

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-22.05-05.01/ 12.00.1/М/ ВК-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 14 / 1

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
«Системний та мережевий моніторинг»
факультет інформаційно-комп'ютерних технологій**

для здобувачів вищої освіти освітнього ступеня «магістр»

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

Завідувач кафедри

 Андрій ЄФІМЕНКО

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

Житомир
2024 – 2025 н.р.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-22.05-05.01/ 12.00.1/М/ ВК-1-2024
	<i>Випуск 1</i>	<i>Зміни 0</i>	<i>Екземпляр № 1</i>	<i>Арк 14 / 2</i>

Робоча програма навчальної дисципліни фахової підготовки «Системний та мережевий моніторинг» для здобувачів вищої освіти освітнього ступеня «магістр» затверджена Вченою радою факультету інформаційно-комп'ютерних технологій від 28 серпня 2024 р., протокол № 8.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-22.05-05.01/ 12.00.1/М/ ВК-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 14 / 3

1. Опис навчальної дисципліни

Найменування показників	Галузь знань, напрям підготовки, освітній ступінь	Характеристика навчальної дисципліни
		денна форма навчання
Кількість кредитів – 4	Галузь знань 12 «Інформаційні технології»	Вибіркова компонента
Модулів – 1	Спеціальність 121 Інженерія програмного забезпечення 122 Комп'ютерні науки 123 Комп'ютерна інженерія 125 Кібербезпека та захист інформації	Рік підготовки:
Змістових модулів – 3		1
Загальна кількість годин – 120		Семестр
		2
Тижневих годин для денної форми навчання аудиторних – 64 год. самостійної роботи – 56 год.	Освітній ступінь «магістр»	Лекції
		16 год.
		Практичні
		–
		Лабораторні
		48 год.
		Самостійна робота
		56 год.
Вид контролю:	залік	

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

для денної форми навчання – 53,3% аудиторних занять, 46,7% самостійної та індивідуальної роботи.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-22.05-05.01/ 12.00.1/М/ ВК-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 14 / 4

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.

Під час вивчення навчальної дисципліни здобувачі вищої освіти зможуть отримати та покращити наступні Soft skills:

- *комунікативні навички*: письмове, вербальне й невербальне спілкування; уміння грамотно спілкуватися по e-mail; вести дискусію і відстоювати свою позицію; навички працювати в команді;

- *уміння виступати привселюдно*: навички, необхідні для виступів на публіці; навички проведення презентації;

- *керування часом*: уміння справлятися із завданнями вчасно;

- *гнучкість і адаптивність*: гнучкість, адаптивність і здатність змінюватися; уміння аналізувати ситуацію, орієнтування на вирішення проблеми;

- *лідерські якості*: уміння спокійно працювати в напруженому середовищі; уміння ухвалювати рішення; уміння ставити мету, планувати діяльність;

- *особисті якості*: креативне й критичне мислення; етичність, чесність, терпіння, повага до оточуючих.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-22.05-05.01/ 12.00.1/М/ ВК-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 14 / 5

3. Програма навчальної дисципліни

МОДУЛЬ 1.

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.

Протоколи збору трафіку: SNMP, Netflow, IPFIX, sFlow, JFlow
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.
Типові інструменти мережевого моніторингу
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.
Моніторинг та виявлення загроз безпеки за допомогою Wazuh та MS SCOM..

Тема 8. Застосування моніторингу для виявлення загроз безпеці.

Застосування моніторингу для виявлення загроз безпеці.
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.
Компроміси безпеки

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-22.05-05.01/ 12.00.1/М/ ВК-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 14 / 6

4. Структура (тематичний план) навчальної дисципліни

Змістові модулі і теми	Кількість годин							
	денна форма				заочна форма			
	у с ь о г о	л ек ці ї	ла бо ра то рн і	с а м о ст і й н а р о б о т а	у с ь о г о	л ек ці ї	ла бо ра то рн і	с а м о ст і й н а р о б о т а
Модуль 1								
Змістовий модуль 1. Основи системного моніторингу.								
Тема 1. Вступ до системного моніторингу.	14	2	6	6	–	–	–	–
Тема 2. Архітектура системного моніторингу	14	2	6	6	–	–	–	–
<i>Разом за змістовий модуль 1</i>	28	4	12	12	–	–	–	–
Змістовий модуль 2. Основи мережевого моніторингу.								
Тема 3. Вступ до мережевого моніторингу.	14	2	6	6	–	–	–	–
Тема 4. Протоколи NetFlow та sFlow.	14	2	6	6	–	–	–	–
<i>Разом за змістовий модуль 1</i>	28	4	12	12	–	–	–	–
Змістовий модуль 3. Інструменти моніторингу та аналізу даних.								
Тема 5. Інструменти та технології системного моніторингу.	16	2	6	8	–	–	–	–
Тема 6. Аналіз та візуалізація даних мережевого моніторингу.	16	2	6	8	–	–	–	–
Тема 7. Впровадження системи моніторингу на основі Wazuh та MS SCOM.	16	2	6	8	–	–	–	–
Тема 8. Застосування моніторингу для виявлення загроз безпеці	16	2	6	8	–	–	–	–
<i>Разом за змістовий модуль 3</i>	64	8	24	32	–	–	–	–
ВСЬОГО	120	16	48	56	–	–	–	–

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-22.05-05.01/ 12.00.1/М/ ВК-1-2024
	<i>Випуск 1</i>	<i>Зміни 0</i>	<i>Екземпляр № 1</i>	<i>Арк 14 / 7</i>

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-22.05-05.01/ 12.00.1/М/ ВК-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 14 / 8

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. Налаштування NAT Network. Створення віртуальних машини для моніторингу.	6	–
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.	6	–
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.	6	–
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.	6	–
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.	6	–
6	Візуалізація та аналіз даних моніторингу: Використання інструментів візуалізації, таких як Grafana або Kibana, для створення графіків, діаграм та звітів на основі даних моніторингу. Аналіз результатів моніторингу та виявлення цікавих залежностей та трендів.	6	–
7	Встановлення та налаштування WAZUH: створення віртуального серверу WAZUH, налаштування агентів моніторингу, конфігурація правил моніторингу, налаштування моніторингу вразливостей та виявлення індикаторів компрометації.	6	–
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.	6	–
РАЗОМ		48	–

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-22.05-05.01/ 12.00.1/М/ ВК-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 14 / 9

6. Завдання для самостійної роботи

1. Основи віртуалізації та налаштування VirtualBox:
 - Принципи роботи віртуалізації.
 - Створення та керування віртуальними машинами в Oracle VirtualBox.
 - Мережеві налаштування віртуальних машин (NAT, Bridge, Host-only).
2. Концепції моніторингу IT-систем:
 - Що таке моніторинг та його значення.
 - Основні метрики моніторингу: CPU, RAM, дисковий простір, мережеві ресурси.
 - Вибір відповідних інструментів моніторингу для різних типів систем.
3. Встановлення та конфігурація Zabbix:
 - Створення базових моніторингових елементів (хости, тригери, шаблони).
 - Вивчення механізму оповіщення про події.
 - Налаштування моніторингу служб, що працюють на різних операційних системах.
4. Інтеграція Zabbix з Grafana для візуалізації:
 - Підключення Zabbix як джерела даних до Grafana.
 - Створення дашбордів для візуалізації даних про системи.
 - Огляд різних типів графіків для моніторингу мережевого стану.
5. Поглиблене налаштування Nagios:
 - Створення та конфігурація плагінів для моніторингу специфічних ресурсів.
 - Налаштування оповіщень та звітів.
 - Порівняння з іншими системами моніторингу.
6. Протоколи NetFlow та sFlow: порівняння та використання:
 - Основи роботи з NetFlow і sFlow для збору мережевих даних.
 - Налаштування мережевих пристроїв для генерації потоків NetFlow/sFlow.
 - Порівняння протоколів та аналіз результатів.
7. Аналіз мережевого трафіку з Wireshark:
 - Основи роботи з Wireshark.
 - Аналіз та фільтрація мережевих пакетів для виявлення потенційних проблем.
 - Використання кольорового кодування та фільтрів для спрощення аналізу.
8. Моніторинг мережевої безпеки:
 - Виявлення DDoS атак та методи їх запобігання.
 - Використання інструментів IDS/IPS для виявлення аномалій у мережі.
 - Вивчення методів виявлення спроб сканування мережі та вторгнень.
9. Використання WAZUH для виявлення загроз:
 - Встановлення та налаштування агентів WAZUH на клієнтських машинах.
 - Створення правил для виявлення аномальних подій.
 - Реагування на інциденти безпеки.
10. Моніторинг уразливостей за допомогою WAZUH:
 - Автоматичне виявлення вразливостей у системах.
 - Інтеграція з інструментами для патч-менеджменту.
 - Порівняння різних типів вразливостей та інструментів для їх моніторингу.
11. Збір та аналіз журналів подій за допомогою ELK Stack (Elasticsearch, Logstash, Kibana):
 - Налаштування збору логів з різних джерел.
 - Візуалізація та аналіз подій у Kibana.
 - Виявлення аномалій та загроз через аналіз логів.
12. Інтеграція WAZUH з SIEM-системами:

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-22.05-05.01/ 12.00.1/М/ ВК-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 14 / 10

- Основи роботи з SIEM-системами (Security Information and Event Management).
Підключення WAZUH до SIEM для аналізу інцидентів.
Моніторинг в реальному часі та оповіщення про інциденти.
13. Моніторинг мережевого обладнання (SNMP):
Протокол SNMP: основні концепції та конфігурація.
Моніторинг маршрутизаторів, комутаторів та інших мережевих пристроїв.
Вивчення ролі MIB-файлів у налаштуванні моніторингу.
 14. Інцидент-менеджмент: розробка політик та стратегій реагування:
Розробка та впровадження політик безпеки.
Симуляція інцидентів та створення планів відновлення.
Управління постінцидентним аналізом та звітуванням.
 15. Налаштування Syslog-серверу для збору подій:
Налаштування Syslog для збору логів з мережевих пристроїв.
Фільтрація та управління логами на сервері.
Порівняння Syslog з іншими інструментами для збору подій.
 16. Розгортання агентів моніторингу на хмарних інфраструктурах:
Вивчення особливостей моніторингу хмарних сервісів (AWS, Azure, GCP).
Моніторинг ресурсів у хмарі за допомогою Nagios, Zabbix або WAZUH.
Особливості налаштування безпеки та управління доступом в хмарних середовищах.

7. Індивідуальні самостійні завдання

Індивідуальні завдання не передбачені навчальним планом.

8. Методи навчання

Застосовуються такі форми організації навчання, як лекція-бесіда, лекція-презентація, лабораторна робота, аудиторна та позааудиторна контрольна робота, 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. Оцінювання результатів навчання здобувачів вищої освіти

Оцінювання результатів навчання здобувачів вищої освіти з навчальної дисципліни здійснюється відповідно до Положення про оцінювання результатів навчання здобувачів вищої освіти у Державному університеті «Житомирська політехніка» та розподілу балів, що наведений нижче.

Система оцінювання результатів навчання здобувачів вищої освіти з навчальної дисципліни включає поточний та підсумковий контроль.

Поточний контроль проводиться для оцінювання рівня засвоєння знань, формування умінь і навичок здобувачів вищої освіти впродовж вивчення ними матеріалу модуля (змістових

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-22.05-05.01/ 12.00.1/М/ ВК-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 14 / 11

модулів) навчальної дисципліни. Поточний контроль здійснюється під час проведення навчальних занять.

Підсумковий контроль проводиться для підсумкового оцінювання результатів навчання здобувачів вищої освіти з навчальної дисципліни. Підсумковий контроль здійснюється після завершення вивчення навчальної дисципліни або наприкінці семестру. Підсумковий контроль проводиться у формі заліку. Процедура складання заліку визначена у Положенні про організацію освітнього процесу у Державному університеті «Житомирська політехніка».

Розподіл балів з навчальної дисципліни

Види робіт здобувача вищої освіти	Кількість балів за семестр	
	денна форма	заочна форма
Виконання завдань поточного контролю	100	100
Підсумкова семестрова оцінка	100	100

Розподіл балів за виконання завдань поточного контролю

Види робіт здобувача вищої освіти	Кількість балів за семестр	
	денна форма	заочна форма
Виконання завдань під час навчальних занять	100	—
Виконання та захист індивідуальних самостійних завдань	0	—
Виконання науково-дослідної роботи та інших видів робіт (додаткові – заохочувальні бали):		
1. Участь у студентських предметних олімпіадах, Всеукраїнському конкурсі студентських наукових робіт, грантах, науково-дослідних проектах	—	—
2. Підготовка наукових статей, тез доповідей наукових конференцій		
3. Інші види робіт (наводиться перелік інших видів робіт)		
Разом за виконання завдань поточного контролю	100	100

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідас ДСТУ ISO 9001:2015			Ф-22.05-05.01/ 12.00.1/М/ ВК-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 14 / 12

Розподіл балів за виконання завдань під час навчальних занять

З метою застосування цілих чисел для оцінювання активностей здобувачів вищої освіти під час навчальних занять протягом семестру використовується 100-бальна шкала оцінювання кожного окремо виду робіт. Розрахунок набраних здобувачем вищої освіти балів за виконання завдань під час навчальних занять за семестр проводиться за формулою:

$$P_{\text{НЗ}} = (P_{\text{В100}} \times \text{ВК}_{\text{В}} + P_{\text{Уд100}} \times \text{ВК}_{\text{Уд}} + P_{\dots} \times \text{ВК}_{\dots}) \times K_{\text{НЗ}}, \quad (1)$$

де $P_{\text{НЗ}}$ – кількість набраних здобувачем вищої освіти балів за виконання завдань під час навчальних занять за семестр;

$P_{\text{В100}}$, $P_{\text{Уд100}}$, P_{\dots} – кількість набраних здобувачем вищої освіти балів за семестр відповідно за відповіді (виступи) на заняттях, за участь у дискусії, за виконання іншого виду робіт, визначеного викладачем (кожний окремо вид робіт на навчальних заняттях оцінюється за 100-бальною шкалою);

$\text{ВК}_{\text{В}}$, $\text{ВК}_{\text{Уд}}$, ВК_{\dots} – вагові коефіцієнти відповідно за відповіді (виступи) на заняттях, за участь у дискусії, за виконання іншого виду робіт, визначеного викладачем. Значення вагових коефіцієнтів розраховуються шляхом ділення кількості балів, які встановлені за виконання окремого виду робіт під час навчальних занять, на сумарну кількість балів за виконання цих робіт (дані для розрахунку вагових коефіцієнтів наведено в табл. «Розподіл балів за виконання завдань під час навчальних занять»);

$K_{\text{НЗ}}$ – коригувальний коефіцієнт, який визначається шляхом ділення кількості балів, що встановлені за виконання завдань під час навчальних занять, на 100 балів.

Якщо здобувач вищої освіти набрав за поточний контроль 60 балів або більше, він може погодити дану оцінку в електронному кабінеті і вона стане семестровою оцінкою за вивчення навчальної дисципліни.

Якщо здобувач вищої освіти під час вивчення навчальної дисципліни набрав 60 балів або більше і бажає покращити свій результат успішності, він проходить процедуру підсумкового контролю у формі заліку. За складання заліку здобувач вищої освіти може набрати 100 балів. Семестрова оцінка з навчальної дисципліни формується за результатами підсумкового контролю.

Здобувач вищої освіти допускається до процедури підсумкового контролю у формі заліку, якщо за виконання завдань поточного контролю набрав 50 балів або більше.

Якщо здобувач вищої освіти за результатами поточного контролю набрав 35–49 балів, він отримує право за власною заявою повторно опанувати окремі теми (змістові модулі) навчальної дисципліни понад обсяги, встановлені навчальним планом освітньої програми. Повторне вивчення окремих складових навчальної дисципліни понад обсяги, встановлені навчальним планом освітньої програми, здійснюється у вільний від занять здобувача вищої освіти час.

Якщо здобувач вищої освіти за результатами поточного контролю набрав від 0 до 34 балів (включно), він вважається таким, що не виконав вимоги робочої програми навчальної дисципліни та має академічну заборгованість. Здобувач вищої освіти отримує право за власною заявою повторно опанувати навчальну дисципліну у наступному семестрі понад обсяги, встановлені навчальним планом освітньої програми.

Процедура надання додаткових освітніх послуг здобувачу вищої освіти з метою повторного вивчення навчальної дисципліни чи її окремих складових частин визначена у Положенні про надання додаткових освітніх послуг здобувачам вищої освіти в Державному університеті «Житомирська політехніка».

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-22.05-05.01/ 12.00.1/М/ ВК-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 14 / 13

Визнання результатів навчання, набутих у неформальній та/або інформальній освіті

Визнання результатів навчання, набутих у неформальній та/або інформальній освіті в рамках окремих тем навчальної дисципліни, здійснюється викладачем за зверненням здобувача вищої освіти та представленням документів, які підтверджують результати навчання (сертифікати, свідоцтва, скріншоти тощо). Рішення про визнання та оцінка за відповідну частину освітнього компонента приймається викладачем за результатами співбесіди зі здобувачем вищої освіти.

Визнання результатів навчання, набутих у неформальній та/або інформальній освіті в рамках цілого освітнього компонента, здійснюється за процедурою, яка визначена у Положенні про організацію освітнього процесу у Державному університеті «Житомирська політехніка».

Шкала оцінювання

Шкала ЄКТС	Національна шкала	100-бальна шкала
A	Зараховано	90-100
B	Зараховано	82-89
C		74-81
D	Зараховано	64-73
E		60-63
FX	Не зараховано	35-59
F	Не зараховано	0-34

11. Рекомендована література

Основна література

1. Fouad Sabry. Monitoring and Surveillance Agents: Fundamentals and Applications. – Artificial Intelligence. 2022.
2. Патрік Дебуа, Джон Вілліс, Джин Кім, Джек Хамбл. DevOps. Посібник. Як домогтися гнучкості, надійності й безпеки світового рівня в технологічних компаніях. – Фабула. 2024
3. Fouad Sabry. Autonomic Networking: Fundamentals and Applications. – Artificial Intelligence. 2023.
4. P. Yosifovich, A. Ionescu, M. E. Russinovich, D. A. Solomon. Windows internals. Part 1: System architecture, processes, threads, memory management, and more. – 7th edition. – Microsoft Press, 2017.
5. E. Wilson. Windows PowerShell 3.0 Step by Step. – Microsoft, 2013.

Допоміжна література

1. A. Allievi, M. Russinovich, A. Ionescu, D. Solomon. Windows Internals. Part 2: Developer Reference. – 7th edition. – Microsoft Press, 2021.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-22.05-05.01/ 12.00.1/М/ ВК-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 14 / 14

2. G. Held. Windows Networking Tools. The Complete Guide to Management, Troubleshooting, and Security. – CRC Press, 2013.

3. O. Thomas. Windows Server 2016 Inside Out. Pearson Education, 2017.

12. Інформаційні ресурси в Інтернеті

1. How To Create And Use NAT Network In VirtualBox
<https://www.techbeatly.com/how-to-create-and-use-natnetwork-in-virtualbox/>
2. Oracle VirtualBox. Virtual Networking
<https://www.virtualbox.org/manual/ch06.html>
3. VirtualBox Network Settings: Complete Guide
<https://www.nakivo.com/blog/virtualbox-network-setting-guide/>
4. Посібник з налаштування інтернет-з'єднання в Ubuntu
<https://uk.soringprepair.com/configure-network-in-ubuntu/>
5. How to change from DHCP to Static IP address in Ubuntu 22.04
<https://linuxhint.com/change-dhcp-static-ip-address-ubuntu-22-04/>
6. Nagios Core 4.x Version History
<https://www.nagios.org/projects/nagios-core/4x/>
7. Step-by-step Installing Nagios 4 on Ubuntu 20.04 from scratch
<https://medium.com/@DevOpsfreak/step-by-step-installing-nagios-4-on-ubuntu-20-04-from-scratch-558f8fc09653>
8. Сторінка завантаження плагінів Nagios 4
<https://nagios-plugins.org/download/>
9. Nagios Vs. Icinga: the real story of one of the most heated forks in free software
http://freesoftwaremagazine.com/articles/nagios_and_icinga/
10. Nagios Add-Ons Projects
<https://www.nagios.org/downloads/nagios-core-addons/>
11. GitHub. NSClient. NagiosExchange
<https://exchange.nagios.org/directory/Addons/Monitoring-Agents/NSClient++/details>
12. GitHub. NSClient. Version history. Download page
<https://github.com/mickem/nscp/releases>
13. Installing the Windows Agent NSClient++
<https://nagiosenterprises.my.site.com/support/s/article/Installing-the-Windows-Agent-NSClient-0b485593>
14. How to Install NSClient Nagios Monitoring Agent on Windows System
<https://kifarunix.com/how-to-install-nclient-nagios-monitoring-agent-on-windows-system/>
15. Installing NSClient++
<https://nclient.org/docs/installing/>
16. How to Monitor and Configure a Windows Server Using Nagios
<https://webhostinggeeks.com/howto/how-to-monitor-and-configure-a-windows-server-using-nagios/>
17. NCPA. Downloads latest stable agent
<https://www.nagios.org/ncpa/#downloads>
18. Installing NCPA
https://nagiosenterprises.my.site.com/support/s/article/Installing-NCPA-9f1de62f#Installing_NCPA_On_Windows
19. NCPA. Getting Started
<https://www.nagios.org/ncpa/getting-started.php>

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015			Ф-22.05-05.01/ 12.00.1/М/ ВК-1-2024
	Випуск 1	Зміни 0	Екземпляр № 1	Арк 14 / 15

20. Download check_ncpa.py
https://raw.githubusercontent.com/NagiosEnterprises/ncpa/master/client/check_ncpa.py
21. Nagios Plugins Downloads
<https://nagios-plugins.org/downloads/>
22. GitHub. NagiosEnterprises/ncpa
<https://github.com/NagiosEnterprises/ncpa>
23. GitHub. NagiosEnterprises/ncpa/"free disk space"
<https://github.com/NagiosEnterprises/ncpa/issues/857>
24. Nagios Support Knowledgebase. Network Interface Checks
<https://support.nagios.com/kb/article/network-interface-checks-781.html>
25. NRPE - How To Install NRPE v4 From Source
<https://support.nagios.com/kb/article/nrpe-how-to-install-nrpe-v4-from-source-515.html>
26. NRPE - How to install NRPE
<https://support.nagios.com/kb/article/nrpe-how-to-install-nrpe-8.html>
27. Index of /downloads/nagiosxi/agents
<https://assets.nagios.com/downloads/nagiosxi/agents/>
28. Exchange Nagios. NRPE - Nagios Remote Plugin Executor
<https://exchange.nagios.org/directory/Addons/Monitoring-Agents/NRPE--2D-Nagios-Remote-Plugin-Executor/details>
29. Using NSClient++ with check_nrpe
<https://nsclient.org/docs/howto/nrpe/>
30. The Nagios Plugins. Category: Operating Systems
<https://exchange.nagios.org/directory/Plugins/Operating-Systems>
31. Nagios Core. Time Periods.
<https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/timeperiods.html>
32. Nagios Core. Time Period Definition
<https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/objectdefinitions.html#timeperiod>
33. Nagios Core. CGI Configuration File Options
<https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/configcgi.html>
34. How to Install and Use SendEmail on Linux
<https://tecadmin.net/how-to-install-sendemail-in-linux/>
35. NagiosQL - Nagios configuration tool Files
<https://sourceforge.net/projects/nagiosql/files/nagiosql/>