НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра комп'ютерних систем, мереж та кібербезпеки

"ЗАТВЕРДЖУЮ"
Декан факультету інформаційних технологій
_____ проф. О.Г. Глазунова
"___" _____ 2023 р.

НАВЧАЛЬНО-МЕТОДИЧНИЙ КОМПЛЕКС

з дисципліни

«НАВЧАЛЬНА ПРАКТИКА З ПРОЕКТУВАННЯ СИСТЕМ КІБЕРБЕЗПЕКИ»

для підготовки бакалаврів за спеціальністю 125 «Кібербезпека»

КИЇВ-2023

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Кафедра комп'ютерних систем, мереж та кібербезпеки

"ЗАТВЕРДЖУЮ"
Декан факультету інформаційних технологій
_____ проф. О.Г. Глазунова
"__" _____ 2023 р.

СХВАЛЕНО
на засіданні кафедри
комп'ютерних систем, мереж та кібербезпеки
Протокол №10 від "17" травня 2023 р.
Завідувач кафедри
(доц. Касаткін Д.Ю.)

РОЗГЛЯНУТО
Гарант ОП
«Кібербезпека»
_____
Гарант ОП
_____ (проф. Лахно В.А.)

«НАВЧАЛЬНА ПРАКТИКА З ПРОЕКТУВАННЯ СИСТЕМ КІБЕРБЕЗПЕКИ»

Спеціальність	125 - Кібербезпека
Освітня програма	Кібербезпека
Факультет	інформаційних технологій
Розробник:	Сагун А.В., к.т.н., доцент

Київ – 2023

Опис навчальної дисципліни

«НАВЧАЛЬНА ПРАКТИКА З ПРОЕКТУВАННЯ СИСТЕМ КІБЕРБЕЗПЕКИ»

Галузь знань, спеціальність, освітня програма, освітній ступінь		
Освітній ступінь	Бакалавр	
Галузь знань	12 – Інформаційні технології	
Спеціальність	125 – 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) (якщо є в робочому навчальному плані)	-	
Форма контролю	залік	
Показники навчальної дисципліни для денної та заочної форм навчання		
	денна форма навчання	заочна форма навчання
Рік підготовки	2	
Семестр	4	
Лекційні заняття, год.	-	
Практичні, семінарські заняття	150	
Лабораторні заняття, год.	-	
Самостійна робота, год.	-	
Індивідуальні завдання	-	
Кількість тижневих аудиторних годин для денної форми навчання	30 (5 тижнів)	

1. Мета, завдання та компетентності навчальної дисципліни

Мета: вивчення технологій проектування систем захисту інформації в інформаційно-комунікаційних системах та мережах відповідно до вимог чинних нормативних документів, дослідження проблем зберігання, опрацювання, пошуку, передачі, перетворення, закриття та відновлення інформації в організаціях і на підприємствах різних напрямків діяльності та різних форм власності, механізмів захисту конфіденційності, цілісності та доступності інформаційних активів.

Завдання навчальної дисципліни: навчитися аналізувати та застосовувати на практиці стандарти та механізми аналізу вразливостей та захищеності інформаційних активів; навчитися розробляти моделі функціонування та захисту інформаційних ресурсів підприємств, Отримати вміння тестування механізмів захисту та розробки організаційних засобів захисту інформації.

В результаті вивчення навчальної дисципліни студент повинен

знати:

- стандарти та механізми аналізу вразливостей та захищеності інформаційних активів
- моделі функціонування та захисту інформаційних ресурсів підприємств
- методи ефективного рішення спеціалізованих задач професійної діяльності;
- основні теорії, принципи, методи і поняття в галузі кібербезпеки.

вміти:

- розробляти моделі загроз та порушника інформаційної безпеки корпоативної мережі;
- готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки;
- проводити аудит і тестування механізмів захисту конфіденційності, цілісності та доступності інформації;
- розробляти та впроваджувати організаційні методи захисту інформації.

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 застосовувати знання у практичних ситуаціях.

ЗК 2. Знання та розуміння предметної області та розуміння професії.

ЗК 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.

ЗК 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

ЗК 5. Здатність до пошуку, оброблення та аналізу інформації.

ЗК 8. Здатність до абстрактного і системного мислення, аналізу та синтезу.

Спеціальні (фахові, предметні) компетентності (СК):

СК1. 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.

СК2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

СК3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

СК5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

СК6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

СК7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

СК9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.

СК11. . Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

СК12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

СК13. Здатність розробляти апаратне, алгоритмічне та програмне забезпечення, компоненти комп'ютерних систем захисту інформації.

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

ПРН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.

ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

ПРН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.

ПРН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.

ПРН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.

ПРН 12. Розробляти моделі загроз та порушника.

ПРН 21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

ПРН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-

телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.

ПРН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційнотелекомунікаційних (автоматизованих) системах.

ПРН 24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).

ПРН 25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.

ПРН 26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційнотелекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.

ПРН 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.

ПРН 33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.

ПРН 34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.

ПРН 35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і/або кібербезпеки.

ПРН 56. Виявляти небезпечні сигнали технічних засобів.

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 «Навчальна практика з проектування систем кібербезпеки» є курси «Інформаційна безпека держава», «Комплексні системи захисту інформації», «Методи та засоби захисту інформації», «Інформаційні технології» ОПП першого (бакалаврського) рівня вищої освіти.

2. Програма та структура навчальної дисципліни

– повного терміну денної (заочної) форми навчання;

Назви змістових модулів і тем	Кількість годин												
	денна форма							Заочна форма					
	тиж-ні	всього	у тому числі					всього	у тому числі				
			л	п	лр	інд	с.р.		л	п	лр	інд	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13	14
Змістовий модуль 1. **Стандарти та механізми аналізу вразливостей та захищеності інформаційних активів**													
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 віртуалізації процесів захисту	1	15		15									
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		15									
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	15		15									
Тема 6. Визначення користувачів та функціональних груп доступу до захищених ресурсів ІКС	3	10		10									
Тема 7. Розробка механізмів авторизації та парольних політик користувачів	3	15		15									

корпоративної комп'ютерної мережі													
Тема 8. Організація захищених сховищ корпоративної інформації.. Проектування та реалізація RAID-масивів	4	10		10									
Разом за змістовим модулем 2		**50**		**50**									
Змістовий модуль 2. Тестування механізмів захисту. Організаційні засоби захисту інформації													
Тема 9. Налаштування механізмі корпоративної безпеки служби каталогів AD: об'єкти та групові політики для доступу в рамках корпоративної мережевої ОС. Групові та локальні політики доступу.	4	20		20									
Тема 10. Механізми захисту корпоративних ресурсів з використанням технологій резервування та реплікації	4	15		15									
Тема 11. Налаштування засобів захисту розсилань електронної пошти на базі корпоративної e-mail серверу MS Exchange	5	15		15									
Разом за змістовим модулем 3		**50**		**50**									
Всього годин		**150**	**-**	**150**	**-**		**-**						

3. Теми лабораторних занять

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

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
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	Встановлення ролей та компонентів Active Directory WS 2012 r2 та створення каталогу AD та контролера домену DC в середовищі Windows Server 2012 r2	15
5	Дочірні домени та об'єктів для групових політик доступу	15
6	Організація облікових записів та груп користувачів в корпоративних мережах	10
7	Організація захищених сховищ корпоративної інформації. RAID- масиви	15
8	Адміністрування облікових записів користувачів. Управління парольними та авторизаційними політиками КМ	10
9	Створення групових політик для учасників корпоративної мережі	20
10	Захист даних контролера домена WS. Реплікація контролера домену	15
11	Встановлення та налаштування корпоративного поштового серверу MS Exchange	15
	Разом	**150**

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

6.1. Питання для перевірки знань студентів

1. Методики та засоби аналізу та аудиту інформаційних web-ресурсів.
2. Механізми захисту інформаційного контенту web-ресурсу. Захист конфіденційності, цілісності та доступності.
3. Сканування вразливостей web-ресурсу.
4. Стандарти захисту конфіденційності та цілісності інформаційних активів підприємств.
5. Засоби та методи аналізу вразливостей та механізмів захисту web-ресурсів.
6. Методи самоаналізу запропонованих механізмів захисту web-ресурсу.
7. Розробка моделі порушника та загроз ІБ для інформаційної системи підприємства.
8. Розробка та налаштування штатних механізмів захисту цілісності та конфіденційності web-ресурсу.
9. Платформи та хостінгу для розміщення корпоративного web-ресурсу. Нормативні вимоги безпеки для хостінг-платформ.
10. Методика самоаналізу розроблених механізмів захисту інформаційного ресурсу.
11. Методи та засоби тестування функціональності захищеного web-ресурсу та розроблених механізмів захисту.
12. Проектування процедури інтеграції захищеного web-ресурсу в загальну інформаційну структуру підприємства**.**

13. Організаційні методи захисту інформаційних активів та web-сторінок.

14. Політики безпека. Алгоритм розробки змін до політики безпеки підприємства в частині захисту інформаційних ресурсів

15. Тести перевірки рівня знань з інформаційної безпеки.

16. Складання тесту перевірки знань з ІБ оператора захищеного web-ресурсу.

17. Методика самоаналізу результатів тестування ресурсів та організаційних засобів захисту.

7. Методи навчання

Виконання практичних робіт з використанням утиліт відбувається з використанням діючих нормативно-правових документів в галузі захисту інформації та кібербезпеки, фізичних та віртуальних центрів обробки даних та спеціалізованих ІКС, що сертифіковані органами ДСЗУ України; виконання індивідуальних навчально-дослідних завдань.

8. Форми контролю

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

- на практичних роботах шляхом перевірки підготовки до виконання роботи;
- роботу над індивідуальними завданнями практичних робіт;
- вивчення літератури, що рекомендувалася та нормативних галузевих документів;
- оформлення звіту про виконання практики;
- публічний захист звіту з навчальної практика з проектування систем кібербезпеки.

9. Розподіл балів, які отримують студенти.

Оцінювання знань студента відбувається за 100-бальною шкалою і переводиться в національні оцінки згідно з табл.1 «Положення про екзамени та заліки у НУБіП України» (наказ про уведення в дію від 27.12.2019 р. № 1371):

Рейтинг здобувача вищої освіти, бали	Оцінка національна за результати складання екзаменів заліків	
	Екзамен	Залік
90-100	Відмінно	зараховано
74-89	Добре	
60-73	Задовільно	
0-59	незадовільно	не зараховано

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): $R_{дис}=R_{НР}+R_{АТ}$.

10. Методичне забезпечення

1. Конспект лекцій з курсу "основи криптоаналізу". - Київ, НУБіП, 2021 (elearn.nubip.edu.ua/course/view.php?id)

11. Рекомендована література

Основна

1. ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements. Technical Committee : ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection [Edition : 2], 2013, 23 p. Access via: https://www.iso.org/ru/isoiec-27001-information-security.html
2. Закон «Про інформацію»: від 2 жовтня 1992 р. №2657-XII // Відомості Верховної Ради України, 1992. – № 48. – С. 650.
3. Закон України «Про доступ до публічної інформації» // Відомості Верховної Ради України (ВВР), 2011, № 32, ст. 314. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2939-17#Text
4. Закон України «Про захист інформації в автоматизованих системах» // Відомості Верховної Ради України, 1994. - № 31. – С. 286.
5. Закон України «Про захист персональних даних» // Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17#Text
6. Закон України «Про основні засади забезпечення кібербезпеки України» //Відомості Верховної Ради (ВВР), 2017, № 45, ст.403 Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text

7. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 2.5-004-99. ДСТСЗІ СБ України, Київ. – 1999.

8. НД ТЗІ 2.5-005-99. «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу». - 1999. Київ. – 22 с.

9. НД ТЗІ 2.6-002-2015. Порядок зіставлення функціональних компонентів безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99. ДСТСЗІ СБ України. Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, Київ. – 2016.

10. А.В. Сагун, В.Б. Бобков. Операційні системи та комп'ютерні мережі [навчальний посібник] : 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. – Електронні текстові данні (1 файл 10 Мбайт). – Київ : КПІ ім. Ігоря Сікорського», 2021. – 164 с. – Назва з екрана.

Допоміжна

1. Фільштінський В. А. Математичні основи криптографії: конспект лекцій для студ. спец. 7.080202 "Прикладна математика" денної форми навчання / В. А. Фільштінський, А. В. Бережний.– Суми: СумДУ, 2011. – 138 с.

2. Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C. – John Wiley & Sons, 2015. – 784 p. – URL: https://books.google.com.ua/books?id=VjC9BgAAQBAJ&printsec =frontcover&hl=uk#v=onepage&q&f=false

3. Swenson C. Modern Cryptanalysis: Techniques for Advanced Code Breaking. – Wiley Publishing, Inc., 2008. – 264 p. – URL: https://books.google.com.ua/books?id=BuceBTs4ZwC&printsec=frontcover&hl=uk#v=onepage&q&f=false

Інформаційні ресурси

https://elearn.nubip.edu.ua/course/view.php?id=5066