ЗАТВЕРДЖЕНО

Вченою радою факультету
факультету інформаційно-
комп'ютерних технологій
31 серпня2023 р., протокол № 5

Голова Вченої ради
_____ Тетяна НІКІТЧУК

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ВК «СИСТЕМНИЙ ТА МЕРЕЖЕВИЙ МОНІТОРИНГ»

для здобувачів вищої освіти освітнього ступеня «магістр»
спеціальності 125 «Кібербезпека та захист інформації»
освітньо-професійна програма «Кібербезпека»
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
_____ Володимир ВОРОТНІКОВ

Розробник: старший викладач кафедри комп'ютерної інженерії та кібербезпеки
Ігор ФАЛЬКОВСЬКИЙ

Житомир
2023 – 2024 н.р.

1. Опис навчальної дисципліни

Найменування показників	Галузь знань, напрям підготовки, освітній ступінь	Характеристика навчальної дисципліни
		денна форма навчання
Кількість кредитів – 8	Галузь знань 12 «Інформаційні технології»	Нормативна
Модулів – 1	Спеціальність 125 «Кібербезпека та захист інформації»	Рік підготовки:
Змістових модулів – 3		1
		Семестр
Загальна кількість годин – 48		2
		Лекції
Тижневих годин для денної форми навчання 2-й семестр: аудиторних – 48 самостійної роботи – 72	Освітній ступінь «бакалавр»	16 год.
		Практичні
		–
		Лабораторні
		32 год.
		Самостійна робота
		72 год.
		Вид контролю: залік

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

для денної форми навчання – 60% аудиторних занять, 40% самостійної та індивідуальної роботи.

2. Мета та завдання навчальної дисципліни

Метою навчальної дисципліни полягає у наданні студентам 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.

Завданнями вивчення навчальної дисципліни є:

–надання студентам необхідних теоретичних знань про види, методи моніторингу та функціонування сучасних моніторингових систем;

–вироблення в студентів навичок побудови систем моніторингу на прикладі Linux і Windows з особливою увагою безпековим налаштуванням цих систем.

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

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

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

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 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 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.

КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики 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 10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.

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

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

РН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.

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

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

РН 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.

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

РН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.

РН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

РН 24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).

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 26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.

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

3. Програма навчальної дисципліни

Модуль 1. Системний та мережевий моніторинг

Змістовий модуль 1. Основи системного моніторингу

Тема 1. Вступ до системного моніторингу.

Визначення системного моніторингу та його роль у сучасних інформаційних технологіях.

Основні принципи та цілі системного моніторингу.

Види метрик, що вимірюються при системному моніторингу.

Тема 2. Архітектура системного моніторингу.

Компоненти системи моніторингу: агенти, сервери, бази даних.

Розгорнуті та розподілені архітектури моніторингу.

Протоколи зв'язку між компонентами системи моніторингу.

Змістовий модуль 2. Основи мережевого моніторингу

Тема 3. Вступ до мережевого моніторингу.

Значення мережевого моніторингу у сучасних мережевих інфраструктурах.
Основні завдання та вимоги до мережевого моніторингу.
Засоби та технології, використовувані для збору мережевих даних.

Тема 4. Протоколи NetFlow та sFlow.

Визначення та основні характеристики протоколів NetFlow та sFlow.
Використання протоколів NetFlow та sFlow для збору мережевих статистичних даних.
Аналіз та використання даних, зібраних за допомогою протоколів NetFlow та sFlow..

Змістовий модуль 3. Інструменти моніторингу та аналізу даних

Тема 5. Інструменти та технології системного моніторингу.

Огляд популярних інструментів системного моніторингу, таких як Nagios, Zabbix, Prometheus, MS SCOM.
Практичне використання інструментів для моніторингу системних ресурсів та додатків.
Налаштування сповіщень та автоматизація управління системним моніторингом.

Тема 6. Аналіз та візуалізація даних мережевого моніторингу.

Методи аналізу даних мережевого моніторингу та їх застосування для виявлення аномалій та проблем в мережі.
Використання інструментів візуалізації даних для створення графіків, діаграм та звітів.
Розробка звітів та дашбордів для ефективного моніторингу мережі..

Тема 7. Впровадження систем моніторингу на основі Wazuh та MS SCOM.

Огляд Wazuh як відкритої платформи для моніторингу безпеки.
Огляд MS SCOM як інструменту системного моніторингу від Microsoft.
Підготовка та налаштування Wazuh-сервера, агентів і MS SCOM.
Моніторинг та виявлення загроз безпеки за допомогою Wazuh та MS SCOM..

Тема 8. Застосування моніторингу для виявлення загроз безпеці.

Роль візуалізації у розумінні та представленні даних моніторингу.

Використання системного та мережевого моніторингу для виявлення вторгнень, зламів та інших загроз безпеці.

Аналіз логів, виявлення аномалій та паттернів, пов'язаних із зловмисними діями.

Розробка стратегій реагування та відновлення після виявлення загроз.

4. Структура (тематичний план) навчальної дисципліни

Змістові модулі і теми	Кількість годин							
	денна форма				заочна форма			
	усього	лекції	лабораторні	самостійна робота	усього	лекції	лабораторні	самостійна робота
Модуль 1								
Змістовий модуль 1. Основи системного моніторингу.								
Тема 1. Вступ до системного моніторингу.	14	2	4	8	–	–	–	–
Тема 2. Архітектура системного моніторингу	14	2	4	8	–	–	–	–
Разом за змістовий модуль 1	28	4	8	16	–	–	–	–
Змістовий модуль 2. Основи мережевого моніторингу.								
Тема 3. Вступ до мережевого моніторингу.	14	2	4	8	–	–	–	–
Тема 4. Протоколи NetFlow та sFlow.	14	2	4	8	–	–	–	–
Разом за змістовий модуль 1	28	4	8	16	–	–	–	–
Змістовий модуль 3. Інструменти моніторингу та аналізу даних.								
Тема 5. Інструменти та технології системного моніторингу.	16	2	4	10	–	–	–	–
Тема 6. Аналіз та візуалізація даних мережевого моніторингу.	16	2	4	10	–	–	–	–

Тема 7. Впровадження системи моніторингу на основі Wazuh та MS SCOM.	16	2	4	10	–	–	–	–
Тема 8. Застосування моніторингу для виявлення загроз безпеці	16	2	4	10	–	–	–	–
Разом за змістовий модуль 3	64	8	16	40	–	–	–	–
ВСЬОГО	120	16	32	72	–	–	–	–

5. Теми практичних (лабораторних) занять

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	Налаштування віртуального середовища: Встановлення та конфігурування Oracle VirtualBox на локальному комп'ютері. Створення віртуальних машини для моніторингу. Інсталяція GNS3	4	–
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.	4	–
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.	4	–
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.	4	–
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.	4	–
6	Візуалізація та аналіз даних моніторингу: Використання інструментів візуалізації, таких як Grafana або Kibana, для створення графіків, діаграм та звітів на основі даних моніторингу.	4	–

	Аналіз результатів моніторингу та виявлення цікавих залежностей та трендів.		
7	Встановлення та налаштування WAZUH: створення віртуального серверу WAZUH, налаштування агентів моніторингу, конфігурація правил моніторингу, налаштування моніторингу вразливостей та виявлення індикаторів компрометації.	4	–
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.	4	–
РАЗОМ		32	–

6. Завдання для самостійної роботи

7. Індивідуальні завдання

8. Методи навчання

Застосовуються такі форми організації навчання, як лекція-бесіда, лекціяпрезентація, лабораторна робота, аудиторна та позааудиторна контрольна робота, залік, екзамен.

Використовуються наступні методи навчання: розповідь, пояснення, бесіда, інструктаж, пояснення, демонстрація, спостереження, лабораторна робота, «мозковий штурм», ситуаційний аналіз.

9. Методи контролю

Передбачено заходи поточного та підсумкового контролю. Поточний контроль здійснюється шляхом проходження студентами комп’ютерних тестів, виконання завдань лабораторних робіт, фронтального та індивідуального усного опитування, ситуаційного аналізу. Підсумковий контроль реалізовано у формі електронного тестування та контрольних робіт практичного характеру.

10. Розподіл балів

Навчальна дисципліна вивчається протягом одного семестру. Накопичення студентами рейтингового балу здійснюється протягом цього періоду.

Нарахування балів здійснюється за наступною схемою. 60 балів виділяється на поточне оцінювання, 40 балів – на модульний контроль. Сумарна кількість балів, які студент може отримати під час лекції, становить 5,6 бала за семестр, під час лабораторних занять – 54,4 бала за семестр. Самостійна робота оцінюється під час заходів модульного контролю (15 балів). Детальний розподіл балів наводиться у рейтингових таблицях і доступний студентам протягом усього періоду вивчення дисципліни.

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

Допоміжна література

12. Інформаційні ресурси в Інтернеті