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

ЗАТВЕРДЖЕНО
Факультет інформаційних технологій
02 червня 2025 р

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Навчальна практика з проектування систем кібербезпеки»

Галузь знань _____12 Інформаційні технології
Спеціальність ___123 Кібербезпека_____
Освітня програма _____«Кібербезпека»_____
Факультет (ННІ)_____інформаційних технологій_____
Розробники: _____доцент, к.т.н., доцент, Сагун А.В._____
(посада, науковий ступінь, вчене звання)

Київ – 2025 р.

Опис навчальної дисципліни

Дисципліна вивчає практичні онови технологій проектування систем захисту інформації в інформаційно-комунікаційних системах та мережах відповідно до вимог чинних нормативних документів. В якості основи проектування використана технологія захисту даних в корпоративних мережах Active Directory.

Галузь знань, спеціальність, освітня програма, освітній ступінь		
Освітній ступінь	*бакалавр*	
Спеціальність	*125 «Кібербезпека та захист інформації», F5-«Кібербезпека»*	
Освітня програма	*Кібербезпека*	
Характеристика навчальної дисципліни		
Вид	обов'язкова	
Загальна кількість годин	150	
Кількість кредитів ECTS	5	
Кількість змістових модулів	3	
Курсовий проект (робота) (за наявності)	-	
Форма контролю	*залік*	
Показники навчальної дисципліни для денної та заочної форм здобуття вищої освіти		
	Форма здобуття вищої освіти	
	денна	**заочна**
Курс (рік підготовки)	2	-
Семестр	4	-
Лекційні заняття	- *год.*	*год.*
Практичні, семінарські заняття	*150 год.*	*год.*
Лабораторні заняття	- *год.*	*год.*
Самостійна робота	- *год.*	*год.*
Кількість тижневих аудиторних годин для денної форми здобуття вищої освіти	- *год.*	

1. Мета, компетентності та програмні результати навчальної дисципліни

Мета вивчення дисципліни «Навчальна практика з проектування систем кібербезпеки» є вивчення технологій проектування систем захисту інформації в інформаційно-комунікаційних системах та мережах відповідно до вимог чинних нормативних документів, принципів планування та побудови захищених корпоративних мереж на базі технології Active Directory. Розглядаються основи планування та впровадження систем кібербезпеки на підприємствах різних форм бізнесу і діяльності, технології захисту конфіденційності, цілісності.

Набуття компетентностей:

Інтегральна компетентність (ІК): Здатність комплексно застосовувати знання, навички та методи проєктування систем кібербезпеки на основі чинного законодавства, стандартів і професійних практик, з урахуванням сучасних загроз, технічних та програмно-апаратних рішень, забезпечуючи розробку, впровадження, моніторинг та відновлення функціонування інформаційно-телекомунікаційних систем відповідно до політики інформаційної та/або кібербезпеки, з дотриманням вимог ефективного професійного спілкування та аналітичного мислення.

Загальні компетентності (ЗК): здатність застосовувати знання у практичних ситуаціях; знання та розуміння предметної області та розуміння професії; здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово; вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням; здатність до пошуку, оброблення та аналізу інформації; здатність до абстрактного і системного мислення, аналізу та синтезу.

Спеціальні (фахові) компетентності (СК): здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки; здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки; здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах; здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки; здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження; Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.); здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою; здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки; здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки; здатність розробляти апаратне, алгоритмічне та програмне забезпечення, компоненти комп’ютерних систем захисту інформації.

Програмні результати навчання (ПРН): організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність; аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності; використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності. Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації; застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки; збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи; вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

2. Програма та структура навчальної дисципліни

Назви змістових модулів і тем	**Кількість годин**												
	денна форма							**заочна форма**					
	тижні	усього	у тому числі					усього	у тому числі				
			л	п	лаб	інд	с.р.		л	п	лаб	інд	с.р.
Змістовий модуль 1. Планування та аналіз мережевих технологій для створення захищеної ІКС													
Тема 1. Визначення моделі загроз, порушника. Формування моделі захищеної корпоративної мережі підприємства	1	15		15									
Тема 2. Аналіз та планування комунікаційної складової захищеної корпоративної мережі (КМ). Вибір середовищі моделювання та	1	15		15									

віртуалізації процесів захисту													
Тема 3. Визначення типу та рівня гарантування послуг безпеки функціонального профіля захищеності КМ за НД ТЗІ 2.4-005-99	2	10		10									
Тема 4. Визначення серверних ролей та компонент для забезпечення функціональності проектного рішення системи розмежування доступу до корпоративної інформації засобами Windows Server (враховуючи модель загроз).	2	15		10									
Разом за змістовим модулем 1		**50**		**50**									
Змістовий модуль 2. Моделі функціонування та захисту інформаційних ресурсів підприємств													
Тема 5. Планування та розгортання ефективної доменної структури КМ	2	5		5									
Тема 6. Визначення користувачів та функціональних груп доступу до захищених ресурсів ІКС	3	10		10									
Тема 7. Розробка механізмів авторизації та парольних політик користувачів корпоративної комп'ютерної мережі	3	15		15									
Тема 8. Організація захищених сховищ корпоративної інформації.. Проектування та реалізація RAID-масивів	4	10		10									
Тема 9. Проектування та організація системи розмежування доступу до корпоративних файлових ресурсів та периферійних пристроїв загального користування на базі технології AD	4	10		10									
Разом за змістовим модулем 2		**50**		**50**									
Змістовий модуль 3. Проектування та застосування групових та корпоративних політик безпеки та систем розмежування доступу													
Тема 10. Налаштування механізмі корпоративної безпеки служби каталогів AD: об'єкти та групові політики для доступу в	5	20		20									

рамках корпоративної мережевої ОС. Групові та локальні політики доступу.													
Тема 11. Механізми захисту корпоративних ресурсів з використанням технологій резервування та реплікації	6	15		15									
Тема 12. Налаштування засобів захисту розсилань електронної пошти на базі корпоративної e-mail серверу MS Exchange	6	15		15									
Разом за змістовим модулем 3		**50**		**50**									
Всього годин за курс		**150**	**-**	**150**	**-**		**-**						

3. Теми лекцій не передбачені навчальним планом

4. Теми лабораторних занять (не передбачені навчальним планом)

5. Теми самостійної роботи (не передбачені навчальним планом)

6. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	Визначення моделі загроз, порушника корпоративної комп'ютерної мережі	15
2	Вибір і розгортання фізичної інфраструктури корпоративної комп'ютерної мережі на базі технологій віртуалізації	15
3	Визначення типу та рівня гарантування послуг безпеки функціонального профіля захищеності КМ за НД ТЗІ 2.4-005-99	10
4	Планування фізичної та організаційної структури мережі	5
5	Встановлення ролей та компонентів Active Directory WS 2012 r2 та створення каталогу AD та контролера домену DC в середовищі Windows Server 2012 r2	10
6	Дочірні домени та об'єктів для групових політик доступу	15
7	Організація облікових записів та груп користувачів в корпоративних мережах	10
7	Організація захищених сховищ корпоративної інформації. RAID-масиви	15
8	Проектування та організація системи розмежування доступу до корпоративних файлових ресурсів та периферійних пристроїв загального користування на базі технології AD	10
9	Адміністрування облікових записів користувачів. Управління парольними та авторизаційними політиками КМ	10
10	Створення групових політик для учасників корпоративної мережі	15
11	Захист даних контролера домена WS. Реплікація контролера домену	15
12	Встановлення та налаштування корпоративного поштового серверу MS Exchange	10
	Разом	**150**

7. Теми семінарських занять (не передбачені навчальним планом)

8. Методи та засоби діагностики результатів навчання:

(вибрати необхідне чи доповнити)

- усне та письмове опитування;
- співбесіда;
- тестування;
- захист практичних робіт.

9. Методи навчання *(вибрати необхідне чи доповнити):*

- метод проблемного навчання;
- метод практико-орієнтованого навчання;
- метод командної роботи, мозкового штурму
- метод гейміфікованого навчання.

10. Оцінювання результатів навчання.

Оцінювання знань здобувача вищої освіти відбувається за 100-бальною шкалою і переводиться в національну оцінку згідно чинного «Положення про екзамени та заліки у НУБіП України».

10.1 Розподіл балів за видами навчальної діяльності

Вид навчальної діяльності	Результати навчання	Оцінювання
Змістовий модуль 1. Планування та аналіз мережевих технологій для створення захищеної ІКС		
Практична робота 1 - Визначення моделі загроз, порушника корпоративної комп'ютерної мережі	організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність;	5
Практична робота 2 - Вибір і розгортання фізичної інфраструктури корпоративної комп'ютерної мережі на базі технологій віртуалізації	вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.	7
Практична робота 3 - Визначення типу та рівня гарантування послуг безпеки функціонального профіля захищеності КМ за НД ТЗІ 2.4-005-99	Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.); здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою;	4
Практична робота 4 - Планування	аналізувати, аргументувати, приймати	5

фізичної та організаційної структури мережі	рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення	
Всього за модулем 1		**21**
Змістовий модуль 2. Моделі функціонування та захисту інформаційних ресурсів підприємств		
Практична робота 5 - Встановлення ролей та компонентів Active Directory WS 2012 r2 та створення каталогу AD та контролера домену DC в середовищі Windows Server 2012 r2	Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації;	5
Практична робота 6 - Дочірні домени та об'єктів для групових політик доступу	застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки	6
Практична робота 7 - Організація облікових записів та груп користувачів в корпоративних мережах	організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність;	5
Практична робота 8 - Організація захищених сховищ корпоративної інформації. RAID- масиви	збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи;	6
Практична робота 9 - Проектування та організація системи розмежування доступу до корпоративних файлових ресурсів та периферійних пристроїв загального користування на базі технології AD	застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності;	5
Всього за модулем 2		27
Змістовний модуль 3. Проектування та застосування групових та корпоративних політик безпеки та систем розмежування доступу		
Практична робота 10 - Адміністрування облікових записів користувачів. Управління парольними та авторизаційними політиками КМ	організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність;	**5**
Практична робота 11 - Створення групових політик для учасників корпоративної мережі		**5**
Практична робота 12 - Захист даних контролера домена WS. Реплікація контролера домену	Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі,	**7**

	вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.	
Практична робота 13 - Встановлення та налаштування корпоративного поштового серверу MS Exchange	Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації; застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки	**6**
Всього за модулем 3		**23**
		(М1 + М2)*0,7 ≤ 70
Залік		**30**
Всього за курс		**(Навчальна робота + екзамен) ≤ 100**

10.2Шкала оцінювання знань здобувача вищої освіти

Рейтинг здобувача вищої освіти, бали	Оцінка за національною системою (екзамени/заліки)
90-100	відмінно
74-89	добре
60-73	задовільно
0-59	незадовільно

10.3Політика оцінювання

Політика щодо дедлайнів та перескладання	Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (пропорційно інтервалів пропущеної дати складання). Перескладання модульних контрольних та тестів відбувається із дозволу лектора за наявності поважних причин (наприклад, лікарняний).
Політика щодо академічної доброчесності	Списування під час заліку заборонено (в т.ч. із використанням мобільних девайсів). Практичні роботи мають бути виконані виключна за індивідуальними завданнями варіантів.
Політика щодо відвідування	Відвідування занять є обов'язковим. За об'єктивних причин (хвороба, участь в заходах від кафедри або факультету, міжнародне стажування). В узгоджених офіційно випадках навчання може відбуватись індивідуально (в он-лайн формі)

11. Навчально-методичне забезпечення

Електронний навчальний курс навчальної дисципліни (на навчальному порталі НУБіП України eLearn https://elearn.nubip.edu.ua/course/view.php?id=5066), що складається з:

- навчальний посібник та методичні рекомендації (в електронному вигляді);
- завдання для виконання практичних робіт;
- блоку підсумкового оцінювання знань (залік);
- методичні матеріали щодо вивчення навчальної дисципліни для здобувачів вищої освіти денної та заочної форм здобуття вищої освіти;
- програма навчальної дисципліни.

12. Рекомендовані джерела інформації

Електронний навчальний курс навчальної дисципліни (на навчальному порталі НУБіП України eLearn - https://elearn.nubip.edu.ua/enrol/index.php?id=5066), що складається з:

- лекцій та їх презентації (в електронному вигляді);
- завдань для виконання практичних робіт;
- блоку підсумкового оцінювання знань.
- методичні матеріали щодо вивчення навчальної дисципліни для здобувачів вищої освіти всіх форм навчання вищої освіти;
- програма навчальної дисципліни.

13.Рекомендовані джерела інформації

1. Операційні системи та комп’ютерні мережі [Електронний ресурс]: навчальний посібник для здобувачів ступеня бакалавра за освітньою програмою «Автоматизація та комп’ютерно-інтегровані технології кібер-енергетичних систем» спеціальності 151 «Автоматизація та комп’ютерно-інтегровані технології», освітньо-професійною програмою / КПІ ім. Ігоря Сікорського; уклад. А. В. Сагун, В. Б. Бобков. – Електронні текстові данні (1 файл 10 Мбайт). – Київ : КПІ ім. Ігоря Сікорського», 2022. – 164 с. – Назва з екрана.