ВІННИЦЬКИЙ ДЕРЖАВНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ МИХАЙЛА КОЦЮБИНСЬКОГО

Факультет педагогіки, психології і професійної освіти

Кафедра цифрових технологій і професійної освіти

ЗАТВЕРДЖУЮ
Перший проректор
з науково-педагогічної роботи
_____ проф. Блажко О. А.
«31» 08 2026 р.

РОБОЧА ПРОГРАМА ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«СИСТЕМНЕ АДМІНІСТРУВАННЯ ТА БЕЗПЕКА ІНФОРМАЦІЙНИХ ОСВІТНІХ СИСТЕМ»

підготовки	магістра
галузі знань	А Освіта
спеціальності	А5 Професійна освіта (за спеціалізаціями) Спеціалізація А5.39 Цифрові технології
Освітньо-професійна програма	Професійна освіта. Комп'ютерні технології в управлінні та навчанні

Факультет педагогіки, психології і професійної освіти

Вінниця – 2026 рік

Робоча програма обов'язкової навчальної дисципліни «Системне адміністрування та безпека інформаційних освітніх систем» для здобувачів вищої освіти за спеціальністю А5 Професійна освіта (за спеціалізаціями), спеціалізацією А5.39 Цифрові технології.
Освітньо-професійна програма: Професійна освіта. Комп'ютерні технології в управлінні та навчанні.

Мова навчання: *українська*

«31» серпня 2026 р. 18 с.

Розробник:

Уманець Володимир Олександрович – доцент кафедри цифрових технологій і професійної освіти, кандидат педагогічних наук

Робоча програма розглянута і схвалена на засіданні кафедри цифрових технологій і професійної освіти

Протокол від «31» 08 2026 року № 1

Завідувач кафедри цифрових технологій і професійної освіти _____ доц. Кобися В.М.

«31» 08 2026 року

Робоча програма розглянута і схвалена на засіданні навчально-методичної комісії Факультету педагогіки, психології і професійної освіти

Протокол від «31» 08 2026 року № 1

Голова НМК _____ проф. Волошина О.В.

«31» 08 2026 року

Погоджено:

Гарант освітньої програми _____ доц. Кізім С.С.

«31» 08 2026 року

1. Опис навчальної дисципліни

<table>
<tr><th rowspan="2">Найменування показників</th><th rowspan="2">Галузь знань, спеціальність, предметна спеціальність, спеціалізація, додаткова спеціалізація/спеціальність / предметна спеціальність, освітня (освітньо-професійна або освітньо-наукова) програма, ступінь вищої освіти</th><th colspan="2">Характеристика навчальної дисципліни</th></tr>
<tr><td>денна форма здобуття освіти</td><td>заочна форма здобуття освіти</td></tr>
<tr><td rowspan="2">Загальна кількість кредитів – 3
Кількість кредитів на поточний навчальний рік – 3</td><td>Галузь знань А Освіта</td><td colspan="2" rowspan="2">Обов’язкова</td></tr>
<tr><td rowspan="5">А5 Професійна освіта (за спеціалізаціями)
Спеціалізація А5.39 Цифрові технології
Освітньо-професійна програма: Професійна освіта. Комп’ютерні технології в управлінні та навчанні</td></tr>
<tr><td>Індивідуальне навчально-дослідне завдання (ІНДЗ) – 10 год. сам. роб.</td><td colspan="2">РІК НАВЧАННЯ:</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 90
Кількість годин на поточний навчальний рік – 90
Кількість годин на 1 семестр – 90</td><td colspan="2">2-й</td></tr>
<tr><td colspan="2">СЕМЕСТР</td></tr>
<tr><td rowspan="11">Тижневих годин для денної форми здобуття освіти:

аудиторних – 2
самостійної роботи здобувача – 3</td><td rowspan="11">Ступінь вищої освіти магістр</td><td colspan="2">3-й</td></tr>
<tr><td colspan="2">ЛЕКЦІЇ</td></tr>
<tr><td>12 год.</td><td>4 год.</td></tr>
<tr><td colspan="2">ПРАКТИЧНІ ЗАНЯТТЯ</td></tr>
<tr><td>0 год.</td><td>0 год.</td></tr>
<tr><td colspan="2">ЛАБОРАТОРНІ ЗАНЯТТЯ</td></tr>
<tr><td>18 год.</td><td>6 год.</td></tr>
<tr><td colspan="2">ІНДИВІДУАЛЬНІ ЗАНЯТТЯ</td></tr>
<tr><td>0 год.</td><td>0 год.</td></tr>
<tr><td colspan="2">САМОСТІЙНА РОБОТА</td></tr>
<tr><td>60 год.</td><td>80 год</td></tr>
<tr><td colspan="2">ВИД КОНТРОЛЮ:
екзамен</td></tr>
</table>

Примітка.
Співвідношення кількості годин аудиторних занять до самостійної та індивідуальної роботи (%) становить:

для денної форми здобуття освіти – 30%:70%,
для заочної форми здобуття освіти – 10%:90%.

2. Мета, завдання, компетентності та результати навчання

2.1. Метою вивчення навчальної дисципліни **«Системне адміністрування та безпека інформаційних освітніх систем»** є формування у здобувачів вищої освіти цілісної системи фундаментальних теоретичних знань, професійних умінь і практичних навичок щодо комплексного системного адміністрування сучасних інформаційних освітніх систем (ІОС), конфігурування серверних і мережевих служб, розгортання хмарних і віртуалізованих платформ, а також побудови надійних багаторівневих систем кібербезпеки, дотримання корпоративної кібергігієни та ефективного захисту конфіденційної інформації й персональних даних в умовах цифрової трансформації освітнього простору.

2.2. Основними завданнями вивчення навчальної дисципліни «Системне адміністрування та безпека інформаційних освітніх систем» є:

– формування глибоких знань щодо архітектури, принципів системної організації, функціонування та супроводу інформаційних систем закладів вищої, фахової передвищої та професійної освіти;

– опанування практичних технологій розгортання, конфігурування й адміністрування серверних операційних систем (Linux, Windows Server), служб каталогів (Active Directory, LDAP), доменних сервісів та баз даних освітніх платформ;

– засвоєння методології впровадження технологій віртуалізації (Hyper-V, Proxmox VE), контейнеризації (Docker) та інтеграції корпоративних хмарних середовищ (Google Workspace for Education, Microsoft 365 Education);

– вивчення нормативно-правової бази кібербезпеки України та міжнародних стандартів захисту персональних даних (GDPR, вимоги Держспецзв'язку);

– набуття практичних умінь із налаштування мережевого захисту, систем міжмережевого екранування (Firewall), виявлення та запобігання вторгненням (IDS/IPS), організації захищених VPN-каналів зв’язку;

– розроблення та реалізація регламентів резервного копіювання даних (Backup) за правилом 3-2-1 та планів безперервності функціонування освітніх систем і відновлення після аварій (Disaster Recovery Plan);

– формування культури корпоративної кібергігієни та навичок протидії загрозам соціальної інженерії й фішингу;

– опанування інструментів цілодобового моніторингу працездатності інфраструктури (Zabbix, Prometheus, Grafana) та автоматизації служби технічної підтримки (Helpdesk);

– дослідження та прикладне використання технологій штучного інтелекту (ШІ) та алгоритмів машинного навчання для автоматизованого виявлення кібератак, системного моніторингу та оптимізації освітніх процесів.

2.3. **Пререквізити**: базові знання, уміння та сформовані компетентності з інформаційно-комунікаційних технологій, архітектури обчислювальних систем, комп’ютерних мереж, вебтехнологій, основ інформаційної безпеки, технологій роботи інформаційних центрів, педагогіки та методики професійної освіти, набуті під час вивчення суміжних дисциплін.

Постреквізити: результати навчання, сформовані в процесі опанування дисципліни, є теоретичною, технологічною та інструментальною основою для проходження педагогічної практики, а також для якісного виконання, апробації та захисту кваліфікаційної роботи.

2.4. Компетентності

2.4.1. Інтегральна компетентність

ІК. Здатність розв'язувати задачі дослідницького та/або інноваційного характеру і проблеми у професійній освіті.

2.4.2. Загальні компетентності

ЗК 1. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК 2. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ЗК 4. Здатність працювати в міжнародному контексті.

ЗК 7. Здатність до міжособистісної взаємодії.

2.4.3. Фахові компетентності

СК 1. Здатність застосовувати і розробляти нові підходи до вирішення задач дослідницького та/або інноваційного характеру і проблем професійної освіти.

СК 3. Здатність застосовувати і створювати нові освітні інструменти і технології та інтегрувати їх в освітнє середовище професійної освіти.

СК 4. Здатність аналізувати, прогнозувати, критично осмислювати проблеми у професійній освіті, приймати ефективні рішення щодо їх розв'язання.

СК 7. Навички консультування у сфері професійної освіти.

2.5. Результати навчання за освітньою програмою

РН 2. Ефективно використовувати сучасні цифрові інструменти, інформаційні технології та ресурси у професійній, інноваційній та/або дослідницькій діяльності.

РН 7. Створювати освітнє середовище професійної освіти, що є сприятливим для здобувачів освіти і забезпечує досягнення визначених результатів навчання.

РН 8. Здійснювати у науковій та професійній літературі, базах даних, інших джерелах пошук необхідної інформації з професійної освіти і дотичних питань, систематизувати, аналізувати та оцінювати відповідну інформацію.

РН 9. Будувати і досліджувати моделі процесів у галузі професійної освіти.

РН 10. Здійснювати консультативну діяльність у сфері професійної освіти.

3. Програма навчальної дисципліни

Розділ 1. Системне адміністрування та інфраструктура інформаційних освітніх систем.

Тема 1. Архітектура, структура та системна організація інформаційних освітніх систем (ІОС).

Поняття та багаторівнева структура сучасної інформаційної освітньої системи закладу вищої та професійної освіти. Класифікація підсистем: навчально-методична, управлінська, комунікаційна, дослідницька та безпекова. Системний підхід до організації ІТ-інфраструктури. Ролі, функціональні обов'язки та професійні стандарти системного адміністратора освітнього закладу. Стандартизація та сумісність інформаційних освітніх сервісів. Нормативне регулювання цифровізації закладів освіти.

Тема 2. Адміністрування серверних операційних систем та мережевих служб в освітньому закладі.

Серверні ОС у системі освіти: сімейства Linux (Ubuntu Server, Debian) та Windows Server. Процеси завантаження, конфігурування системних служб (systemd), управління пакетами та репозитаріями. Служби каталогів Active Directory Domain Services (AD DS) та OpenLDAP: структура лісу, доменів, організаційних підрозділів (OU). Управління груповими політиками (GPO), автоматизація створення та синхронізації облікових записів здобувачів освіти і викладачів. Базові мережеві служби: DNS, DHCP, NTP.

Тема 3. Технології віртуалізації, контейнеризації та мікросервісів в освітніх системах.

Апаратна та програмна віртуалізація. Гіпервізори першого типу (Bare-Metal): Proxmox VE, VMware ESXi, KVM. Створення, міграція та резервування віртуальних машин. Контейнеризація на базі Docker: концепція образів, контейнерів, томів та мереж. Оркестрація мікросервісів за допомогою Docker Compose та Kubernetes. Розгортання ізольованих цифрових навчальних лабораторій та середовищ для тестування знань.

Тема 4. Хмарні технології та гібридна інфраструктура управління освітнім процесом.

Моделі хмарних сервісів (IaaS, PaaS, SaaS) у навчальному процесі. Платформи Google Workspace for Education та Microsoft 365 Education: адміністрування хмарного домену, політики доступу, сховища даних, сервіси онлайн-комунікацій. Гібридні середовища: синхронізація локальної Active Directory з хмарою (Azure AD Connect, Google Cloud Directory Sync). Технології єдиної точки входу (Single Sign-On, SSO), протоколи автентифікації SAML 2.0 та OAuth 2.0/OpenID Connect.

Тема 5. Адміністрування платформ електронного навчання (LMS) та баз даних освітніх систем.

Системи управління навчанням: архітектура та встановлення LMS Moodle. Конфігурування зв'язки LAMP/LEMP, оптимізація вебсервера (Nginx/Apache), налаштування PHP-FPM. Адміністрування систем керування базами даних (PostgreSQL, MySQL/MariaDB): індексація, оптимізація запитів, захист баз даних. Налаштування підсистем кешування (Redis, Memcached) для високонавантажених освітніх порталів. Інтеграція LMS з автоматизованими системами управління контингентом здобувачів освіти.

Розділ 2. Кібербезпека, кібергігієна та захист цифрового освітнього середовища.

Тема 6. Загрози інформаційній безпеці, вразливості та нормативно-правова база кіберзахисту в освіті.

Сучасний ландшафт кіберзагроз для освітньої галузі: цільові атаки (APT), фішинг, шкідливе програмне забезпечення, атаки програм-вимагачів (Ransomware), витік конфіденційної інформації, внутрішні загрози. Аналіз та класифікація вразливостей (CVE, база CVSS). Законодавство України у сфері кібербезпеки: Закони України «Про основні засади забезпечення кібербезпеки України», «Про захист інформації в інформаційно-комунікаційних системах». Побудова Комплексних систем захисту інформації (КСЗІ) в освітніх установах. Стандарти ISO/IEC 27001 та NIST Cybersecurity Framework.

Тема 7. Мережева безпека освітніх систем та сегментація трафіку.

Концепція глибокого ешелонованого захисту мережі (Defense-in-Depth). Програмні та апаратні міжмережеві екрани (Firewall: pfSense, OPNsense, iptables/nftables). Сегментація освітніх мереж за допомогою віртуальних локальних мереж (VLAN): ізоляція адміністративного, навчального та гостьового сегментів. Організація захищеного віддаленого доступу засобами VPN (IPsec, OpenVPN, WireGuard). Системи виявлення та запобігання вторгненням (IDS/IPS: Suricata, Snort). Безпека бездротових мереж Wi-Fi закладу освіти: WPA3-Enterprise, автентифікація через RADIUS-сервер (802.1X).

Тема 8. Резервне копіювання, забезпечення відмовостійкості та відновлення освітніх систем після збоїв

Стратегії збереження даних та забезпечення неперервності освітнього процесу (Business Continuity Planning). Політика резервного копіювання за золотим правилом 3-2-1. Типи резервного копіювання: повне (Full), інкрементне (Incremental), диференційне (Differential). Системи автоматизованого резервування (Bacula, Proxmox Backup Server, Veeam). Планування та тестування процедур аварійного відновлення після катастроф (Disaster Recovery Plan, DRP). Розрахунок показників RPO (Recovery Point Objective) та RTO (Recovery Time Objective). Захист резервних копій від модифікації та шифрування зловмисниками (незмінні репозитарії).

Тема 9. Корпоративна кібергігієна, захист персональних даних та цифрової ідентичності в закладі освіти

Захист персональних даних здобувачів вищої освіти, викладачів та персоналу відповідно до Закону України «Про захист персональних даних» та положень General Data Protection Regulation (GDPR). Цифровий слід та цифрова ідентичність учасників освітнього процесу. Формування культури корпоративної кібергігієни в академічному колективі: політика стійких паролів, використання корпоративних менеджерів паролів, захист від атак соціальної інженерії та фішингових розсилок. Багатофакторна автентифікація (MFA/2FA), використання апаратних ключів захисту (FIDO2/WebAuthn), застосування кваліфікованого електронного підпису (КЕП) та цифрових сертифікатів.

Тема 10. Системний моніторинг, реагування на інциденти та застосування штучного інтелекту в кібербезпеці освітніх систем

Цілодобовий моніторинг стану інфраструктури: метрики продуктивності та доступності серверів і сервісів (Zabbix, Prometheus, Grafana). Централізований збір, парсинг та аналіз журналів подій (SIEM/Log Management: стек Elasticsearch-Logstash-Kibana / OpenSearch, Wazuh). Регламенти реєстрації, класифікації та реагування на інциденти кібербезпеки (CSIRT/CERT-UA). Застосування штучного інтелекту та машинного навчання в системному адмініструванні й безпеці: автоматизоване виявлення аномалій у мережевому трафіку, інтелектуальний аналіз поведінки користувачів (UEBA), прогнозування навантаження на сервери. Етичні та безпекові виклики використання генеративного штучного інтелекту в освітньому процесі та захист від новітніх ШІ-загроз.

4. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин											
	денна форма здобуття освіти						заочна форма здобуття освіти					
	усього	зокрема					усього	зокрема				
		ЛК	**ПЗ**	**ЛЗ**	**ІЗ**	**С.Р.**		**ЛК**	**ПЗ**	**ЛЗ**	**ІЗ**	**С.Р.**
1	2	3	4	5	6	7	8	9	10	11	12	13
Розділ 1. Системне адміністрування та інфраструктура ІОС												
Тема 1. Архітектура, структура та системна організація ІОС	9	2		2		6	9	2		2		8
Тема 2. Адміністрування серверних ОС та мережевих служб	8			2		6	9					8
Тема 3. Технології віртуалізації, контейнеризації та мікросервісів	8	2				6	9					8
Тема 4. Хмарні технології та гібридна інфраструктура в освіті	9			2		6	9					8
Тема 5. Адміністрування платформ електронного навчання (LMS)	10	2		2		6	8					8
Разом за 1 розділом	**44**	**6**		**8**		**30**	**44**	**2**		**2**		**40**
Розділ 2. Кібербезпека, кібергігієна та захист освітнього середовища												
Тема 6. Загрози інформаційній безпеці та нормативна база кіберзахисту	**9**	**2**		**2**		**6**	**10**	**2**		**2**		**8**
Тема 7. Мережева безпека освітніх систем та сегментація трафіку	**9**			**2**		**6**	**9**					**8**
Тема 8. Резервне копіювання, відмовостійкість та відновлення (DRP)	**9**	**2**		**2**		**6**	**9**			**2**		**8**
Тема 9. Корпоративна кібергігієна та захист персональних даних	**9**			**2**		**6**	**9**					**8**
Тема 10. Системний моніторинг, інциденти та штучний інтелект	**10**	**2**		**2**		**6**	**9**					**8**
Разом за розділом 2	**46**	**6**		**10**		**30**	**46**	**2**		**4**		**40**
Усього годин	**90**	**12**		**18**		**60**	**90**	**4**		**6**		**80**

5. Теми лекцій

№ з/п	Назва лекційного заняття	Кількість годин	
		Денна форма здобуття освіти	*Заочна форма здобуття освіти*
1.	Архітектура, нормативно-правове регулювання та системна організація сучасних ІОС	2	
2.	Адміністрування серверних систем та служб каталогів (AD DS / LDAP) в освітніх закладах		2
3.	Технології віртуалізації (Proxmox, Hyper-V) та контейнеризації (Docker) в освіті	2	
4.	Хмарні освітні платформи, гібридна інфраструктура та технології єдиної точки входу (SSO)		
5.	Адміністрування платформ електронного навчання (LMS)	2	
6.	Загрози інформаційній безпеці, побудова КСЗІ та нормативні стандарти захисту інформації	2	2
7.	Мережевий захист: міжмережеві екрани, сегментація VLAN, безпека бездротових мереж та VPN		
8.	Резервне копіювання, корпоративна кібергігієна та штучний інтелект у моніторингу безпеки	2	
9.	Корпоративна кібергігієна та захист персональних даних		
10.	Системний моніторинг, інциденти та штучний інтелект	2	
Усього годин		12	4

6. Теми практичних занять

(навчальним планом не передбачено)

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин	
		Денна форма здобуття	*Заочна форма здобуття*
1.	Розгортання та первинне налаштування серверної ОС Linux (Ubuntu/Debian) та служб DNS/DHCP	2	
2.	Розгортання контролера домену та централізоване управління Active Directory / OpenLDAP	2	2
3.	Встановлення та адміністрування гіпервізора віртуалізації першого типу Proxmox VE	2	
4.	Контейнеризація та розгортання освітніх сервісів за допомогою Docker та Docker Compose	2	
5.	Розгортання, оптимізація та системний аудит вебсервера LMS Moodle і СКБД PostgreSQL	2	

6.	Налаштування міжмережевого екрана (iptables/pfSense) та сегментація локальної мережі (VLAN)	2	2
7.	Організація захищеного віддаленого доступу до сервісів закладу засобами VPN (WireGuard/OpenVPN)	2	
8.	Автоматизація багаторівневого резервного копіювання за правилом 3-2-1 та сценарії аварійного DRP	2	2
9.	Розгортання системи системного моніторингу Zabbix та інтеграція інструментів ШІ для аналізу загроз	2	
Усього годин		18	6

8. Теми індивідуальних занять

(навчальним планом не передбачено)

9. Самостійна робота

№ з/п	Назва теми	Кількість годин	
		Денна форма здобуття освіти	*Заочна форма здобуття освіти*
1.	Аналіз міжнародних моделей та стандартів побудови цифрової інфраструктури університетів	6	8
2.	Скриптові мови системного адміністрування (Bash, PowerShell) для автоматизації рутини	6	8
3.	Безпека та масштабування контейнеризованих додатків у середовищі Kubernetes	6	8
4.	Проєктування хмарних освітніх рішень та аудит прав доступу за принципом найменших привілеїв	6	8
5.	Забезпечення високої доступності (High Availability) та балансування навантаження баз даних	6	8
6.	Нормативні вимоги Держспецзв'язку щодо побудови та атестації КСЗІ в закладах освіти	6	8
7.	Конфігурація систем запобігання витоку конфіденційних даних (DLP-систем) в освітніх установах	6	8
8.	Розробка плану відновлення після відмови та сценаріїв протидії програмам-вимагачам	6	8
9.	Оцінка та запобігання загрозам соціальної інженерії й сучасним схемам фішингу в освіті	6	8
10.	Застосування штучного інтелекту та великих мовних моделей для моніторингу інцидентів безпеки	6	8
	Усього годин	**60**	**80**

10. Індивідуальні навчально-дослідні завдання

(навчальним планом не передбачено)

11. Методи та технології навчання

Вивчення навчальної дисципліни «Системне адміністрування та безпека інформаційних освітніх систем» передбачає поєднання традиційних академічних методів з інноваційними цифровими технологіями викладання та навчання, орієнтованими на формування практичної готовності магістрантів до розв’язання складних інфраструктурних та безпекових задач.

У процесі вивчення дисципліни застосовуються:

– словесні методи: проблемні лекції, лекції-дискусії, пояснення, евристичні бесіди з аналізом реальних інцидентів кібербезпеки у сфері освіти;

– наочні методи: демонстрація топологій мереж, архітектурних схем серверних кластерів, скринкасти конфігурування операційних систем та систем моніторингу;

– практичні методи: лабораторні роботи в ізольованому віртуальному полігоні кафедри (Proxmox/Docker), розгортання та захист серверних служб, відпрацювання сценаріїв ліквідації кібератак;

– інтерактивні технології: проєктне навчання (Project-Based Learning), робота в малих групах над завданнями адміністрування, кейс-метод (Case Study) із розслідування кіберінцидентів;

– цифрові та дистанційні технології навчання: навчальний портал Moodle, корпоративні сервіси Google Workspace та Microsoft 365, використання прикладних сервісів штучного інтелекту для аналізу коду конфігурацій та журналів подій;

– самостійна робота: опрацювання нормативної бази Держспецзв'язку та міжнародних стандартів, підготовка індивідуального комплексного безпекового проєкту, самоконтроль та рефлексія.

12. Методи та критерії оцінювання

Під час викладання навчальної дисципліни використовуються такі види контролю: поточний та підсумковий (екзамен). Оцінювання здійснюється за 100-бальною накопичувальною системою ВДПУ ім. М. Коцюбинського.

Поточний контроль оцінюється сумою набраних балів. Максимальна сума становить 80 балів, зокрема:

– робота під час 6 лекційних занять (по 1 балу за кожну лекцію) – 6 балів;

– виконання 9 лабораторних робіт (по 6 балів за кожне лабораторне заняття) – 54 бали;

– виконання завдань самостійної роботи здобувачів – 20 балів;

Контроль засвоєння лекційного матеріалу здійснюється під час кожного лекційного заняття шляхом короткого тестування в електронній формі. Додатково можуть застосовуватися усне або письмове опитування та участь в обговоренні проблемних питань. Максимальна оцінка за результатами роботи на одному лекційному занятті становить 1 бал:

– 1 бал – правильно виконано 80–100 % тестових завдань або надано повну, правильну й аргументовану відповідь під час опитування чи обговорення;

– 0,5 бала – правильно виконано 50–79 % тестових завдань або відповідь є частково правильною та містить окремі неточності;

0 балів – правильно виконано менше 50 % тестових завдань, завдання не виконано або відповідь не демонструє розуміння лекційного матеріалу

Для здобувачів заочної форми здобуття освіти контроль засвоєння лекційного матеріалу здійснюється за аналогічними формами і критеріями. Результати короткого тестування, усного або письмового опитування та участі в обговоренні враховуються у складі оцінки за аудиторну роботу з відповідної теми. Максимальна кількість балів визначається згідно з таблицею розподілу балів для заочної форми здобуття освіти

Критерії оцінювання лабораторних робіт:

– 6 балів – роботу виконано вчасно, у повному обсязі та відповідно до вимог; отримані результати є правильними й обґрунтованими; здобувач упевнено пояснює хід виконання роботи та формулює висновки;

– 5 балів – завдання виконано в повному обсязі, налаштовані конфігурації функціонують без помилок, у звіті містяться вичерпні матеріали та аналіз, здобувач вільно відповідає на теоретичні питання під час захисту, але допущено незначні неточності;

– 4 бали – роботу виконано в повному обсязі, але допущено окремі неточності в конфігуруванні мережевих чи серверних параметрів, оформлення звіту має недоліки, відповіді на захисті є неповними

– 3 бали – роботу виконано в частково, в не повному обсязі, допущено окремі несуттєві помилки або неточності в оформленні, поясненні результатів чи формулюванні висновків;

– 2 бали — завдання виконано частково або допущено суттєві помилки; здобувач потребує допомоги під час пояснення результатів;

– 1 бал – представлено окремі результати виконання завдання, однак робота є неповною, містить значні помилки або не захищена;

– 0 балів — роботу не виконано, не подано або встановлено порушення принципів академічної доброчесності.

Для здобувачів заочної форми здобуття освіти оцінювання роботи під час аудиторних занять здійснюється відповідно до виконаних завдань та максимальної кількості балів, визначеної в таблиці розподілу балів для заочної форми.

Підсумковий контроль (екзамен):

Підсумковий контроль проводиться у формі семестрового екзамену та має на меті комплексну перевірку знань здобувача освіти, володіння понятійним апаратом і здатності застосовувати набуті знання на практиці. Максимальна кількість балів за екзамен становить 20 балів.

Контроль самостійної роботи здійснюється відповідно до тем і завдань навчальної дисципліни. Завдання для самостійного виконання змістовно доповнюють і поглиблюють матеріал лабораторних занять та можуть передбачати опрацювання наукових джерел, пошук і систематизацію інформації, застосування цифрових інструментів, аналіз отриманих результатів, підготовку висновків або вдосконалення створених цифрових матеріалів.

Для здобувачів денної форми здобуття освіти до кожної лабораторної роботи передбачено завдання для самостійного виконання. Максимальна оцінка за одне таке завдання становить 2 бали:

– 2 бали – завдання виконано самостійно, своєчасно, у повному обсязі та відповідно до встановлених вимог; результати є правильними й обґрунтованими;

– 1 бал – завдання виконано частково або допущено окремі помилки й неточності;

– 0 балів — завдання не виконано, не подано або його виконання не відповідає встановленим вимогам.

Загальна максимальна кількість балів за самостійну роботу здобувачів денної форми становить 20.

Для здобувачів заочної форми здобуття освіти, з огляду на менший обсяг аудиторних занять, основна частина навчальних завдань виконується самостійно. Максимальна кількість балів за самостійну роботу становить 58. Розподіл балів за окремими темами наведено в таблиці оцінювання заочної форми здобуття освіти.

Під час оцінювання самостійної роботи здобувачів заочної форми враховуються повнота і правильність виконання завдань, обґрунтованість застосування цифрових технологій та інструментів, самостійність, якість аналізу й представлення результатів, своєчасність виконання та дотримання принципів академічної доброчесності.

Розподіл балів за питаннями екзаменаційного білета:

– перше теоретичне питання (архітектура та системне адміністрування ІОС) – 6 балів;

– друге теоретичне питання (кібербезпека, кібергігієна та нормативні засади захисту інформації) – 6 балів;

– третє практичне ситуаційне завдання (розрахунок конфігурації, налаштування правил захисту, ліквідація інциденту) – 8 балів.

Зведена таблиця максимальної кількості балів за видами навчальної діяльності

Вид навчальної діяльності	Максимальна кількість балів
Робота під час 6 лекційних занять (по 1 балу за кожну лекцію)	6
Виконання та захист 9 лабораторних робіт (по 6 балів за кожне заняття)	54
Виконання завдань самостійної роботи здобувачів вищої освіти	20
Поточний контроль	**80**
Підсумковий контроль (екзамен)	**20**
Усього за навчальну дисципліну	**100**

Зарахування результатів неформальної та/або інформальної освіти: здобувачу можуть бути зараховані окремі теми та лабораторні роботи за умови надання сертифікатів відповідних курсів в обсязі до 1/3 від загальної кількості годин освітнього компонента.

Результат освітньої діяльності здобувача вищої освіти оцінюється згідно з Критеріями оцінювання знань і вмінь здобувачів вищої освіти Вінницького державного педагогічного університету імені Михайла Коцюбинського за такими рівнями і критеріями:

Оцінка за шкалами ECTS, стобальною, розширеною	Критерії оцінювання	Рівень досягнень здобувача вищої освіти
A 90-100 балів ВІДМІННО	Здобувач вищої освіти володіє понятійним і фактичним апаратом освітнього компонента на поглибленому рівні; комплексом знань та вмінь, який характеризується системністю. Застосування знань здійснюється на основі самостійного цілеутворення, побудови власних програм діяльності. Здобувач вищої освіти проявляє нешаблонність мислення у виборі і використанні елементів комплексу знань, здатний самостійно і творчо використовувати набуті уміння відповідно до варіативних ситуацій навчання. Здобувач вищої освіти спроможний самостійно формулювати узагальнення та висновки, нові задачі, розв'язувати нестандартні задачі, ситуації. Навчально-пізнавальна активність обумовлена пізнавальними інтересами, мотивами саморозвитку і професійного становлення. Здобувач вищої освіти проявляє інтерес до актуальних проблем відповідного освітнього компонента, може під керівництвом викладача вибрати предмет наукового дослідження, проводити самостійну науково-дослідну роботу.	ВИСОКИЙ

B 80-89 балів ДУЖЕ ДОБРЕ	Здобувач вищої освіти володіє понятійним і фактичним апаратом освітнього компонента на поглибленому рівні. Здобувач вищої освіти володіє комплексом знань та вмінь, який є частково-впорядкованим. У процесі застосування знань здобувач вищої освіти спроможний вибрати необхідній елемент комплексу знань та вмінь. Застосування знань та вмінь здійснюється як у стандартних ситуаціях, так і при незначних варіаціях умов на основі використання загальних рекомендацій. Відбувається перенесення сформованих умінь або їх комплексів на розв'язування незнайомих задач, ситуацій. Навчально-пізнавальна активність стимулюється пізнавальними інтересами, продукт діяльності оцінюється як професійно значущий.	ВИСОКИЙ
C 75-79 балів ДОБРЕ	Здобувач вищої освіти володіє понятійним і фактичним апаратом освітнього компонента на підвищеному рівні, може усвідомлено застосовувати знання та вміння для висвітлення суті питання. Комплекс знань частково-структурований. Знання застосовуються переважно у знайомих ситуаціях. Здобувач вищої освіти усвідомлює особливості навчальних задач, ситуацій тощо. Пошук способів їх розв'язання здійснюється за зразком. Здобувач вищої освіти спроможний аргументувати застосування певної методичної дії у ході розв'язування задач, ситуацій тощо. Навчально-пізнавальна активність стимулюється мотивами професійного становлення і пізнавальними інтересами.	ДОСТАТНІЙ
D 60-74 балів ЗАДОВІЛЬНО	Здобувач вищої освіти володіє понятійним і фактичним апаратом освітнього компонента на середньому рівні, може проілюструвати власними прикладами відповідь на питання, частково усвідомлює специфіку навчальних та прикладних задач, ситуацій тощо, має знання про способи розв'язування типових задач, ситуацій тощо. Однак процес самостійного розв'язування задач, ситуацій тощо потребує опори на зразок. Навчально-пізнавальна активність здобувачів вищої освіти є ситуативно-евристичною. Домінують мотиви обов'язку та особистого успіху. Використання засобів саморозвитку та самопізнання відбувається не усвідомлено.	ЗАДОВІЛЬНИЙ
E 50-59 балів ДОСТАТНЬО	Здобувач вищої освіти володіє понятійним і фактичним апаратом освітнього компоненту на середньому рівні. Має уявлення про специфіку навчальних та прикладних задач, ситуацій тощо. Виконання дій при роз'ясненні задач, ситуацій частково усвідомлюється, здійснюється частково правильно.	НИЗЬКИЙ
FX 35-49 балів НЕЗАДОВІЛЬНО	Здобувач вищої освіти володіє понятійним і фактичним апаратом освітнього компонента на елементарному рівні, має уявлення про зміст основних розділів. Виконання окремих дій відбувається не усвідомлено, однак переважно правильно, навчально-пізнавальна активність мотивується ситуативно-прагматичним інтересом.	НЕЗАДОВІЛЬНИЙ
F 0-34 балів НЕПРИЙНЯТНО	Здобувач вищої освіти володіє понятійним і фактичним апаратом освітнього компонента на елементарному рівні, має уявлення про зміст окремих розділів. Виконання окремих методичних дій відбувається несвідомо, у більшості неправильно, навчально-пізнавальна активність проявляється лише у ситуаціях зовнішнього примусу.	

13. Розподіл балів, які отримують здобувачі вищої освіти

ПОТОЧНИЙ КОНТРОЛЬ ТА САМОСТІЙНА РОБОТА																		Підсумковий контроль (екзамен)	Загальна кількість балів
РОЗДІЛ 1										РОЗДІЛ 2									
Т1		Т2		Т3		Т4		Т5		Т6		Т7		Т8		Т9		Т10			
ауд	ср	ауд	ср	ауд	ср	ауд	ср	ауд	ср	ауд	ср	ауд	ср	ауд	ср	ауд	ср	ауд	ср		
7	2	6	2	1	2	6	2	7	2	7	2	6	2	7	2	6	2	7	2	20	100

Шкала оцінювання: стобальна, ECTS, розширена

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за розширеною шкалою для екзамену, заліку, курсового проєкту (роботи), практики
90-100	A	ВІДМІННО
80-89	B	ДУЖЕ ДОБРЕ
75-79	C	ДОБРЕ
60-74	D	ЗАДОВІЛЬНО
50-59	E	ДОСТАТНЬО
35-49	FX	НЕЗАДОВІЛЬНО З МОЖЛИВІСТЮ ПОВТОРНОГО СКЛАДАННЯ
0-34	F	НЕЗАДОВІЛЬНО З ОБОВ'ЯЗКОВИМ ПОВТОРНИМ ВИВЧЕННЯМ ДИСЦИПЛІНИ

14. Методичне забезпечення

Методичне забезпечення навчальної дисципліни охоплює:

1. Робоча програма навчальної дисципліни «Системне адміністрування та безпека інформаційних освітніх систем».
2. Електронний навчально-методичний комплекс дисципліни, розміщений на навчальному порталі Moodle ВДПУ ім. М. Коцюбинського. https://moodle.vspu.edu.ua/course/view.php?id=12
3. Методичні рекомендації до навчальної дисципліни «Системне адміністрування та безпека інформаційних освітніх систем».
4. Мультимедійні презентації лекцій, відеоінструкції, структурні схеми серверних архітектур та мережевих протоколів безпеки.
5. Каталоги та інструкції з налаштування сучасного програмного забезпечення з відкритим кодом (FOSS), систем моніторингу, сканерів вразливостей та хмарних освітніх платформ.

15. Рекомендована література

Основна

1. Гулай О. І., Кабак В. В., Герасимчук Г. А. Засоби та технології цифрового навчання: теоретичний та практичний аспекти : монографія. Луцьк : Вежа-Друк, 2025. 159 с. ISBN 978-966-940-645-3.

2. Цифрова компетентність вчителя нової української школи: 2024: інновації в умовах змін : монографія / за заг. ред. О. В. Овчарук. Київ : ІЦО НАПН України, 2024. 268 с. ISBN 978-617-8330-35-4.

3. Шарова Т. М., Шаров С. В. Цифровізація освіти як чинник розвитку інтелектуального потенціалу обдарованих дітей та молоді : монографія. Запоріжжя, 2026. 342 с. ISBN 978-617-7823-87-1.

4. Digital Transformation of Education: Challenges and Prospects : Monograph / Institute of Pedagogy of NAES of Ukraine; ed.: O. Topuzov, M. Holovko, I. Tverdokhlib, Z. Sharlovych, K. Ladonia. Lomza – Kyiv, 2025. 344 c. DOI: 10.32405/mono-lomza-kyiv-2025.

5. Уманець В. О. Системне адміністрування та безпека інформаційних освітніх систем : методичні рекомендації для здобувачів вищої освіти другого (магістерського) рівня за спеціальністю А5 Професійна освіта (за спеціалізаціями), спеціалізація А5.39 Цифрові технології. Вінниця : ВДПУ імені Михайла Коцюбинського, 2026. 56 с.

Додаткова

1. Гріщенко П. С., Кізім С. С. Цифрова інфраструктура та сучасне програмне забезпечення у підготовці бакалаврів з інформаційних систем та технологій. Сучасні інформаційні технології та інноваційні методики навчання в підготовці фахівців. 2025. Вип. 78. С. 45–56. DOI: 10.31652/2412-1142-2025-78-45-56.

2. Лазаренко Н. І., Кізім С. С., Волошина О. В. Трансформаційна професійна підготовка майбутніх фахівців в умовах цифровізації освіти. Сучасні інформаційні технології та інноваційні методики навчання в підготовці фахівців. 2025. Вип. 78. С. 279–290. DOI: 10.31652/2412-1142-2025-78-279-290.

3. Ковальчук А. Цифрові інструменти в діяльності педагога професійного навчання. Молодь і ринок. 2024. № 6 (226). С. 171–176. DOI: 10.24919/2308-4634.2024.307879.

4. Kizim S., Voloshyna O., Sarancha I., Nahorniak S., Stoliarenko O. Organization of adaptive training using artificial intelligence technologies in the context of war. Environment. Technology. Resources. 2025. Vol. 2. P. 205–212. DOI: 10.17770/etr2025vol2.8606.

5. Hwu H. H., Foster D., Ramsay C., Dick A., Li N. Identifying Competencies of Digitally Fluent Educators in Higher Education: A Delphi Study. Education Sciences. 2026. Vol. 16, No. 2. Article 342. DOI: 10.3390/educsci16020342.

6. Дідух Л. Індивідуалізація освітнього процесу в закладах вищої освіти засобами цифрових технологій: можливості та виклики. Наукові записки ВДПУ. Серія: Педагогіка і психологія. 2026. Вип. 85. С. 9–16. DOI: 10.31652/2415-7872-2026-85-9-16.

16. Інформаційні ресурси в Інтернеті

1. Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку): Нормативна база та рекомендації. URL: https://cip.gov.ua/

2. Національний координаційний центр кібербезпеки (НКЦК) при РНБО України. URL: https://nccc.gov.ua/

3. Команда реагування на комп’ютерні надзвичайні події України CERT-UA. URL: https://cert.gov.ua/

4. Дія.Освіта: Національна платформа цифрової грамотності та кібергігієни. URL: https://osvita.diia.gov.ua/

5. NIST Cybersecurity Framework (CSF 2.0) Reference Guide. URL: https://www.nist.gov/cyberframework
6. Proxmox Virtual Environment & Backup Server Documentation. URL: https://www.proxmox.com/
7. Microsoft Learn: Enterprise Security, Active Directory and Threat Protection. URL: https://learn.microsoft.com/
8. Wazuh: Open Source Security Platform & SIEM Documentation. URL: https://wazuh.com/
9. Open Web Application Security Project (OWASP Foundation). URL: https://owasp.org/