НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
Кафедра комп'ютерних систем, мереж та кібербезпеки

«ЗАТВЕРДЖУЮ»

Декан факультету
інформаційних технологій

_____ проф. О.Г. Глазунова
«___» _____ 2022р.

СХВАЛЕНО
на засіданні кафедри
комп'ютерних систем,
мереж та кібербезпеки
Протокол №12 від «11» травня» 2022р.
Завідувач кафедри
(проф. Лахно В.А.)

РОЗГЛЯНУТО
Гарант ОП «Кібербезпека»

_____ (Лахно В.А.)

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «УПРАВЛІННЯ ДОСТУПОМ»

Спеціальність	125 «Кібербезпека»
Факультет	інформаційних технологій
Розробник:	Сагун А.В., доцент, к.т.н., доцент

Київ – 2022 р.

1. Опис навчальної дисципліни «Управління доступом»

Галузь знань, напрям підготовки, спеціальність, освітньо-кваліфікаційний рівень		
Галузь знань	12 – Інформаційні технології	
Спеціальність	125 – Кібербезпека	
Освітньо-кваліфікаційний рівень	бакалавр	
Характеристика навчальної дисципліни		
Вид	Вибіркова	
Загальна кількість годин	150	
Кількість кредитів ECTS	5	
Кількість змістових модулів	2	
Курсовий проект (робота) (якщо є в робочому навчальному плані)	-	
Форма контролю	екзамен	
Показники навчальної дисципліни для денної та заочної форм навчання		
	денна форма навчання	заочна форма навчання
Рік підготовки (курс)	3	
Семестр	6	
Лекційні заняття, год.	30	
Практичні, семінарські заняття	-	
Лабораторні заняття, год.	30	
Самостійна робота, год.	90	
Індивідуальні завдання	-	
Кількість тижневих аудиторних годин для денної форми навчання	4	

2. Мета, завдання та компетентності навчальної дисципліни

Мета: формування у студентів знань з планування та реалізації механізмів та систем управління доступом.

Завдання навчальної дисципліни: отримання знань та навичок з організації управління доступом до інформації в інформаційних системах типу корпоративних мереж на основі розгортання служби каталогу Active Directory та ознайомлення з основами проектування систем управління доступу у ОС Windows Server.

В результаті вивчення навчальної дисципліни студент повинен:

- **знати:**

- принципи планування механізмів управління доступом в інформаційних мережах та системах;
- технології та особливості створення та використання об'єктів та суб'єктів доступу, групових політик доступу до інформації в рамках КМ;
- моделі та механізми захисту властивостей інформації в корпоративних системах доступу на базі AD, регулювання доступу та захисту властивостей дискової інформації;
- рівні доступу в КМ, принципи створення та використання доменної структури доступу в КМ та авторизаційні протоколи в системах доступу да базі AD Windows Server.

- **вміти:**

– планувати структуру та механізми розмежування доступу в корпоративних інформаційних системах;

– створювати та маніпулювати груповими політиками доступу на рівні ОС Windows Server;

– організовувати фізичну інфраструктура для механізмів резервування корпоративної бази доступу AD.

– Створювати корпоративні дискові системи зберігання даних з необхідним рівнем захищеності інформації в Windows Server.

Набуття компетентностей:

Відповідно до освітньої програми підготовки фахівців за спеціальністю 125 «Кібербезпека» навчальна дисципліна забезпечує формування загальних і фахових компетентностей:

Загальні компетентності:

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

ЗК 2. Здатність вчитися і оволодівати сучасними знаннями.

ЗК 5. Здатність спілкуватися іноземною мовою.

ЗК 7. Вміння виявляти, ставити та вирішувати проблеми.

Спеціальні (фахові, предметні) компетентності (СК):

СК 1. Базові знання технічних характеристик, конструктивних особливостей, застосування правил експлуатації комп'ютерних систем, мереж та програмно-технічних засобів.

СК 4. Здатність проектувати, впроваджувати та обслуговувати комп'ютерні системи та мережі різного виду та призначення.

СК 7. Готовність брати участь в роботах з впровадження комп'ютерних систем та мереж, введення їх до експлуатації на об'єктах різного призначення.

СК 9. Здатність системно адмініструвати, використовувати, адаптувати та експлуатувати наявні інформаційні технології та системи.

СК 10. Здатність здійснювати організацію робочих місць, їхнє технічне оснащення, розміщення комп'ютерного устаткування, використання організаційних, технічних, алгоритмічних та інших методів і засобів захисту інформації.

СК 13. Здатність досліджувати проблему в галузі комп'ютерних та інформаційних технологій, визначати їх обмеження.

СК 15. Здатність аргументувати вибір методів розв'язування спеціалізованих задач, критично оцінювати отримані результати та захищати прийняті рішення.

В результаті вивчення навчальної дисципліни студент набуде певні програмні результати (РН), а саме

ПРН 2. Знати основи професійно-орієнтованих дисциплін спеціальності.

ПРН 4. Мати знання з новітніх технологій в галузі комп'ютерної інженерії.

ПРН 6. Вміти застосовувати знання для ідентифікації, формулювання і розв'язування технічних задач спеціальності, використовуючи відомі методи.

ПРН 7. Вміти застосовувати знання для розв'язування задач аналізу та синтезу засобів, характерних для спеціальності.

ПРН 9. Вміти застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп'ютерних систем та мереж для вирішення технічних задач спеціальності.

ПРН 10. Вміти розробляти системне і прикладне програмне забезпечення для вбудованих і розподілених застосувань, мобільних систем, розраховувати, експлуатувати, типове для спеціальності обладнання.

ПРН 13. Вміти ідентифікувати, класифікувати та описувати роботу комп'ютерних систем та їх компонентів.

ПРН 14. Вміти поєднувати теорію і практику, а також приймати рішення та виробляти стратегію діяльності для вирішення завдань спеціальності з урахуванням загальнолюдських цінностей, суспільних, державних та виробничих інтересів.

ПРН 16. Вміти оцінювати отримані результати та аргументовано захищати прийняті рішення.

ПРН 17. Вміння спілкуватись, включаючи усну та письмову комунікацію українською мовою та однією з іноземних мов (англійською, німецькою, італійською, французькою, іспанською).

ПРН 19. Здатність адаптуватись до нових ситуацій, обґрунтовувати, приймати та реалізовувати у межах компетенції рішення.

В контексті зазначених вище компетентностей та програмних результатів навчання задачі викладання дисципліни визначають необхідний комплекс знань і вмінь, що отримують студенти під час вивчення дисципліни.

Навчальна програма розрахована на студентів, які навчаються за освітньою програмою підготовки бакалавра за спеціальністю «Кібербезпека».

Програма побудована за вимогами кредитно-модульної системи організації навчального процесу у закладах вищої освіти і використанням академічної системи оцінювання досягнень студентів та шкали оцінок Європейської кредитно-трансферної системи (ECTS).

Робоча навчальна програма з курсу є основним документом, що охоплює всі види навчальної роботи при вивченні курсу студентами та відбиває основні методичні настанови кафедри.

Навчальна програма дисципліни розроблена на підставі наступних документів:

- освітня програма підготовки бакалаврів за спеціальністю 125 «Кібербезпека»;
- навчальний план підготовки бакалаврів за спеціальністю 125 «Кібербезпека».
- освітньо-професійної програми «Кібербезпека» першого (бакалаврського) рівня вищої освіти за спеціальністю 125 «Кібербезпека».

Навчальна програма характеризує шляхи перетворення інформації, що одержується студентом впродовж вивчання курсу, і відбиває зміст курсу, розподілення його на розділи та їх обсяги, дані про форми вивчення та контролю знань.

Теоретичною базою для вивчення курсу «Віртуалізація та системи зберігання даних» є курси «Безпека інформації в інформаційно - комунікаційних системах», «Захист інформації в комп'ютерних системах», «Навчальна практика з проектування систем кібербезпеки», ОПП першого (бакалаврського) рівня вищої освіти.

3. Програма та структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин												
	денна форма							Заочна форма					
	тижні	всього	у тому числі					всього	у тому числі				
			л	п	лр	інд	ср		л	п	лр	інд	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13	14
Змістовий модуль 1.													
Тема 1. Інформація та інформаційна система, як об'єкт доступу. Планування механізмів доступу до інформації в рамках корпорації	1	14	2	-	2	-	10						
Тема 2. Засоби та методи управління доступом до інформації. Технологія Active Directory	2-3	18	4	-	4	-	10						
Тема 3. Планування структури корпоративної мережі (КМ). Об'єкти та суб'єкти доступу до інформації в рамках КМ	4	20	4	-	4	-	12						
Тема 4. Моделі та механізми захисту властивостей інформації в корпоративних системах доступу на базі AD	5-7	20	4	-	4	-	12						
Разом за змістовим модулем 1		**72**	**14**		**14**		**44**						
Змістовий модуль 2.													
Тема 1. Механізми доступу до дискової інформації. Технологія RAID.	8	20	4	-	4	-	12						
Тема 2. Рівні доступу в КМ. Доменна структура доступу в КМ. Авторизаційні протоколи в системах доступу да базі AD Windows Server	9	20	4	-	4	-	12						
Тема 3. Організація фізичної інфраструктури для механізму резерування корпоративної бази доступу AD. Корпоративні дискові системи зберігання даних з необхідним рівнем захищеності інформації в Windows Server	10-12	20	4	-	4	-	12						
Тема 4. Групові політики доступу. Проектування GPO для групового доступу	13	18	4	-	4	-	10						
Разом за змістовим модулем 2		**78**	**16**	**-**	**16**	**-**	**46**						
Всього годин		**150**	**30**	**-**	**30**	**-**	**90**						

4. Теми семінарських занять

№ з/п	Назва теми	Кількість годин
	Не передбачено робочим навчальним планом	

5. Теми практичних занять

№ з/п	Назва теми	Кількість годин
	Не передбачено робочим навчальним планом	

6. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Вибір і розгортання фізичної інфраструктури на базі технологій віртуалізації та налаштування маршрутизації мережі віртуальних комп'ютерів корпоративної мережі	2
2	Встановлення ролей та компонентів Active Directory, створення каталогу та адміністрування AD та контролера домену DC в середовищі Windows Server 2012 r2»	4
3	Створення політик та системи до об'єктів AD доступу для учасників корпоративної мережі	4
4	Організація фізичної інфраструктури для механізму резервування корпоративної бази доступу AD. Корпоративні дискові системи зберігання даних з необхідним рівнем захищеності інформації в Windows Server	4
5	Адміністрування доменної структури КМ в рамках управління доступом	4
6	Адміністрування облікових записів користувачів. Управління парольними та авторизаційними політиками КМ	4
7	Створення групових політик для учасників корпоративної мережі	4
8	Встановлення та налаштування механізмів доступу до корпоративного поштового серверу MS Exchange	4
	Всього	30

7. Контрольні питання, комплекти тестів для визначення рівня засвоєння знань студентами

7.1. Контрольні питання для перевірки знань студентів:

1. Віртуалізація. Використання віртуалізації при розробці систем управління доступу.

2. Збереження та керування віртуалізації VMware Workstation в системах доступу корпоративних мереж?

3. Обмеження на встановлення та розгортання ОС мають середовищі VMware Workstation?

4. Статична IP маршрутизація для серверів розмежування доступу на базі технології AD в КМ.

5. Фізичне розташування DNS-серверів та AD WS в корпоративних мережах.

6. Віртуальна маршрутизація та алгоритм його налаштування в корпоративних мережах.

7. Спеціалізовані ролі серверів в КМ.

8. Призначення DNS-сервера в корпоративній мережі та його роль при створенні корпоративних систем розмежування доступу.

9. Спеціалізовані ролі серверів ОС Windows Server в КМ.

10. Функції реалізації серверів додатків Windows Server 2012 r2.

11. Правила політик безпеки для створення шляхів до каталогів, де розташовано Active Directory.

12. Роль контролера домену (DC) та його компоненти в корпоративних мережах на базі Windows Server?

13. Ліс доменів. Призначення та зв'язок між лісом та технології AD.

14. Встановлення ролей Active Directory Domain Services для серверів по стандартам корпоративної системи.

15. Встановлення статичної IP-адреси в налаштуваннях мережного підключення початком встановлення ролі Active Directory Domain Services.

16. Алгоритм створення користувачів та правила їх іменування та алгоритм додавання користувача в групу доступу.

17. Поняття та принципи формування функціональних груп при реалізації політик доступу в WS?

18. Парольні політики. Приклади формування парольних політик для груп доступу в WS.

19. Принципи початкових налаштувань загальної парольної політики користувачів.

20. Роль функціональних груп в системі розмежування доступу Windows Server 2012.

21. Типи груп користувачі існують в Active Directory, їх особливості.

22. Фізичні та логічні диски в системах управління доступу.

23. Реплікація даних та відмінність технології реплікації від механізму резервного копіювання?

24. Об’єкти доступу для учасників корпоративної мережі.

25. Механізми створення та розмежування доступу до дискової корпоративної інформації. Розробка та налаштування RAID-масивів.

26. Субдомен, створення субдоменів при конфігуруванні механізмів керування даними в КМ.

27. Основні конфігурації для простору доступу в КМ на базі технології AD та їх призначення.

28. Призначення та принцип роботи протоколами авторизації при функціонуванні систем розмежування доступу

29. Адміністрування облікових записів користувачів. Управління парольними та авторизаційними політиками КМ.

30. Правила та механізми створення групових політик для учасників корпоративної мережі.

8. Методи навчання

Виконання лабораторних робіт з використанням наочних технічних засобів навчання у вигляді систем моделювання на базі програмних та апаратних засобів віртуалізації та маршрутизації трафіку; виконання індивідуальних навчально-дослідних завдань.

9. Форми контролю

Систематичний контроль за самостійною роботою студентів і якістю засвоєння ними поточного навчального матеріалу:

- на лабораторних роботах шляхом перевірки підготовки до виконання роботи;
- роботу над індивідуальними завданнями по лабораторним роботам;
- вивчення літератури, що рекомендувалася, та конспекту лекцій;
- оформлення звітів по лабораторним робота;

Поточний контроль знань студентів проводиться:

- на лабораторних роботах оцінюється підготовка до роботи, обсяг її виконання, результати захисту звіту;
- на лекційних заняттях виконується вибіркове опитування студентів;
- шляхом проведення модульних контролів знань студентів та виставлення рейтингових оцінок знань студентів по усім видам занять.

Самостійна робота студентів передбачає:

- систематичне відвідання усіх видів аудиторних занять і ведення конспекту лекцій;
- систематичне вивчення лекційного матеріалу і навчальної літератури, що рекомендуються;
- сумлінну підготовку до лабораторних занять;
- вчасне і якісне оформлення звітів про лабораторні роботи.

10. Розподіл балів, які отримують студенти.

Оцінювання студента відбувається згідно положення «Про екзамени та заліки у НУБіП України» від 27.02.2019р. протокол №7.

національна	Рейтинг здобувача вищої освіти, бали
Відмінно	**90-100**
Добре	**74-89**
Задовільно	**60-73**
Незадовільно	**0-59**

Для визначення рейтингу студента із засвоєння дисципліни $R_{дис}$ (до 100 балів) одержаний рейтинг з атестації $R_{АТ}$ (до 30 балів) додається до рейтингу студента з навчальної роботи $R_{НР}$ (до 70 балів): $R_{дис}=R_{НР}+R_{АТ}$.

11.Методичне забезпечення

1. Методичні вказівки до виконання лабораторних робіт з курсу «Управління доступом». - Київ, НУБіП, 2022, 86 с.
2. Конспект лекцій з курсу «Управління доступом». - Київ, НУБіП, 2022.

12.Рекомендована література

1. Трегубенко, І. Б. Безпека корпоративних мереж. Служба каталогу Active Directory [Електронний ресурс] : навч. посіб. / І. Б. Трегубенко, О. В. Коваль ; М-во освіти і науки України, Черкас. держ. технол. ун-т. – Черкаси : ЧДТУ, 2010. – 319 с. – ISBN 978-966-402-067-8.

2. Гребенюк А.М. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. – 144 с.

3. Черних О.О. Онлайк: навчально-методичний посібник., К.: BAITE, 2020. – 108 с. https://www.osce.org/files/f/documents/0/f/483533.pdf

Інформаційні ресурси

1. https://elearn.nubip.edu.ua/course/view.php?id