

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.05-05.01/ 123.00.1/М/ ОК8-2023
	Екземпляр № 1	Арк 1/10

ЗАТВЕРДЖЕНО

Вченою радою факультету
факультету інформаційно-
комп'ютерних технологій

28 серпня 2023 р., протокол № 5

Голова Вченої ради

Тетяна НІКІТЧУК

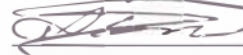


РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ОК 8 «ТЕХНОЛОГІЇ АДМІНІСТРУВАННЯ ТА ЗАХИСТУ ІНФОРМАЦІЙНИХ СИСТЕМ»


для здобувачів вищої освіти освітнього ступеня «магістр»
спеціальності 123 «Комп'ютерна інженерія»
освітньо-професійна програма «Комп'ютерна інженерія»
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

 Ігор ПУЛЕКО

Розробник: кандидат педагогічних наук, доцент кафедри комп'ютерної інженерії та кібербезпеки Олена ГОЛОВНЯ

Житомир
2023 – 2024 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/ 123.00.1/М/ ОК8-2023
	Екземпляр № 1	Арк 2/10

1. Опис навчальної дисципліни

Найменування показників	Галузь знань, спеціальність освітній ступінь	Характеристика навчальної дисципліни	
		денна форма навчання	заочна форма навчання
Кількість кредитів – 4	Галузь знань: 12 Інформаційні технології	Нормативна	
Модулів – 1	Спеціальність 123 Комп'ютерна інженерія	Рік підготовки:	
Змістових модулів – 2		I	I
Загальна кількість годин – 120		Семестр	
		1-й	1-й
Тижневих годин для денної форми навчання денна форма: аудиторних – 4 самостійної роботи – 3,5 заочна форма: аудиторних – 1 самостійної роботи – 6,5	Освітній ступінь «Магістр»	Лекції	
		32 год.	6 год.
		Практичні	
		–	–
		Лабораторні	
		32 год.	6 год.
		Самостійна робота	
		56 год.	108 год.
Вид контролю:			
екзамен			

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

для денної форми навчання – 53% аудиторних занять, 47% самостійної та індивідуальної роботи;

для заочної форми навчання – 10% аудиторних занять, 90% 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/ 123.00.1/М/ ОК8-2023
	Екземпляр № 1	Арк 3/10

2. Мета та завдання навчальної дисципліни

Метою навчальної дисципліни є розвиток компетентностей здобувачів освіти, пов'язаними з адмініструванням комп'ютерних систем та мереж на базі ОС Windows.

Завданнями вивчення навчальної дисципліни є:

– поглиблення та доповнення в здобувачів освіти теоретичних знань про будову та функціонування систем та мереж на основі ОС Windows;

– розвиток у здобувачів освіти навичок управління ОС Windows (зокрема, засобами Active Directory і групових політик) та організації її захисту.

Зміст навчальної дисципліни направлений на формування наступних **компетентностей**, визначених стандартом вищої освіти зі спеціальності 123 «Комп'ютерна інженерія»:

загальних:

КЗ-1. Здатність до адаптації та дій в новій ситуації.

КЗ-2. Здатність до абстрактного мислення, аналізу і синтезу.

КЗ-3. Здатність проводити дослідження на відповідному рівні.

КЗ-4. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

КЗ-5. Здатність генерувати нові ідеї (креативність).

КЗ-6. Здатність виявляти, ставити та вирішувати проблеми.

КЗ-7. Здатність приймати обґрунтовані рішення.

КЗ-8. Здатність спілкуватися іноземною мовою.

фахових:

КФ-1. Здатність до визначення технічних характеристик, конструктивних особливостей, застосування і експлуатації програмних, програмно-технічних засобів, комп'ютерних систем та мереж різного призначення.

КФ-2. Здатність розробляти алгоритмічне та програмне забезпечення, компоненти комп'ютерних систем та мереж, Інтернет додатків, кіберфізичних систем з використанням сучасних методів і мов програмування, а також засобів і систем автоматизації проектування.

КФ-3. Здатність проектувати комп'ютерні системи та мережі з урахуванням цілей, обмежень, технічних, економічних та правових аспектів.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.05-05.01/ 123.00.1/М/ ОК8-2023
	Екземпляр № 1	Арк 4/10

КФ-4. Здатність будувати та досліджувати моделі комп'ютерних систем та мереж.

КФ-5. Здатність будувати архітектуру та створювати системне і прикладне програмне забезпечення комп'ютерних систем та мереж.

КФ-6. Здатність використовувати та впроваджувати нові технології, включаючи технології розумних, мобільних, зелених і безпечних обчислень, брати участь в модернізації та реконструкції комп'ютерних систем та мереж, різноманітних вбудованих і розподілених додатків, зокрема з метою підвищення їх ефективності.

КФ-7. Здатність досліджувати, розробляти та обирати технології створення великих і надвеликих систем.

КФ-8. Здатність забезпечувати якість продуктів і сервісів інформаційних технологій на протязі їх життєвого циклу.

КФ-9. Здатність представляти результати власних досліджень та/або розробок у вигляді презентацій, науково-технічних звітів, статей і доповідей на науково-технічних конференціях.

КФ-10. Здатність ідентифікувати, класифікувати та описувати роботу програмно-технічних засобів, комп'ютерних систем, мереж та їхніх компонентів;

КФ-11. Здатність обирати ефективні методи розв'язування складних задач комп'ютерної інженерії, критично оцінювати отримані результати та аргументувати прийняті рішення.

Отримані знання з навчальної дисципліни стануть складовими наступних **програмних результатів** навчання за спеціальністю 123 «Комп'ютерна інженерія»:

РН-1. Застосовувати загальні підходи пізнання, методи математики, природничих та інженерних наук до розв'язання складних задач комп'ютерної інженерії.

РН-2. Знаходити необхідні дані, аналізувати та оцінювати їх.

РН-3. Будувати та досліджувати моделі комп'ютерних систем і мереж, оцінювати їх адекватність, визначати межі застосовності.

РН-4. Застосовувати спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері комп'ютерної інженерії, необхідні для професійної діяльності, оригінального мислення та проведення досліджень, критичного осмислення проблем інформаційних технологій та на межі галузей знань.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.05-05.01/ 123.00.1/М/ ОК8-2023
	Екземпляр № 1	Арк 5/10

РН-5. Розробляти і реалізовувати проекти у сфері комп'ютерної інженерії та дотичні до неї міждисциплінарні проекти з урахуванням інженерних, соціальних, економічних, правових та інших аспектів.

РН-6. Аналізувати проблематику, ідентифікувати та формулювати конкретні проблеми, що потребують вирішення, обирати ефективні методи їх вирішення.

РН-7. Вирішувати задачі аналізу та синтезу комп'ютерних систем та мереж.

РН-8. Застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп'ютерних систем та мереж для вирішення складних задач комп'ютерної інженерії та дотичних проблем.

РН-11. Приймати ефективні рішення з питань розроблення, впровадження та експлуатації комп'ютерних систем і мереж, аналізувати альтернативи, оцінювати ризики та імовірні наслідки рішень.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.05-05.01/ 123.00.1/М/ ОК8-2023
	Екземпляр № 1	Арк 6/10

3. Програма навчальної дисципліни

Модуль 1. АДМІНІСТРУВАННЯ ТА ЗАХИСТ КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ

Змістовий модуль 1. Базові засоби керування ОС Windows

Тема 1. Ключові компоненти за засоби ОС Windows

Робота у командній оболонці CMD. Структура файлів у Windows. Файлові дозволи у Windows. Робота у командній оболонці PowerShell. Робота з системним реєстром. Керування службами Windows. Планування завдань за допомогою інструмента Task Scheduler. Файлові асоціації у Windows. Управління програмним забезпеченням у Windows.

Тема 2. Автентифікація та контроль доступу в ОС Windows

Протокол автентифікації NTLM. Одержання хешів від процесу LSA (Local Security Authority). Локальна та віддалена автентифікація у Windows. Керування доступом в Active Directory. Організація спільного доступу до ресурсів на базі протоколу SMB. Об'єкти групової політики (group policy objects, GPO) в Active Directory.

Тема 3. Журнали подій у Windows

Регулярні вирази та їх застосування на платформі Splunk. Робота з журналами подій за допомогою інструменту Event Logs. Збереження журналів подій командної оболонки PowerShell. Перескерування журналів подій у Splunk. Робота з журналами подій засобами Sysmon.

Змістовий модуль 2. Засоби керування безпекою ОС Windows

Тема 4. Інфраструктура публічних ключів у Windows

Знайомство з інфраструктурою публічних ключів (public key infrastructure, PKI). Шаблони веб-сертифікатів PKI. Використання серверу сертифікації Web Server Cert для вебсайту на базі IIS. Безпека і сертифікація скриптів PowerShell.

Тема 5. Безпека систем та мереж на базі ОС Windows

Хмарні безпекові рішення для Windows. Можливості Azure Active Directory. Розгортання захисту робочих станцій на базі Wazuh Agent. Вбудований антивірусний компонент Захисник Windows (Windows Defender). Керування безпекою у середовищі Microsoft 365.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.05-05.01/ 123.00.1/М/ ОК8-2023
	<i>Екземпляр № 1</i>	<i>Арк 7/10</i>

Тема 6. Додаткові питання безпеки ОС Windows

Розширені можливості Sysmon (CaptureClipboard, виявлення застосування зловмисником техніки process injection). Виявлення та усунення слабких паролів користувачів Active Directory. Виявлення атаки Pass-the-Hash під час автентифікації за допомогою NTLM. Відстеження шкідливих процесів у Windows.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.05-05.01/ 123.00.1/М/ ОК8-2023
	Екземпляр № 1	Арк 8/10

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. Базові засоби керування ОС Windows								
Тема 1. Ключові компоненти за засоби ОС Windows	20	6	6	8	20	1	0	19
Тема 2. Автентифікація та контроль доступу в ОС Windows	20	5	6	9	20	2	2	16
Тема 3. Журнали подій у Windows	20	5	4	11	20	0	0	20
Разом за змістовий модуль 1	60	16	16	28	60	3	2	55
Змістовий модуль 2. Засоби керування безпекою ОС Windows								
Тема 4. Інфраструктура публічних ключів у Windows	20	6	2	12	20	1	2	17
Тема 5. Безпека систем та мереж на базі ОС Windows	20	6	4	10	20	2	0	18
Тема 6. Додаткові питання безпеки ОС Windows	20	4	10	6	20	0	2	18
Разом за змістовий модуль 2	60	16	16	28	60	3	4	53
ВСЬОГО	120	32	32	56	120	6	6	108

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.05-05.01/ 123.00.1/М/ ОК8-2023
	Екземпляр № 1	Арк 9/10

5. Темі практичних (лабораторних) занять

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	Лабораторна робота №1. Робота з файлами у CMD та PowerShell	1	0
2	Лабораторна робота №2. Дослідження файлових дозволів у Windows	1	0
3	Лабораторна робота №3. Додаткові прийоми роботи з системним реєстром	1	0
4	Лабораторна робота №4. Керування службами у Windows	1	0
5	Лабораторна робота №5. Керування файловими розширеннями у Windows	1	0
6	Лабораторна робота №6. Управління програмним забезпеченням у Windows	1	0
7	Лабораторна робота №7. Робота з протоколом автентифікації NTLM в Active Directory	2	2
8	Лабораторна робота №8. Керування доступом в Active Directory	2	0
9	Лабораторна робота №9. Використання регулярних вирахів у Splunk	2	0
10	Лабораторна робота №10. Робота з журналами подій	2	0
11	<i>Модульна контрольна робота №1</i>	2	0
12	Лабораторна робота №11. Робота з сертифікатами РКІ	2	2
13	Лабораторна робота №12. Розгортання захисту робочих станцій на базі Wazuh Agent	2	0
14	Лабораторна робота №13. Робота з Захисником Windows (Windows Defender)	2	0
15	Лабораторна робота №14. Розширені можливості Sysmon	2	0
16	Лабораторна робота №15. Додаткові безпекові питання Active Directory	2	2
17	Лабораторна робота №16. Відстеження шкідливих процесів у Windows	4	0
18	<i>Модульна контрольна робота №2</i>	2	0
РАЗОМ		32	6

6. Завдання для самостійної роботи

У межах самостійної роботи передбачене проходження здобувачами освіти електронного онлайн курсу Microsoft Security Core (Learning Path: Microsoft Security Core) на базі освітньої платформи Rangeforce. Здійснюється опрацювання здобувачами освіти теоретичних матеріалів, виконання ними практичних завдань та проходження контрольних заходів курсу. Результати підсумкових контрольних заходів курсу Microsoft Security Core враховуються під час обчислення рейтингового балу студента.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.05-05.01/ 123.00.1/М/ ОК8-2023
	Екземпляр № 1	Арк 10/10

7. Індивідуальні 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. Розподіл балів

Нарахування балів здійснюється за наступною схемою. 60 балів виділяється на поточне оцінювання в межах модулів, 40 балів – на модульний контроль. 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

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.05-05.01/ 123.00.1/М/ ОК8-2023
	Екземпляр № 1	Арк 11/10

11. Рекомендована література

Основна література

1. 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.
2. 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.
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. Курс «Технології адміністрування та захисту інформаційних систем» – Державний університет "Житомирська політехніка" – Освітній портал. URL: <https://learn.ztu.edu.ua/course/view.php?id=2844>.
2. RangeForce – Team Cyber Readiness. URL: <https://www.rangeforce.com>
3. Developer tools, technical documentation and coding examples – Microsoft Docs. URL: <https://docs.microsoft.com/en-us/>.
4. Stack Exchange. URL: <https://stackexchange.com/>.