

**ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»
ФІЗИЧНИЙ ФАКУЛЬТЕТ
Кафедра твердотільної електроніки та інформаційної безпеки**



РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

**ТЕХНОЛОГІЇ АДМІНІСТРУВАННЯ ТА ЕКСПЛУАТАЦІЯ ЗАХИЩЕНИХ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ**

Рівень вищої освіти	другий (магістерський) рівень
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека
Предметна спеціальність (Спеціалізація) <i>(за наявності)</i>	
Освітня програма	Безпека інформаційних і комунікаційних систем
Статус дисципліни	обов'язкова
Мова навчання	українська

Робоча програма навчальної дисципліни «Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем» для здобувачів вищої освіти галузі знань **12 Інформаційні технології** спеціальності **125 Кібербезпека** освітньої програми **Безпека інформаційних і комунікаційних систем**.

Розробники: Пригара М.П., канд. техн. наук, доц. кафедри ТМ


Робочу програму розглянуто та затверджено на засіданні кафедри *твердотільної електроніки та інформаційної безпеки*

протокол № 7 від «28» 04 2022р.

Завідувач кафедри  Різак В.М.

Схвалено науково-методичною комісією фізичного факультету

протокол № 10 від «29» 04 2022р.

Голова науково-методичної комісії  Карбованець М. І.

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Найменування показників	Розподіл годин за навчальним планом	
	Денна форма навчання	Заочна форма навчання
Кількість кредитів ЄКТС – 4,5	Рік підготовки:	
Загальна кількість годин – 135	1-й	
Кількість модулів – 2	Семестр:	
Тижневих годин для денної форми навчання: аудиторних – 3 самостійної роботи студента – 4	1-й	
	Лекції:	
	36	
	Практичні (семінарські):	
Вид підсумкового контролю: іспит	Лабораторні:	
	18	
Форма підсумкового контролю: усна	Самостійна робота:	
	81	

2. МЕТА ТА ЗАВДАННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Мета навчальної дисципліни є навчити студентів сучасним методам адміністрування захищених програмно апаратних комплексів та комп'ютерних мереж.

Процес вивчення дисципліни спрямований на формування елементів наступних **компетентностей**:

КЗ-1. Здатність застосовувати знання у практичних ситуаціях.

КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт.

КФ1. 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.

КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.

КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.

КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

КФ8. 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.

3. ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Відповідно до освітньої програми **«Безпека інформаційних і комунікаційних систем»**, вивчення навчальної дисципліни **«Технології адміністрування та експлуатація захищених інформаційно-комунікаційних систем»** повинно забезпечити досягнення здобувачами вищої освіти таких програмних результатів навчання (ПРН):

ПРН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

ПРН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

ПРН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.

PH14. 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.

PH16. 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.

PH18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напрямку інформаційної безпеки та\або кібербезпеки.

PH23. 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.

Після вивчення навчальної дисципліни студенти повинні знати:

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

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

- Використовувати сучасне програмно апаратне забезпечення інформаційно комунікаційних технологій.

- Використовувати програмні та програмно апаратні комплекси захисту інформаційних ресурсів.

- Використовувати сучасне програмно апаратне забезпечення інформаційно-комунікаційних технологій.

Вміти:

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

Розробляти, застосовувати, інтегрувати, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі у сфері інформаційної безпеки та\або кібербезпеки.

Критично осмислювати проблеми інформаційної безпеки та\або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі нових результатів досліджень інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.

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

Досліджувати, розробляти і супроводжувати системи та засоби захисту інформації та\або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та\або кібербезпекою організації на базі стратегії і політики інформаційної безпеки

4. Методи контролю

Види контролю:

Поточне тестування студентів здійснюється через:

- бланкове тестування;

- оцінювання практичних навичок;

- оцінювання виконання самостійної роботи студентів.

Серед методів контролю: оцінювання практичних робіт та сформованих навичок, оцінювання доповідей, виконання різнорівневих завдань, бланкове тестування тощо.

Підсумкова оцінка отримується студентом за результатами всіх видів поточного контролю та результату іспиту.

5. Розподіл балів, які отримують студенти. Критерії та шкала оцінювання: національна та ECTS

Реалізація основних завдань контролю знань здобувачів вищої освіти в ОНУ досягається системними підходами до оцінювання та комплексністю застосування різних видів контролю. Згідно з діючою в університеті системою комплексної діагностики знань здобувачів вищої освіти, з метою стимулювання планомірної та систематичної навчальної роботи, оцінка знань здійснюється за 100-бальною системою, яка переводиться відповідно у національну шкалу («відмінно», «добре», «задовільно», «незадовільно») та шкалу європейської кредитно-трансферної системи (ЄКТС –А, В, С, D, E, FX, F).

За системою УжНУ	За шкалою ECTS	За національною системою	Критерії
90-100	A	5 (відмінно)	Повно та ґрунтовно засвоїв всі теми навчальної програми вміє вільно та самостійно викласти зміст всіх питань програми навчальної дисципліни, розуміє її значення для своєї професійної підготовки, повністю виконав усі завдання кожної теми, поточного та підсумкового контролю в цілому.
85-89	B	4 (дуже добре)	Недостатньо повно та ґрунтовно засвоїв окремі питання робочої програми. Вміє самостійно викласти зміст основних питань програми навчальної дисципліни, виконав завдання кожної теми, поточного та підсумкового контролю в цілому.
75-84	C	4 (добре)	Недостатньо повно та ґрунтовно засвоїв деякі теми робочої програми, не вміє самостійно викласти зміст деяких питань програми навчальної дисципліни. Окремі завдання кожної теми, поточного та підсумкового контролю в цілому виконав не повністю.
70-74	D	3 (задовільно)	Засвоїв лише окремі теми робочої програми. Не вміє вільно самостійно викласти зміст основних питань навчальної дисципліни, окремі завдання кожної теми, поточного та підсумкового контролю не виконав.
60-69	E	3 (достатньо)	Засвоїв лише окремі питання навчальної програми. Не вміє достатньо самостійно викласти зміст більшості питань програми навчальної дисципліни. Виконав лише окремі завдання кожної теми та поточного контролю в цілому.

35-59	FX	2 (незадовільно)	Не засвоїв більшості тем навчальної програми не вміє викласти зміст більшості основних питань навчальної дисципліни. Не виконав більшості завдань кожної теми та підсумкового контролю в цілому.
0-34	F	2 (незадовільно)	Не засвоїв навчальної програми, не вміє викласти зміст жодної теми навчальної дисципліни, не виконав підсумкового контролю, з обов'язковим повторним вивченням дисципліни.

Поточне тестування та самостійна робота																Підсумковий контроль	Сума
Змістовий модуль №1								Змістовий модуль № 2								Іспит	100
T1	T2	T3	T4	T5	T6	T7	T8	T8	T9	T10	T11	T12	T13	T14	T15		
2	2	2	2	2	2	4	4	2	2	2	4	5	5	5	5		
20								30								50	100

6. Зміст навчальної дисципліни

ЗМІСТОВИЙ МОДУЛЬ 1. «Адміністрування Windows»

Тема 1. Адміністрування Windows.

Встановлення. Початкове налаштування. Сервери Windows. Основні мережеві налаштування.

Література: 1, 4, 5.

Тема 2. Віртуалізація.

Поняття віртуалізації. Контейнеризація. Докер. Види віртуальних машин.

Література: 1, 2, 6.

Тема3. Встановлення і початкове налаштування Windows Server.

Базове мережеве налаштування. Розгортання системи через мережу. Встановлення Active Directory

Література: 2, 3, 5.

Тема 4. Основні концепції Active Directory.

Основні концепції служби каталогів. Профілі користувачів. Квотування диску. Розмежування прав.

Література: 1, 2, 4, 5.

Тема 5. Файлові системи.

Файлова система FAT16, Файлова система FAT32, Файлова система NTFS. Файлові системи хмарного зберігання даних.

Література: 2, 4, 5.

Тема 6. Використання групових політик.

Створення власних групових політик, базові налаштування. Локальні та глобальні групові політики. Розподіл прав.

Література: 1, 2, 5.

Тема 7. Сервери DHCP і DNS.

Базові налаштування сервера DHCP. Налаштування DNS сервера на контролері домену.

Література: 1, 2, 3, 7.

Тема 8. Встановлення і налаштування Domain Controller.

Поняття домену. Сервери в середині домену. Групові політики контролера домену, Профілі користувачів та авторизація.

Література: 1, 2, 5, 8.

ЗМІСТОВИЙ МОДУЛЬ 2. «Адміністрування Linux»

Тема 9. Планування і розгортання Linux.

Ієрархія версій. Встановлення Linux. Розподіл дискового простору. Вибір пакетів. Графічні оболонки.

Література: 1, 4, 5, 9.

Тема 10. Файлові системи, диски і розділи.

Робота з файловими системами EXT3, EXT4. Призначення розділу SWAP. Робота з файловими системами. Файл fstab. Монтування пристроїв.

Література: 1, 2, 5, 6.

Тема 11. Програмний комплекс для віддаленого керування системою Webmin.

Встановлення Webmin. Базові налаштування Apache server. Віддалений доступ через telnet та SSH

Література: 1, 4, 5, 9.

Тема 12. Міжмережвий екран IPTABLES.

Поняття файрволу. Трансляція адрес. Міжмережева взаємодія. Пакет Iptables. Пакет IPChains.

Література: 2, 4, 5.

Тема 13. Проксі-сервер SQUID.

Поняття проксі сервера. Налаштування сервера SQUID. Прозорий проксі сервер.

Можливості авторизації через проксі сервер.

Література: 4, 10.

Тема 14. Файловий сервер SAMBA.

Протокол SMB. Спільний доступ до файлів принтерів та папок. Базові налаштування сервера SAMBA.

Література: 6, 7, 10.

Тема 15. Засоби створення резервних копій. RAID-масиви.

Поняття резервного копіювання. RAID-масиви. Автоматичні резервні копії.

Відновлення з резервної

копії. Література: 6, 7, 9, 10.

7. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

№ з/п	Тема	Кількість годин					
		Очне відділення			Заочне відділення		
		Л	л/р	Ср	Л	л/р	Ср
Змістовий модуль 1. Адміністрування Windows							
1	Тема 1. Адміністрування Windows	2		4			
2	Тема 2. Віртуалізація	2		4			
3	Тема 3. Встановлення і початкове налаштування Windows Server.	2	2	4			
4	Тема 4. Основні концепції Active Directory.	2	2	4			

5	Тема 5. Файлові системи	2		4			
6	Тема 6. Використання групових політик.	2	2	4			
7	Тема 7. Сервери DHCP і DNS.	2		8			
8	Тема 8. Встановлення і налаштування Domain Controller	4	2	8			
<i>Разом за змістовим модулем 1</i>		18	8	40			
Змістовий модуль 2. Адміністрування Linux							
9	Тема 9. Файлові системи, диски і розділи.	2		6			
10	Тема 10. Планування і розгортання Linux	2	2	7			
11	Тема 11. Програмний комплекс для віддаленого керування системою Webmin.	2	2	4			
12	Тема 12. Міжмережевий екран IPTABLES.	2	2	4			
13	Тема 13. Проксі-сервер SQUID.	4	2	8			
14	Тема 14. Файловий сервер SAMBA.	4	2	8			
15	Тема 15. Засоби створення резервних копій. RAID-масиви.	2		4			
<i>Разом за змістовим модулем 2</i>		18	10	41			
<i>Разом</i>		36	18	81			

8. ТЕМИ СЕМІНАРСЬКИХ ТА ЛАБОРАТОРНИХ ЗАНЯТЬ

№ з/п	№ теми	Тема	Кількість годин	
			денні	заочні
1	3,4	Встановлення і початкове налаштування Windows Server.	2	
2	5	Налаштування Active Directory	2	
3	10	Використання групових політик	2	
4	13	Встановлення і налаштування Domain Controller	2	
5	14	Планування і розгортання Linux.	2	
6	11	Програмний комплекс для віддаленого керування системою Webmin.	2	
7	12	Отримати практичні навички з налаштування IPTABLES	2	
8	13	Отримати практичні навички з налаштування SQUID	2	
9	14	Отримати практичні навички з налаштування SAMBA.	2	
Разом			18	

9. ТЕМИ ПРАКТИЧНИХ ЗАНЯТЬ

Начальним планом не передбачені

10. ОРГАНІЗАЦІЯ САМОСТІЙНОЇ РОБОТИ СТУДЕНТІВ

Завдання для самостійної роботи студентів

Самостійна робота студентів під час вивчення даного навчального курсу включає теоретичну підготовку з окремих тем курсу, що вивчаються в порядку самостійної роботи, а також підготовку до практичних занять з тем, що вказані вище.

Місце виконання самостійної роботи

Самостійна робота студента над засвоєнням навчального матеріалу виконується у бібліотеці, навчальних аудиторіях і лабораторіях, комп'ютерних класах, а також у домашніх умовах.

№ п/п	Тематика	К-сть годин
1	Сертифікації та вміння системного адміністратора.	5
2	Посадові обов'язки і спеціалізація системного адміністратора.	5
3	Плюси і мінуси професії "системний адміністратор". Перспективи. Попит.	4
4	Основні поняття віртуалізації.	5
5	Віртуальна машина.	5
6	Технології віртуалізації.	5
7	Планування і встановлення системи Windows Server.	5
8	Файлові системи, диски і розділи Windows Server.	5
9	Сервери DHCP і DNS Windows Server.	5
10	Основні концепції Active Directory.	5
11	Використання групових політик Windows Server.	5
12	Налаштування параметрів безпеки сервера.	5
13	Додаткові сервіси Windows Server.	6
14	Планування і розгортання Linux.	8
15	Файлові системи, диски і розділи Linux.	8
Разом:		81

До самостійної роботи відноситься: підготовка до лекцій, практичних, семінарських, лабораторних занять; написання рефератів, есе; опрацювання відеоматеріалів, робота в мережі Інтернет, складання тестів, кросвордів, ситуаційних завдань.

11. ІНДИВІДУАЛЬНЕ НАВЧАЛЬНО-ДОСЛІДНЕ ЗАВДАННЯ

Не заплановане.

12. Методи навчання

Заняття із дисципліни проводяться у формі: лекцій з використанням наочних матеріалів, посібників, мультимедійних технологій; практичних занять; самостійної роботи з основною та додатковою літературою, періодичними виданнями, джерелами в інтернеті.

Серед методів навчання використовуються: *словесні* (пояснення, розповідь, інструктажі, ситуативне моделювання, ситуативне навчання, оксфордські дебати, мозковий штурм, аналіз відео- і фотоматеріалів, обмін думками, захист доповідей тощо); *наочні* (демонстрування, мультимедійні презентації); *практичні* (ділові (рольові) ігри, розв'язання ситуаційних задач, аналіз статистичних даних, метод проектів, відпрацювання практичних навичок тощо) методи.

13. Методичне та матеріально-технічне забезпечення

Методичне забезпечення: робоча програма навчальної дисципліни; навчальна програма дисципліни; мультимедійний супровід матеріалів лекцій та семінарських занять; план семінарських занять. Різноманітні прилади, необхідні для ведення практичних занять; засоби індивідуального захисту.

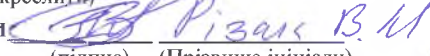
1. Тексти лекцій.
2. Ілюстративний матеріал: слайди, таблиці, презентації.

14. Рекомендована навчальна та навчально-методична література

1. Бикманс Герард. Linux from Scratch. Version 8.4, 2019. — 368 с.
2. Васильєва Н.К. та ін. Інформатика в LINUX-середовищі, Навч. посібник / кол. авт.; за ред. Н.К. Васильєвої. — Дніпропетровськ: Біла К., 2016. — 267 с.
3. Основи адміністрування LAN у середовищі MS Windows. Навчальний посібник / Б. А. Демида, К. М. Обельовська, В. С. Яковина. Львів: Видавництво Львівської політехніки, 2013. 488 с
4. Wiki DHCP. - [Електронний ресурс]. - Режим доступу: <http://en.wikipedia.org/wiki/DHCP>.
5. Microsoft DHCP. - [Електронний ресурс]. - Режим доступу: <http://technet.microsoft.com/en-us/network/bb643151.aspx>
6. Microsoft Corporation Microsoft Windows 7. Group Policy for Beginners. Published: April 2011. - [Електронний ресурс]. - Режим доступу: <http://technet.microsoft.com/ru-ru/library/>
7. Захист операційного середовища систем Інтернет голосування/ВМ Чуприн, ВМ Вишняков, МП Пригара -// Захист інформації, 2017 - Режим доступу: <https://jrnl.nau.edu.ua/index.php/ZI/article/download/11444/15347>
8. Захищена система технічної підтримки процесів дистанційного волевиявлення- Режим доступу: https://dspace.nau.edu.ua/bitstream/NAU/34672/5/diss_Prygara.pdf
9. To install the default LAMP stack in Ubuntu 10.04 and above - Режим доступу: <https://help.ubuntu.com/community/ApacheMySQLPHP>
10. Lee, James; Brent Ware (December 2002). Open Source Web Development with LAMP: Using Linux, Apache, MySQL, Perl, and PHP. Addison Wesley. ISBN 0-201-77061-X. - Режим доступу: <https://archive.org/details/opensourcewebdev0000leej>
11. Налаштування детального запису операцій із файлами на Samba-сервері - Режим доступу: <http://avz.org.ua/wp/2010/03/05/samba-detailed-logging/>
12. Setting up Samba as an Active Directory Domain Controller- Режим доступу: https://wiki.samba.org/index.php/Setting_up_Samba_as_an_Active_Directory_Domain_Controller

**Результати перегляду
робочої програми навчальної дисципліни**

Робоча програма перезатверджена на 20 22 / 20 23 н.р. без змін; зі змінами _____
(потрібне підкреслити)

протокол № 4 від « 9 » 12 20 22 р. Завідувач кафедри 
(підпис) (Прізвище ініціали)

Робоча програма перезатверджена на 20 ____ / 20 ____ н.р. без змін; зі змінами _____
(потрібне підкреслити)

протокол № ____ від « ____ » _____ 20 ____ р. Завідувач кафедри _____
(підпис) (Прізвище ініціали)

Робоча програма перезатверджена на 20 ____ / 20 ____ н.р. без змін; зі змінами _____
(потрібне підкреслити)

протокол № ____ від « ____ » _____ 20 ____ р. Завідувач кафедри _____
(підпис) (Прізвище ініціали)

Робоча програма перезатверджена на 20 ____ / 20 ____ н.р. без змін; зі змінами _____
(потрібне підкреслити)

протокол № ____ від « ____ » _____ 20 ____ р. Завідувач кафедри _____
(підпис) (Прізвище ініціали)