пропорції до визначеного цим силабусом балу із заокругленням до більшого.

Політика щодо академічної доброчесності. Здобувачам вищої освіти дозволяється вивчати довільні джерела інформації, що стосуються тематики завдань, а також консультуватися та працювати у групах зі своїми колегами за курсом. Проте завдання повинні бути виконані самостійно. В іншому разі відповідні бали здобувачу вищої освіти не зараховуються.

Політика щодо дедлайнів та перескладання. Завдання мають бути виконані у межах відведеного на це часу. Невчасно здане без поважної причини завдання зменшує відповідний бал оцінювання на 10 % для забезпечення справедливого рейтингового оцінювання здобувачів вищої освіти, особливо тих, хто вчасно виконує відповідні завдання.

Оцінювання знань здобувачів освіти здійснюється під час поточного контролю за результатами виконання тих видів робіт, які передбачені силабусом освітнього компонента. (згідно Положення про поточне та підсумкове оцінювання знань здобувачів освіти Волинського національного університету імені Лесі Українки).

Оцінювання навчальних досягнень здійснюється за 100 бальною шкалою. Оцінка включає в себе поточний контроль (оцінюється робота на парах, вчасне і якісне виконання домашніх завдань, самостійне розв'язання індивідуальних завдань) та підсумковий модульний контроль (письмові модульні контрольні роботи). Максимальна кількість балів, яку може заробити здобувач під час поточного оцінювання за семестр – 70 балів. Підсумковий модульний контроль за семестр включає в себе оцінки за всі модульні контрольні роботи (МКР). Максимальна кількість балів, яку може заробити здобувач під час модульного контролю за семестр складає 30 балів.

Якщо за результатами семестру накопичено не менше 75 балів і здобувач погоджується із цим результатом, то оцінка за семестр може виставлятися без складання заліку. В іншому разі здобувач складає залік; максимальна кількість балів, яку можна отримати на заліку – 60 балів. Вони замінюють бали модульного семестрового контролю, поточний семестровий контроль при цьому зберігається. Залік проходять в усній формі. Оцінка за семестр у випадку складання екзамену є сумою балів поточного контролю та балів, отриманих під час екзамену.

V. Підсумковий контроль

На залік виносяться основні питання, типові та комплексні задачі, ситуації, завдання, що потребують творчої відповіді та вміння синтезувати отримані знання і застосовувати їх під час розв'язання практичних задач.Іспит проводиться в усній формі. Залік проходить у письмовій формі.

Шкала оцінювання знань здобувачів освіти з освітніх компонентів, де формою контролю є залік	Оцінка в балах	Лінгвістична оцінка
	90–100	Зараховано
	82–89	
	75–81	
	67–74	
	60–66	
	1–59	Незараховано (необхідне перескладання)

VI. Рекомендована література та інтернет-ресурси

Основна література

1. 1. Покроковий посібник по створенню CSIRT / ENISA (в рамках програми WP- 2006). – 2006. – 86 с.
2. 2. Information technology. Security techniques. Information security management. Measurement : ISO/IEC 27004:2009 / International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). – 2020. – 55 p.
3. 3. Information technology. Security techniques. Information security incident management : ISO 27035:2011. – 78 p.
4. 4. Moira J.W.-B. Handbook for Computer Security Incident Response Teams (CSIRTs) / Moira JW-B., Stikvoort D., Kossakowski K.-P. et al. – Pittsburgh, 2021. – 223p.
5. 5. Performance Measurement Guide for Information Security: NIST Special Publication 800-55- rev1. / U.S. Government Printing Office. Washington – 2021. – 80 p.

6. ***Допоміжна література***

7. Новітні теоретичні та практичні дані й матеріали що стосуються теорії та практики моніторингу, аудиту та управління системами кібербезпеки рекомендується відслідковувати засобом звертання до наступних сайтів:

8. 1. https://tzi.com.ua/audbezib.html
9. 2. https://portal.rangeforce.com/
10. 3. https://www.netacad.com/
11. 4. http://www.crest-approved.org
12. 5. https://www.iso27001security.com
13. 6. https://securityonion.net/
14. 7. http://www.enisa.europa.eu
15. 8. https://www.splunk.com