НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Кафедра комп'ютерних систем, мереж та кібербезпеки

ЗАТВЕРДЖУЮ
Декан факультету
_____ Ігор Болбот
"___" _____ 2026 р.

СХВАЛЕНО
на засіданні кафедри
Кафедра комп'ютерних систем, мереж та кібербезпеки
Протокол №___ від "___" _____ 2026 р.
Завідувач кафедри
_____ Дмитро Касаткін

РОЗГЛЯНУТО
Гарант ОП «Комп’ютерні системи захисту інформації » _____
Валерій Лахно

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

КОМПЛЕКСНІ СИСТЕМИ САНКЦІОНОВАНОГО ДОСТУПУ ДО ІНФОРМАЦІЇ

Галузь знань F Інформаційні технології
Спеціальність F7 Комп’ютерна інженерія
Освітня програма Комп’ютерні системи ЗІ
Факультет Інформаційних технологій

Київ - 2026 р.

Опис навчальної дисципліни

Дисципліна «Комплексні системи санкціонованого доступу до інформації» є вибірковим компонентом освітньої програми «Комп'ютерні системи захисту інформації» для студентів другого (магістерського) рівня спеціальності F7 Комп'ютерна інженерія та спрямована на формування глибоких знань у галузі забезпечення безпеки інформаційних систем. Вона охоплює основи теорії та практики реалізації систем контролю доступу, включаючи концепції автентифікації, авторизації, аудитування, а також сучасні моделі та протоколи безпеки, такі як RBAC, ABAC, криптографічні методи та стандарти ISO/IEC. Особлива увага приділяється проектуванню та аналізу комплексних систем безпеки, їхньому впровадженню у корпоративному середовищі та забезпеченню захищеності даних у мережевих структурах. Навчання спрямоване на формування здатності розробляти та впроваджувати ефективні механізми захисту інформації з урахуванням правових, технічних і економічних аспектів, що має прикладне значення для створення сучасних безпечних інформаційних систем та мереж.

Галузь знань, спеціальність, освітня програма, освітній ступінь

Освітній ступінь	Другого (магістерського) ОП
Галузь знань	F Інформаційні технології
Спеціальність	F7 Комп'ютерна інженерія
Освітня програма	Комп'ютерні системи захисту інформації
Факультет/ННІ	Інформаційних технологій

Характеристика навчальної дисципліни

Вид	Вибіркова
Загальна кількість годин	150
Кількість кредитів ECTS	5
Кількість змістових модулів	2
Курсовий проект (робота) (за наявності)	-
Форма контролю	Екзамен

Показники навчальної дисципліни для денної та заочної форм здобуття вищої освіти (повний термін навчання)

	Форма здобуття вищої освіти	
	денна	**заочна**
Курс (рік підготовки)	1	-
Семестр	2	-
Лекційні заняття	20 год.	-
Лабораторні роботи	30 год.	-
Практичні, семінарські заняття	-	-
Самостійна робота	100 год.	-
Кількість тижневих аудиторних годин для денної форми здобуття вищої освіти	3 год.	-
Форма контролю	Екзамен	-

Мета, компетентності та програмні результати навчальної дисципліни

Мета: Мета дисципліни полягає у формуванні у студентів системного розуміння принципів та засобів забезпечення санкціонованого доступу до інформаційних систем, здатності аналізувати та проектувати відповідні механізми захисту, а також застосовувати сучасні методи і технології для розв’язання проблем безпеки інформаційних ресурсів у контексті комп’ютерних мереж і систем.

Перелік навчальних дисциплін, які передують вивченню «Комплексні системи санкціонованого доступу до інформації» (за їх наявності) ОК.2 Методологія наукових досліджень, ОК.3 Теорія і проєктування комп'ютерних систем і мереж, ОК.4 Технології програмування комп'ютерних систем

Набуття компетентностей

Програмні результати навчання

Програма та структура навчальної дисципліни

Назви змістових модулів і тем	**Кількість годин (денна форма)**						**Кількість годин (заочна форма)**					
	л	**лаб**	**сем**	**п**	**с.р.**	**усього**	**л**	**лаб**	**сем**	**п**	**с.р.**	**усього**
Модуль 1. Завдання та методологічні основи КСЗІ.												
Тема 1. Методологічні основи комплексної системи захисту інформації.	2	2	-	-	3	7	-	-	-	-	-	-

Назви змістових модулів і тем	Кількість годин (денна форма)						Кількість годин (заочна форма)					
	л	**лаб**	**сем**	**п**	**с.р.**	**усього**	**л**	**лаб**	**сем**	**п**	**с.р.**	**усього**
Тема 2. Визначення складу інформації, що захищається на підприємстві.	2	4	-	-	9	15	-	-	-	-	-	-
Тема 3. Джерела, способи і результати дестабілізуючого впливу на інформацію.	2	10	-	-	15	27	-	-	-	-	-	-
Тема 4. Канали і методи несанкціонованого доступу до інформації.	2	6	-	-	13	21	-	-	-	-	-	-
Тема 5. Технічні засоби комплексних системи санкціонованого доступу до інформації.	2	2	-	-	10	14	-	-	-	-	-	-
Разом за модулем 1	**10**	**24**	**0**	**0**	**50**	**84**	**-**	**-**	**-**	**-**	**-**	**-**
Модуль 2. Моделювання, технологічна побудова, апаратні компоненти КСЗІ.												
Тема 1. Моделювання процесів комплексної системи захисту інформації.	2	6	-	-	-	8	-	-	-	-	-	-
Тема 2. Технологічна побудова комплексної системи захисту інформації.	2	-	-	-	9	11	-	-	-	-	-	-
Тема 3. Управління комплексною системою захисту інформації.	2	-	-	-	17	19	-	-	-	-	-	-
Тема 4. Планування діяльності комплексної системи захисту інформації на підприємстві.	2	-	-	-	18	20	-	-	-	-	-	-
Тема 5. Управління комплексною системою захисту інформації в умовах таргетованих кібератак на підприємство.	2	-	-	-	6	8	-	-	-	-	-	-
Разом за модулем 2	**10**	**6**	**0**	**0**	**50**	**66**	**-**	**-**	**-**	**-**	**-**	**-**
Курсовий проект (робота)	-	-	-	-	-	-	-	-	-	-	-	-
Усього годин	**20**	**30**	**0**	**0**	**100**	**150**	**-**	**-**	**-**	**-**	**-**	**-**

Теми лекцій

№ з/п	Назва теми	Кількість годин
1	Тема 1. Методологічні основи комплексної системи захисту інформації.	2

№ з/п	Назва теми	Кількість годин
2	Тема 2. Визначення складу інформації, що захищається на підприємстві.	2
3	Тема 3. Джерела, способи і результати дестабілізуючого впливу на інформацію.	2
4	Тема 4. Канали і методи несанкціонованого доступу до інформації.	2
5	Тема 5. Технічні засоби комплексних системи санкціонованого доступу до інформації.	2
6	Тема 6. Моделювання процесів комплексної системи захисту інформації.	2
7	Тема 7. Технологічна побудова комплексної системи захисту інформації.	2
8	Тема 8. Управління комплексною системою захисту інформації.	2
9	Тема 9. Планування діяльності комплексної системи захисту інформації на підприємстві.	2
10	Тема 10. Управління комплексною системою захисту інформації в умовах таргетованих кібератак на підприємство.	2
Всього годин		**20**

Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Аналіз структури та складу інформації, що підлягає захисту, за допомогою інструментальних методів	2
2	Дослідження джерел та способів дестабілізуючого впливу на інформацію у комп’ютерних системах	2
3	Практичне дослідження каналів і методів несанкціонованого доступу до інформації в мережевих середовищах	2
4	Вивчення технічних засобів комплексної системи санкціонованого доступу до інформації на основі симуляційних моделей	2
5	Практичне дослідження методів і засобів виявлення та запобігання несанкціонованого доступу до інформації	2
6	Аналіз та порівняння методів забезпечення цілісності та конфіденційності інформації у системах захисту	2
7	Розробка та тестування прототипу системи контролю доступу до інформації з використанням сучасних технічних засобів	2
8	Дослідження та аналіз методів аутентифікації та авторизації у комплексних системах захисту інформації	2

№ з/п	Назва теми	Кількість годин
9	Практичне застосування засобів моніторингу та аудиту для забезпечення безпеки інформаційних систем	2
10	Розробка сценаріїв тестування системи захисту інформації та аналіз отриманих результатів	2
11	Дослідження та аналіз сучасних стандартів та протоколів забезпечення безпеки інформації	2
12	Практичне дослідження методів захисту від атак типу «людина посередині» та інших сучасних загроз	2
13	Моделювання процесів в системі захисту інформації за допомогою програмних інструментів	3
14	Технологічна побудова апаратних компонентів комплексної системи захисту інформації	3
Всього годин		**30**

Теми самостійної роботи

№ з/п	Назва теми	Кількість годин
1	Написати реферат про історію та сучасний стан методології КСЗІ.	9
2	Проаналізувати основні принципи та моделі забезпечення безпеки інформаційних систем.	9
3	Порівняти різні підходи до розробки політик доступу у КСЗІ.	8
4	Розрахувати рівень ризику для визначеної інформаційної системи на основі заданих параметрів.	8
5	Розробити схему або модель системи контролю доступу з урахуванням принципів КСЗІ.	8
6	Розв'язати практичну задачу з визначенням оптимальної стратегії захисту інформації в умовах обмежених ресурсів.	8
7	Аналіз сучасних технологій моделювання комплексних систем захисту інформації	9
8	Порівняльна характеристика апаратних компонентів КСЗІ	9
9	Розробка блок-схеми технологічної побудови системи захисту інформації	8
10	Розрахунок надійності та стійкості апаратних компонентів КСЗІ	8
11	Моделювання процесу інтеграції апаратних та програмних компонентів системи захисту	8
12	Розробка проекту прототипу моделі комплексної системи санкціонованого доступу	8

№ з/п	Назва теми	Кількість годин
Всього годин		**100**

Методи навчання

Методи та засоби діагностики результатів навчання:

- Усне опитування для перевірки розуміння теоретичних основ систем контролю доступу та концепцій безпеки.
- Тестування з вибором правильних відповідей для оцінки знань про моделі та протоколи безпеки (RBAC, ABAC, криптографічні методи).
- Комп'ютерне тестування для автоматизованої оцінки знань щодо стандартів ISO/IEC та сучасних технологій безпеки.
- Аналіз кейс-стаді для оцінки здатності застосовувати теоретичні знання до практичних ситуацій.
- Поточне оцінювання участі у дискусіях та практичних заняттях для визначення рівня активності та розуміння матеріалу.

Методи навчання:

- Лекційно-практичні заняття з демонстрацією сучасних систем безпеки та протоколів
- Практикуми з проектування та аналізу систем контролю доступу
- Модульне навчання з використанням сучасних інформаційних технологій та симуляторів
- Обговорення та дебати щодо сучасних викликів і тенденцій у сфері безпеки інформації
- Самостійна робота з аналізу стандартів і протоколів безпеки

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»

Розподіл балів за видами навчальної діяльності

Вид навчальної діяльності	Результати навчання	Оцінювання
Модуль 1. Завдання та методологічні основи КСЗІ.		
Лабораторна робота. Аналіз структури та складу інформації, що підлягає захисту, за допомогою інструментальних методів	ПРН 1, ПРН 2, ПРН 3. Модуль спрямований на ознайомлення студентів з основами теорії та методології комплексних систем захисту інформації (КСЗІ). Студенти здобудуть знання щодо структури та складу інформації, що підлягає захисту, дослідження джерел дестабілізуючого впливу, а також методів несанкціонованого доступу та їх запобігання. Вивчення технічних засобів та прототипування систем контролю доступу, а також аналіз стандартів і протоколів забезпечення безпеки інформації.	10
Лабораторна робота. Дослідження джерел та способів дестабілізуючого впливу на інформацію у комп’ютерних системах		10
Лабораторна робота. Практичне дослідження каналів і методів несанкціонованого доступу до інформації в мережевих середовищах		5
Лабораторна робота. Вивчення технічних засобів комплексної системи санкціонованого доступу до інформації на основі симуляційних моделей		5
Лабораторна робота. Практичне дослідження методів і засобів виявлення та запобігання несанкціонованого доступу до інформації		5
Лабораторна робота. Аналіз та порівняння методів забезпечення цілісності та конфіденційності інформації у системах захисту		5

Вид навчальної діяльності	Результати навчання	Оцінювання
Лабораторна робота. Розробка та тестування прототипу системи контролю доступу до інформації з використанням сучасних технічних засобів		5
Лабораторна робота. Дослідження та аналіз методів аутентифікації та авторизації у комплексних системах захисту інформації		5
Лабораторна робота. Практичне застосування засобів моніторингу та аудиту для забезпечення безпеки інформаційних систем		5
Лабораторна робота. Розробка сценаріїв тестування системи захисту інформації та аналіз отриманих результатів		5
Лабораторна робота. Дослідження та аналіз сучасних стандартів та протоколів забезпечення безпеки інформації		5
Лабораторна робота. Практичне дослідження методів захисту від атак типу «людина посередині» та інших сучасних загроз		5
Самостійна робота. Написати реферат про історію та сучасний стан методології КСЗІ.		5
Самостійна робота. Проаналізувати основні принципи та моделі забезпечення безпеки інформаційних систем.		5

Вид навчальної діяльності	Результати навчання	Оцінювання
Самостійна робота. Порівняти різні підходи до розробки політик доступу у КСЗІ.		5
Самостійна робота. Розрахувати рівень ризику для визначеної інформаційної системи на основі заданих параметрів.		5
Самостійна робота. Розробити схему або модель системи контролю доступу з урахуванням принципів КСЗІ.		5
Самостійна робота. Розв'язати практичну задачу з визначенням оптимальної стратегії захисту інформації в умовах обмежених ресурсів.		5
Всього за модулем 1		**100**
Модуль 2. Моделювання, технологічна побудова, апаратні компоненти КСЗІ.		
Лабораторна робота. Моделювання процесів в системі захисту інформації за допомогою програмних інструментів	ПРН 4, ПРН 5, ПРН 6. Модуль спрямований на ознайомлення студентів із методами моделювання, побудови та інтеграції апаратних компонентів систем захисту інформації. Студенти здобудуть навички моделювання процесів, аналізу технологічних рішень, розробки схем та проектів прототипів систем, а також оцінки їх надійності та стійкості.	20
Лабораторна робота. Технологічна побудова апаратних компонентів комплексної системи захисту інформації		20
Самостійна робота. Аналіз сучасних технологій моделювання комплексних систем захисту інформації		10
Самостійна робота. Порівняльна характеристика апаратних компонентів КСЗІ		10

Вид навчальної діяльності	Результати навчання	Оцінювання
Самостійна робота. Розробка блок-схеми технологічної побудови системи захисту інформації		10
Самостійна робота. Розрахунок надійності та стійкості апаратних компонентів КСЗІ		10
Самостійна робота. Моделювання процесу інтеграції апаратних та програмних компонентів системи захисту		10
Самостійна робота. Розробка проекту прототипу моделі комплексної системи санкціонованого доступу		10
Всього за модулем 2		**100**
Навчальна робота (разом за семестр)		**70**
Підсумковий екзамен		**30**
Разом за курс		**100**

Шкала оцінювання знань здобувача вищої освіти

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

Політика оцінювання

Політика щодо дедлайнів та перескладання:	Лабораторні, самостійні та модульні роботи необхідно здавати у заплановані терміни. Перескладання модульних робіт допускається за наявності поважних причин у визначені кафедрою строки.
Політика щодо академічної доброчесності:	Списування, використання сторонніх матеріалів і несанкціонованих пристроїв під час виконання контрольних робіт, заліку або екзамену заборонено.
Політика щодо відвідування:	Відвідування занять є обов’язковим. Пропуски відпрацьовуються згідно з індивідуальним графіком та правилами кафедри.

Навчально-методичне забезпечення

-електронний навчальний курс навчальної дисципліни (на навчальному порталі НУБіП України eLearn - https://elearn.nubip.edu.ua/course/view.php?id=4571);

Рекомендовані джерела інформації

1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [Електронний ресурс] / База законодавства України // № 80/94-ВР – Режим доступу: http://zakon4.rada.gov.ua/laws/show/80
2. Комплекс засобів захисту від НСД в АС класу 1 «Рубіж-РСО» версія 2 [Електронний ресурс] / ТОВ «Технічний захист інформації» // 2013 - Режим доступу: http://tzi.com.ua/rubzh-rso-versya20.html
3. Комплексні системи захисту інформації: проектування, впровадження, супровід. Збірник лекцій [Електронний ресурс] / Гребенніко В.В. // 2015 - Режим доступу: http:// 03-KSZI
4. Операційна система «OpenBSD, шифр BBOS» [Електронний ресурс] / Кампанія «ATMNIS» // 2012 - Режим доступу: http://www.atmnis.com/files/user files/BBOS overview.pdf
5. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. НД ТЗІ 3.7-003-05 [Електронний ресурс] / Нормативна база Держспецзв'язку // 2015 - Режим доступу:http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art id=46074