НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

комп'ютерних систем, мереж та кібербезпеки

ЗАТВЕРДЖУЮ	**СХВАЛЕНО**
Декан факультету	на засіданні кафедри комп'ютерних систем, мереж та кібербезпеки
_____ Ігор БОЛБОТ	Протокол №___ від "___" _____ 2026 р.
"___" _____ 2026 р.	Завідувач кафедри
	_____ Дмитро КАСАТКІН

РОЗГЛЯНУТО

Гарант ОП «Комп’ютерні системи захисту інформації»

_____ Валерій ЛАХНО

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

МЕТОДИ СТВОРЕННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Галузь знань F Інформаційні технології

Спеціальність F7 Комп’ютерна інженерія

Освітня програма Комп’ютерні системи захисту інформації

Факультет Інформаційних технологій

Київ — 2026 р.

Опис навчальної дисципліни

Дисципліна "Методи створення систем захисту інформації" – складова ОП магістратури з комп'ютерної інженерії. Вона спрямована на формування у студентів знань і навичок, необхідних для створення ефективних систем захисту інформації, здатних протистояти сучасним загрозам. У рамках курсу студенти ознайомляться з основними поняттями безпеки інформації, а також з методами аналізу ризиків, які дозволяють оцінити вразливості інформаційних систем. Курс також охоплює технічні засоби захисту, включаючи криптографічні алгоритми та системи виявлення атак. Окрім цього, важливу роль відіграють організаційні заходи безпеки, такі як політики безпеки та процедури реагування на інциденти.

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	Факультет Інформаційних технологій

Характеристика навчальної дисципліни

Вид	Обов'язкова
Загальна кількість годин	180
Кількість кредитів ECTS	6
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	1	—
Лекційні заняття	15 год.	—
Практичні, семінарські заняття	–	—
Самостійна робота	135 год.	—
Кількість тижневих аудиторних годин для денної форми здобуття вищої освіти	9 год.	—
Форма контролю	Екзамен	—

Мета, компетентності та програмні результати навчальної дисципліни

Мета: Метою дисципліни “Методи створення систем захисту інформації” є отримання магістрами компетентностей в області практичного створення систем технічного захисту інформації.

Перелік навчальних дисциплін, які передують вивченню «Методи створення систем захисту інформації» (за їх наявності)

Набуття компетентностей

ЗК2 — Здатність до абстрактного мислення, аналізу і синтезу.

ЗК3 — Здатність проводити дослідження на відповідному рівні.

ЗК4 — Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ЗК5 — Здатність генерувати нові ідеї (креативність).

ЗК6 — Здатність виявляти, ставити та вирішувати проблеми.

ЗК7 — Здатність приймати обґрунтовані рішення.

СК1 — Здатність до визначення технічних характеристик, конструктивних особливостей, застосування і експлуатації програмних, програмно-технічних засобів, комп’ютерних систем та мереж різного призначення.

СК2 — Здатність розробляти алгоритмічне та програмне забезпечення, компоненти комп’ютерних систем та мереж, Інтернет додатків, кіберфізичних

систем з використанням сучасних методів і мов програмування, а також засобів і систем автоматизації проектування.

СК3 — Здатність проектувати комп’ютерні системи та мережі з урахуванням цілей, обмежень, технічних, економічних та правових аспектів.

СК4 — Здатність будувати та досліджувати моделі комп’ютерних систем та мереж.

СК5 — Здатність будувати архітектуру та створювати системне і прикладне програмне забезпечення комп’ютерних систем та мереж.

СК7 — Здатність досліджувати, розробляти та обирати технології створення великих і надвеликих систем.

СК8 — Здатність забезпечувати якість продуктів і сервісів інформаційних технологій на протязі їх життєвого циклу.

СК9 — Здатність представляти результати власних досліджень та/або розробок у вигляді презентацій, науково-технічних звітів, статей і доповідей на науково-технічних конференціях.

СК10 — Здатність ідентифікувати, класифікувати та описувати роботу програмно-технічних засобів, комп’ютерних систем, мереж та їхніх компонентів.

СК11 — Здатність обирати ефективні методи розв’язування складних задач комп’ютерної інженерії, критично оцінювати отримані результати та аргументувати прийняті рішення.

СК12 — Здатність досліджувати, розробляти і супроводжувати методи та засоби кібербезпеки для комп’ютерних систем та мереж у різних галузях, зокрема АПК.

Програмні результати навчання

ПРН1 — Застосовувати загальні підходи пізнання, методи математики, природничих та інженерних наук до розв’язання складних задач комп’ютерної інженерії.

ПРН2 — Знаходити необхідні дані, аналізувати та оцінювати їх.

ПРН3 — Будувати та досліджувати моделі комп’ютерних систем і мереж, оцінювати їх адекватність, визначати межі застосовності.

ПРН4 — Застосовувати спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері комп’ютерної інженерії, необхідні для професійної діяльності, оригінального мислення та проведення досліджень, критичного осмислення проблем інформаційних технологій та на межі галузей знань.

ПРН5 — Розробляти і реалізовувати проекти у сфері комп’ютерної інженерії та дотичні до неї міждисциплінарні проєкти з урахуванням інженерних, соціальних, економічних, правових та інших аспектів.

ПРН6 — Аналізувати проблематику, ідентифікувати та формулювати конкретні проблеми, що потребують вирішення, обирати ефективні методи їх вирішення.

ПРН7 — Вирішувати задачі аналізу та синтезу комп’ютерних систем та мереж.

ПРН9 — Розробляти програмне забезпечення для вбудованих і розподілених застосувань, мобільних і гібридних систем.

ПРН10 — Здійснювати пошук інформації в різних джерелах для розв’язання задач комп’ютерної інженерії, аналізувати та оцінювати цю інформацію.

ПРН11 — Приймати ефективні рішення з питань розроблення, впровадження та експлуатації комп’ютерних систем і мереж, аналізувати альтернативи, оцінювати ризики та імовірні наслідки рішень.

ПРН13 — Зрозуміло і недвозначно доносити власні знання, висновки та аргументацію з питань інформаційних технологій і дотичних міжгалузевих питань до фахівців і нефахівців, зокрема до осіб, які навчаються.

ПРН14 — Досліджувати, розробляти і супроводжувати системи та засоби кібербезпеки для комп’ютерних систем та мереж у різних галузях та об’єктах інформаційної діяльності, зокрема АПК.

Програма та структура навчальної дисципліни

Назви змістових модулів і тем	**Кількість годин (денна форма)**					**Кількість годин (заочна форма)**			
	тижні	**л**	**лаб**	**с.р.**	**усього**	**л**	**п**	**с.р.**	**усього**
Модуль 1. Створення СЗІ.									
Тема 1. Послідовність робіт зі створення СЗІ (КСЗІ).	-	1	2	20	23	-	-	-	-

Назви змістових модулів і тем	Кількість годин (денна форма)					Кількість годин (заочна форма)			
	тижні	л	лаб	с.р.	усього	л	п	с.р.	усього
Тема 2. Формування служби захисту інформації.	-	1	4	15	20	-	-	-	-
Тема 3. Обстеження умов функціонування ІТС та розробка технічного завдання на створення СЗІ (КСЗІ).	-	1	4	30	35	-	-	-	-
Тема 4. Розробка та реалізація проекту СЗІ (КСЗІ).	-	2	4	-	6	-	-	-	-
Тема 5. Введення СЗІ (КСЗІ) в дію.	-	2	-	-	2	-	-	-	-
Тема 6. Оцінка захищеності інформаційних ресурсів ІТС на підприємстві.	-	2	-	15	17	-	-	-	-
Разом за модулем 1	**-**	**9**	**14**	**80**	**103**	**-**	**-**	**-**	**-**
Модуль 2. Дослідна експлуатація СЗІ (КСЗІ).									
Тема 1. Попередні випробування СЗІ (КСЗІ).	-	2	12	20	34	-	-	-	-
Тема 2. Дослідна експлуатація СЗІ (КСЗІ).	-	4	4	35	43	-	-	-	-
Разом за модулем 2	**-**	**6**	**16**	**55**	**77**	**-**	**-**	**-**	**-**
Курсовий проект (робота) з _____ (якщо є в навчальному плані)									
Усього годин	**-**	**15**	**30**	**135**	**180**	**-**	**-**	**-**	**-**

Теми лекцій

№ з/п	Назва теми	Кількість годин
1	Тема 1. Послідовність робіт зі створення СЗІ (КСЗІ).	1
2	Тема 2. Формування служби захисту інформації.	1
3	Тема 3. Обстеження умов функціонування ІТС та розробка технічного завдання на створення СЗІ (КСЗІ).	1
4	Тема 4. Розробка та реалізація проекту СЗІ (КСЗІ).	2
5	Тема 5. Введення СЗІ (КСЗІ) в дію.	2

№ з/п	Назва теми	Кількість годин
6	Тема 6. Оцінка захищеності інформаційних ресурсів ІТС на підприємстві.	2
7	Тема 7. Попередні випробування СЗІ (КСЗІ).	2
8	Тема 8. Дослідна експлуатація СЗІ (КСЗІ).	4
Всього годин		**15**

Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Послідовність робіт зі створення СЗІ (КСЗІ).	2
2	Формування служби захисту інформації на підприємствах АПК.	4
3	Обстеження умов функціонування ІТС та розробка технічного завдання на створення СЗІ (КСЗІ) на підприємствах АПК.	4
4	Розробка та реалізація проекту СЗІ (КСЗІ) на підприємствах АПК.	4
5	Введення СЗІ (КСЗІ) в дію та оцінка захищеності інформаційних ресурсів ІТС.	4
6	Оцінка захищеності інформаційних ресурсів ІТС на підприємстві.	4
7	Попередні випробування СЗІ (КСЗІ).	4
8	Дослідна експлуатація СЗІ (КСЗІ).	4
Всього годин		**30**

Теми самостійної роботи

№ з/п	Назва теми	Кількість годин
1	Технічні канали витоку інформації та механізм їх утворення.	20
2	Розробка та реалізація проекту СЗІ (КСЗІ) на підприємствах АПК.	15

№ з/п	Назва теми	Кількість годин
3	Введення СЗІ (КСЗІ) в дію та оцінка захищеності інформаційних ресурсів ІТС.	15
4	Оцінка захищеності інформаційних ресурсів ІТС на підприємстві.	15
5	Попередні випробування СЗІ (КСЗІ).	15
6	Дослідна експлуатація СЗІ (КСЗІ). Комплексне управління довгостроковими інвестиціями у політику ІБ ОБІ.	15
7	Засоби управління локальними ресурсами ЗІКС та КМ.	20
8	Система управління ризиками ІБ.	20
Всього годин		**135**

Методи навчання

Методи та засоби діагностики результатів навчання:

— Усне опитування для перевірки розуміння основних понять і термінів курсу

— Тестування для оцінювання знань про криптографічні алгоритми та технічні засоби захисту

— Поточне оцінювання у вигляді виконання практичних завдань та вправ

— Модульний контроль для перевірки засвоєння ключових модулів курсу

— Підсумковий екзамен для комплексної оцінки знань та навичок

Методи навчання:

— Лекційний метод із використанням мультимедійних презентацій для викладення теоретичних аспектів захисту інформації

— Практичні заняття з використанням спеціалізованого програмного забезпечення для створення та тестування систем захисту

— Кейс-стаді для аналізу реальних інцидентів та розробки заходів реагування

— Метод проектів для розробки прототипів систем захисту інформації

— Обговорення та аналіз сучасних загроз і засобів їх нейтралізації у формі семінарських занять

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

Тема	Результати навчання	Оціночні бали
Модуль 1. Створення СЗІ.		
Лабораторна робота. Послідовність робіт зі створення СЗІ (КСЗІ)	ПРН 1, ПРН 4, ПРН 6, ПРН 14. Модуль спрямований на формування знань та навичок у створенні систем захисту інформації (СЗІ), зокрема у розробці та реалізації технічних та організаційних заходів безпеки. Студенти здобудуть уміння аналізувати технічні умови функціонування інформаційних систем, формулювати технічне завдання, застосовувати сучасні методи та інструменти для створення та впровадження систем захисту інформації на підприємствах АПК.	10
Лабораторна робота. Формування служби захисту інформації на підприємствах АПК		10
Лабораторна робота. Обстеження умов функціонування ІТС та розробка технічного завдання на створення СЗІ (КСЗІ) на підприємствах АПК		15
Лабораторна робота. Розробка та реалізація проекту СЗІ (КСЗІ) на підприємствах АПК		15
Самостійна робота. Технічні канали витоку інформації та механізм їх утворення		10

Тема	Результати навчання	Оціночні бали
Самостійна робота. Розробка та реалізація проекту СЗІ (КСЗІ) на підприємствах АПК		10
Самостійна робота. Введення СЗІ (КСЗІ) в дію та оцінка захищеності інформаційних ресурсів ІТС		10
Самостійна робота. Оцінка захищеності інформаційних ресурсів ІТС на підприємстві		10
Самостійна робота. Попередні випробування СЗІ (КСЗІ)		10
Всього за модулем 1		**100**
Модуль 2. Дослідна експлуатація СЗІ (КСЗІ).		
Лабораторна робота. Введення СЗІ (КСЗІ) в дію та оцінка захищеності інформаційних ресурсів ІТС	ПРН 1, ПРН 4, ПРН 6, ПРН 14. Модуль орієнтований на здобуття навичок експлуатації та управління системами захисту інформації у реальних умовах. Студенти навчаться оцінювати захищеність інформаційних ресурсів, проводити випробування та аналіз ризиків, застосовувати сучасні засоби управління та моніторингу безпеки інформаційних систем.	10
Лабораторна робота. Оцінка захищеності інформаційних ресурсів ІТС на підприємстві		15
Лабораторна робота. Попередні випробування СЗІ (КСЗІ)		15
Лабораторна робота. Дослідна експлуатація СЗІ (КСЗІ)		15

Тема	Результати навчання	Оціночні бали
Самостійна робота. Дослідна експлуатація СЗІ (КСЗІ). Комплексне управління довгостроковими інвестиціями у політику ІБ ОБІ		15
Самостійна робота. Засоби управління локальними ресурсами ЗІКС та КМ		15
Самостійна робота. Система управління ризиками ІБ		15
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=5060);

Рекомендовані джерела інформації

1. 1. Методи та засоби захисту інформації [Навчальний посібник] / В.А. Лахно, Є.В. Васіліу, В.М. Гладких, В.М. Домрачев, Н.М. Сивкова. – К. : ЦП «Компринт» О.В., 2020. – 444 с.
2. 2. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії / О.О. Кузнецов, С.П. Євсеєв, О.Г. Король. – Х.: Вид. ХНЕУ, 2010. – 316 с.
3. 3. Браіловський М.М. Захист інформації у банківській діяльності / М.М. Браіловський, Г.П. Лазарєв, В.О. Хорошко. – К.: ТОВ “ПоліграфКонсалтинг”, 2010. – 216 с.
4. 4. Проєктування комплексних систем захисту інформації. Підручник / В. О. Хорошко, І. М. Павлов, Ю. Я. Бобало, В. Б. Дудикевич, І. Р. Опірський, Л. Т. Пархуць. Львів : Видавництво Львівської політехніки, 2020. 320 с.
5. 5. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с. (Укр. мов.).
6. 6. Сагун А.В., Лахно В.А., Бобков В.Б., Касаткін Д.Ю., Хайдуров В.В. навчальний посібник «Спеціалізовані комп'ютери» / А.В. Сагун, В.А. Лахно, В.Б. Бобков, Д.Ю. Касаткін, В.В. Хайдуров // НУБіП України, - Київ, Видавничий центр Компринт 2021, 24 у.д.а.
7. 7. Кузнецов О.О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х.: Вид. ХНЕУ, 2011. – 510 с.