ЗАТВЕРДЖЕНО

Вченою радою
факультету інформаційно-
комп'ютерних технологій
31 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 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: кандидат педагогічних наук, доцент, доцент кафедри комп'ютерної інженерії та кібербезпеки Олена ГОЛОВНЯ

Житомир
2023 – 2024 н.р.

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань,
спеціальність
освітній ступінь</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td>Кількість кредитів – 4</td><td>Галузь знань:
12 Інформаційні технології</td><td colspan="2">Нормативна</td></tr>
<tr><td>Модулів – 1</td><td rowspan="5">Спеціальність
125 Кібербезпека та захист інформації</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td rowspan="2">Змістових модулів – 2</td><td>I</td><td>I</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 120</td><td>1-й</td><td>1-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="10">Тижневих годин для денної форми навчання

денна форма:
аудиторних – 4
самостійної роботи – 3,5

заочна форма:
аудиторних – 1
самостійної роботи – 6,5</td><td rowspan="10">Освітній ступінь «Магістр»</td><td>32 год.</td><td>6 год.</td></tr>
<tr><td colspan="2">Практичні</td></tr>
<tr><td>–</td><td>–</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>32 год.</td><td>6 год.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>56 год.</td><td>108 год.</td></tr>
<tr><td colspan="2">Вид контролю:</td></tr>
<tr><td colspan="2">екзамен</td></tr>
</table>

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.

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 125 «Кібербезпека та захист інформації»:

КЗ1. Здатність застосовувати знання у практичних ситуаціях.

КФ-1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.

КФ-3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

КФ-6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ-8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ-9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.

Отримані знання з навчальної дисципліни стануть складовими наступних **програмних результатів** навчання за спеціальністю 125 «Кібербезпека»:

РН-2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.

РН-4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

РН-6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

РН-7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

РН-8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

РН-10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

РН-11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

РН-13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.

РН-14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.

РН-16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.

РН-20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.

РН-21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

РН-23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

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.

Тема 6. Додаткові питання безпеки ОС Windows

Розширені можливості Sysmon (CaptureClipboard, виявлення застосування зловмисноком 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.

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**

5. Теми 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	*Модульна контрольна робота №1*	2	0
12	Лабораторна робота №11. Робота з сертифікатами PKI	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	*Модульна контрольна робота №2*	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.

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

11. Рекомендована література

Основна література

1. P. Yosifovich, A. Ionesku, 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/.