МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Волинський національний університет імені Лесі Українки
Факультет інформаційних технологій і математики
Кафедра комп'ютерних наук та кібербезпеки

СИЛАБУС
вибіркового освітнього компонента
Штучний інтелект в задачах кібербезпеки

галузь знань F Інформаційні технології
підготовка другого (магістерського) рівня вищої освіти
спеціальності F3 Комп'ютерні науки
освітньо-професійна програма Комп'ютерні науки та інформаційні технології

Луцьк - 2025

Силабус вибіркової освітнього компонента «Штучний інтелект в задачах кібербезпеки**»** для другого (магістерського) рівня вищої освіти галузі знань F Інформаційні технології, спеціальності F 3 Комп’ютерні науки за освітньо-професійною програмою Комп'ютерні науки та інформаційні технології.

Розробник: доцент, кандидат технічних наук Онищук Оксана Олександрівна

Погоджено

Гарант освітньо-професійної програми: Булатецький В.В., доцент, кандидат фізико-математичних наук

 Булатецький В.В.

Силабус освітнього компонента затверджено на засіданні кафедри комп’ютерних наук та кібербезпеки

протокол № 2 від 17 вересня 2025 р.

Завідувач  кафедри: Гришанович Т. О.

І. Опис навчальної дисципліни

<table>
<tr><td>Найменування показників</td><td>Галузь знань, напрям підготовки, освітній ступінь</td><td>Характеристика навчальної дисципліни</td></tr>
<tr><td>Денна (очна) форма навчання</td><td></td><td><u>за вибором</u>
(нормативна, за вибором)</td></tr>
<tr><td>Модулів – 2</td><td rowspan="3">Галузі знань F Інформаційні технології, спеціальність F3 Комп’ютерні науки Освітньо-професійна програма Комп'ютерні науки та інформаційні технології</td><td>Рік підготовки: 5ий</td></tr>
<tr><td>Змістових модулів – 4</td><td rowspan="2">Семестр: 2 ий</td></tr>
<tr><td>Загальна кількість годин/кредити - 120/ 4</td></tr>
<tr><td rowspan="5">ІНДЗ: <u>є</u></td><td rowspan="5">Другий (магістерський)</td><td>Лекції:10 год</td></tr>
<tr><td>Практичні:14 год.</td></tr>
<tr><td>Самостійна робота: 88 год</td></tr>
<tr><td>Консультації: 8 год</td></tr>
<tr><td>Вид контролю: залік</td></tr>
<tr><td colspan="3">Мова навчання – <u>українська</u></td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної та індивідуальної роботи становить: для денної форми навчання – 53 % аудиторних занять, 47 % самостійної та індивідуальної роботи.

ІІ. Інформація про викладача

ПІП – Онищук Оксана Олександрівна
Науковий ступінь – кандидат технічних наук
Вчене звання – доцент
Посада – доцент комп'ютерних наук та кібербезпеки
Контактна інформація: +38-0966943585, Onyshchuk.oksana@vnu.edu.ua

ІІІ. Опис освітнього компонента

1. **Метою освітньогог компонента** є набуття здобувачами знань, умінь і здатностей (компетенцій) щодо розробки та застосування методів штучного інтелекту в задачах кібербезпеки для ефективного вирішення завдань професійної діяльності.
2. **Завданнями вивчення навчальної дисципліни** є:

– отримання здобувачами фундаментальних систематизованих знань про підходи, моделі і методи, розроблені в рамках наукового напрямку «штучний інтелект» за весь період його існування;

– освоєння здобувачами основних методів штучного інтелекту, що застосовуються в системах кібербезпеки;

– ознайомлення здобувачів з новими методами і підходами до вирішення традиційних завдань, що розробляються в рамках напрямку "штучний інтелект" та застосовуються для

рішення завдань кібербезпеки;

– формування у здобувачів аналітичних здібностей, які б дозволяли їм робити обґрунтований вибір вивчених моделей і методів при вирішенні завдань з проблемної області, в якій вони спеціалізуються (кібербезпека, інформаційні технології та комп'ютерні науки).

3.Результати навчання (компетентності)

Компетентності:

ЗК01. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК02. Здатність застосовувати знання у практичних ситуаціях. З

ЗК03. Здатність спілкуватися державною мовою як усно, так і письмово.

ЗК04. Здатність спілкуватися іноземною мовою.

ЗК05. Здатність вчитися й оволодівати сучасними знаннями.

ЗК06. Здатність бути критичним і самокритичним.

Спеціальні (фахові) компетентності:

СК02. Здатність формалізувати предметну область певного проєкту у вигляді відповідної інформаційної моделі.

СК03. Здатність використовувати математичні методи для аналізу формалізованих моделей предметної області.

СК04. Здатність збирати і аналізувати дані (включно з великими), для забезпечення якості прийняття проєктних рішень.

СК05. Здатність розробляти, описувати, аналізувати та оптимізувати архітектурні рішення інформаційних та комп’ютерних систем різного призначення.

СК06. Здатність застосовувати існуючі і розробляти нові алгоритми розв’язування задач у галузі комп’ютерних наук.

Отримані знання з навчальної дисципліни стануть складовими наступних **результатів** навчання.

Результати навчання:

РН2. Мати спеціалізовані уміння/навички розв’язання проблем комп’ютерних наук, необхідні для проведення досліджень та/або провадження інноваційної діяльності з метою розвитку нових знань та процедур.

РН3. Зрозуміло і недвозначно доносити власні знання, висновки та аргументацію у сфері комп’ютерних наук до фахівців і нефахівців, зокрема до осіб, які навчаються.

РН4. Управляти робочими процесами у сфері інформаційних технологій, які є складними, непередбачуваними та потребують нових стратегічних підходів.

РН5. Оцінювати результати діяльності команд та колективів у сфері інформаційних технологій, забезпечувати ефективність їх діяльності.

РН6. Розробляти концептуальну модель інформаційної або комп’ютерної системи. РН7. Розробляти та застосовувати математичні методи для аналізу інформаційних моделей.

РН8. Розробляти математичні моделі та методи аналізу даних (включно з великим).

РН11. Створювати нові алгоритми розв’язування задач у сфері кокомп’ютерних наук, оцінювати їх ефективність та обмеження на їх застосування.

4. Програма навчальної дисципліни

Змістовий модуль 1.

Концептуальні положення систем штучного інтелекту в задачах кібербезпеки, нечіткі множини та штучні нейронні мережі

Тема 1. Напрямки застосування штучного інтелекту в кібербезпеці. Історія розвитку штучного інтелекту. Напрямки досліджень в галузі штучного інтелекту. Напрямки застосування штучного інтелекту в кібербезпеці. Недоліки і проблеми сучасного штучного інтелекту.

Тема 2. Нечіткі множини та логіко-лінгвістичне моделювання в задачах кібербезпеки. Теорія нечітких множин. Методи побудови функцій приналежності нечітких множин. Нечіткі оператори. Логіка роботи нечіткої системи. Практичне застосування нечіткої логіки в задачах кібербезпеки.

Тема 3. Нейронні мережі та їх застосування в задачах кібербезпеки. Аналогія з мозком людини. Штучний нейрон. Архітектура з'єднань штучних нейронів. Навчання штучної нейронної мережі. Основні етапи розв'язання задач за допомогою нейромереж. Перцептрон Розенблата. Нейромережа зворотного поширення похибки (Backpropagation). Мережа Delta Bar Delta. Мережа Extended Delta Bar Delta. Мережа спрямованого випадкового пошуку. Нейронна мережа вищого порядку або функціонально - пов'язана нейронна мережа. Мережа Кохонена. Мережа квантування навчального вектора (Learning Vector Quantization). Мережа зустрічного поширення (CounterPropagation). Ймовірнісна нейронна мережа. Мережа Хопфілда. Мережа «Машина Больцмана». Мережа Хемінга. Мережа мережної моделі з двонаправленою асоціативною пам’яттю. Мережа адаптивної резонансної теорії (ART).

Змістовий модуль 2.

Еволюційні методи та методи засновані на знаннях в задачах кібербезпеки

Тема 4. Еволюційне моделювання та генетичні алгоритми в задачах кібербезпеки.

Природний відбір у природі. Основні поняття генетичних алгоритмів. Особливості генетичних алгоритмів. Задачі оптимізації і застосування алгоритмів. Опис типового генетичного алгоритму. Класичний генетичний алгоритм. Представлення даних у генах. Приклади кодування параметрів задачі в генетичному алгоритмі. Основна теорема про генетичні алгоритми. Будівельні блоки (Building blocks). Еволюційні алгоритми. Еволюційні алгоритми в нейронних мережах.

Тема 5. Представлення знань і вивід на знаннях в задачах кібербезпеки. Поняття даних та знань. Класифікація знань. Моделі представлення знань. Виведення на знаннях.

Змістовий модуль 3.

Інтелектуальні агенти та машинне навчання в задачах кібербезпеки

Тема 6. Теоретичні основи інтелектуальних програмних агентів. Основні властивості програмних агентів. Архітектури агентів. Мультиагентні системи.

Тема 7. Машинне навчання в системах кібербезпеки. Складові машинного навчання та штучний інтелект. Класифікація методів машинного навчання. Класичне навчання. Навчання з підкріпленням. Ансамблі. Штучні нейронні мережі.

Змістовий модуль 4.

Технології комп’ютерного зору в задачах кібербезпеки

Тема 8. Комп’ютерний зір та попередня обробка зображень. Сучасний погляд на комп’ютерний зір. Типові задачі комп'ютерного зору. Системи комп'ютерного зору. Цифрове подання зображень. Характеристики якості зображення. Радіометрична корекція цифрових зображень. Цифрові фільтри.

Тема 9. Розпізнавання образів в задачах кібербезпеки.Постановка завдання. Сегментація зображень - загальний підхід. Сегментація, що заснована на методах класифікації. Контрольована класифікація. Основи загальної теорії розпізнавання образів. Підходи до розпізнавання зображень. Локалізація об'єктів на зображеннях. Ознаки об'єктів на зображенні.

5. Структура (тематичний план) навчальної дисципліни

	Змістовні модулі	Кількість годин

		Всього	Лек	Лаб	Консультації	Сам
1	2	3	4	5		6
№ 1	Змістовий модуль 1. Концептуальні положення систем штучного інтелекту в задачах кібербезпеки, нечіткі множини та штучні нейронні мережі					
	Тема 1. Напрямки застосування штучного інтелекту в кібербезпеці.	11	1	1	1	8
	Тема 2. Нечіткі множини та логіко-лінгвістичне моделювання в задачах кібербезпеки	10	1	1	1	7
	Тема 3. Нейронні мережі та їх застосування в задачах кібербезпеки.	9	1	1		7
	Разом змістовий модуль 1	30	3	3	2	22
№ 2	Змістовий модуль 2. Еволюційні методи та методи засновані на знаннях в задачах кібербезпеки					
	Тема 4. Еволюційне моделювання та генетичні алгоритми в інтелектуальних системах.	15	1	2	1	11
	Тема 5. Представлення знань і вивід на знаннях в задачах кібербезпеки	15	1	2	1	11
	Разом змістовий модуль 2	30	2	4	2	22
№ 3	Змістовий модуль 3. Інтелектуальні агенти та машинне навчання в задачах кібербезпеки					
	Тема 6. Теоретичні основи інтелектуальних програмних агентів.	16	2	2	1	11
	Тема 7. Машинне навчання в системах кібербезпеки	15	1	2	1	11
	Разом змістовий модуль 3	30	3	4	2	22
№ 4	Змістовий модуль 4. Технології комп'ютерного зору в задачах кібербезпеки					
	Тема 8. Комп'ютерний зір та попередня обробка зображень	15	1	2	1	11
	Тема 9. Розпізнавання образів в задачах кібербезпеки	15	1	1	1	11
	Разом змістовий модуль4	30	2	3	2	22
	РАЗОМ 195	120	10	14	8	88

6.Теми лабораторних робіт

№ з/п	Назва теми	Кількість годин
1	Моделювання елементів теорії нечітких множин та формування нечітких правил в задачах кібербезпеки	2
2	Моделювання простих нейронних мереж	2
3	Дослідження складних нейронних мереж	2
4	Дослідження радіальних та рекурентних нейронних мереж	2
5	Дослідження методів оптимізації за допомогою генетичних алгоритмів в задачах кібербезпеки	2
6	Дослідження методів машинного навчання в задачах кібербезпеки	2
7	Попередня обробка зображень та простий аналіз	1
8	Дослідження методів виявлення та кластеризації зображень в задачах кібербезпеки	1
РАЗОМ		14

7. Завдання для самостійної роботи

Самостійна робота студентів виконується за завданням і при методичному керівництві викладача але без його безпосередньої участі. Самостійна робота підрозділяється на самостійну роботу на аудиторних заняттях і на позааудиторну самостійну роботу. Самостійна робота студентів включає як повністю самостійне освоєння окремих тем (розділів) дисципліни, так і опрацювання (розділів), освоюваних під час аудиторної роботи. Під час самостійної роботи навчаються читаючи та конспектуючи навчальну, наукову та довідкову літературу, виконують завдання, спрямовані на закріплення знань і відпрацювання умінь і навичок, готуються до поточного і проміжного контролю з дисципліни.

Організація самостійної роботи студентів регламентується нормативними документами, навчально-методичною літературою та електронними освітніми ресурсами.

Змістовий модуль 1. Концептуальні положення систем штучного інтелекту в задачах кібербезпеки, нечіткі множини та штучні нейронні мережі

Самостійна робота за темою 1. Напрямки застосування штучного інтелекту в кібербезпеці. Історія розвитку штучного інтелекту. Напрямки застосування штучного інтелекту в кібербезпеці. Недоліки і проблеми сучасного штучного інтелекту. Рекомендована література: 2–3, 9

Література: Основна: 1-5. Допоміжна: 3-9

Самостійна робота за темою 2. Нечіткі множини та логіко-лінгвістичне моделювання в задачах кібербезпеки. Практичне застосування нечіткої логіки в задачах кібербезпеки. *Література: Основна: 1-15. Допоміжна: 1-17*

Самостійна робота за темою 3. Нейронні мережі та їх застосування в задачах кібербезпеки.

Основні етапи розв'язання задач за допомогою нейромереж. Мережа квантування вчального вектора (Learning Vector Quantization). Мережа «Машина Больцмана». Мережа Хемінга. Мережа мережної моделі з двонаправленою асоціативною пам’яттю. Мережа адаптивної резонансної теорії (ART).

Література: Основна: 1-8 Допоміжна: 3-5

Змістовий модуль 2. Еволюційні методи та методи засновані на знаннях в задачах кібербезпеки

Самостійна робота за темою 4. Еволюційне моделювання та генетичні алгоритми в задачах кібербезпеки. Еволюційні алгоритми. Еволюційні алгоритми в нейронних мережах.

Література: Основна: 1-15 Допоміжна: 1-17

Самостійна робота за темою 5. Представлення знань і вивід на знаннях в задачах кібербезпеки.

Моделі представлення знань. Виведення на знаннях.

Змістовий модуль 3. Інтелектуальні агенти та машинне навчання в задачах кібербезпеки

Самостійна робота за темою 6. Теоретичні основи інтелектуальних програмних агентів. Архітектури агентів. Мультиагентні системи.

Самостійна робота за темою 7. Машинне навчання в системах кібербезпеки. Класичне навчання. Навчання з підкріпленням. Ансамблі. Штучні нейронні мережі.

Література: Основна: 1-15. Допоміжна: 1-17

Змістовий модуль 4. Технології комп'ютерного зору в задачах кібербезпеки

Самостійна робота за темою 8. Комп'ютерний зір та попередня обробка зображень.Варіанти радіометричної корекції цифрових зображень. Цифрові фільтри.

Література: Основна: 1-15. Допоміжна: 1-17

Самостійна робота за темою 9. Розпізнавання образів в задачах кібербезпекиСегментація, що заснована на методах класифікації. Контрольована класифікація. Підходи до розпізнавання зображень. Локалізація об'єктів на зображеннях.

Література: Основна: 1-15. Допоміжна: 1-17

Застосовуються словесні наочні і практичні методи навчання. Словесні методи: пояснення, лекція, навчальна дискусія. Наочні методи: демонстрація та ілюстрація. Практичні методи навчання: лабораторні заняття. Лекції з використанням електронних дидактичних демонстраційних матеріалів (презентації), що призначені для супроводу навчального процесу. Самостійна робота з використанням можливості локальної мережі та Інтернет з наданням відповідних посилань на джерело інформації. Самостійна підготовка з використанням друкованих та електронних підручників, навчальних посібників (з вільним доступом усім учасникам навчального процесу), а також інших локальних і мережевих інформаційних ресурсів.

IV. Політика оцінювання

Політика викладача щодо здобувача освіти. Здобувачі освіти повинні відвідувати лабораторні заняття та вчасно складати відповідні завдання до роботи на комп'ютерах. Оцінювання робіт здійснюється з урахуванням вірно виконаного обсягу у пропорції до визначеного цим силабусом балу із заокругленням до більшого.

Політика щодо академічної доброчесності. Здобувачам вищої освіти дозволяється вивчати довільні джерела інформації, що стосуються тематики завдань, а також консультуватися та працювати у групах зі своїми колегами за курсом. Проте завдання повинні бути виконані самостійно. В іншому разі відповідні бали здобувачу вищої освіти не зараховуються.

Політика щодо дедлайнів та перескладання. Завдання мають бути виконані у межах відведеного на це часу. Невчасно здане без поважної причини завдання зменшує відповідний бал оцінювання на 10 % для забезпечення справедливого рейтингового оцінювання здобувачів вищої освіти, особливо тих, хто вчасно виконує відповідні завдання.

Оцінювання знань здобувачів освіти здійснюється під час поточного контролю за результатами виконання тих видів робіт, які передбачені силабусом освітнього компонента. (згідно Положення про поточне та підсумкове оцінювання знань здобувачів освіти Волинського національного університету імені Лесі Українки).

Оцінювання навчальних досягнень здійснюється за 100 бальною шкалою. Оцінка включає в себе поточний контроль (оцінюється робота на парах, вчасне і якісне виконання домашніх завдань, самостійне розв'язання індивідуальних завдань) та підсумковий модульний контроль (письмові модульні контрольні роботи). Максимальна кількість балів, яку може заробити студент під час поточного оцінювання за семестр – 70 балів. Підсумковий модульний контроль за семестр включає в себе оцінки за всі модульні контрольні роботи (МКР). Максимальна кількість балів, яку може заробити студент під час модульного контролю за семестр складає 30 балів.

Якщо за результатами семестру накопичено не менше 75 балів і студент погоджується із цим результатом, то оцінка за семестр може виставлятися без складання заліку. В іншому разі студент складає залік; максимальна кількість балів, яку можна отримати на заліку – 60 балів. Вони замінюють бали модульного семестрового контролю, поточний семестровий

контроль при цьому зберігається. Залік проходять в усній формі. Оцінка за семестр у випадку складання екзамену є сумою балів поточного контролю та балів, отриманих під час екзамену.

V. Підсумковий контроль

На залік виносяться основні питання, типові та комплексні задачі, ситуації, завдання, що потребують творчої відповіді та вміння синтезувати отримані знання і застосовувати їх під час розв'язання практичних задач.Іспит проводиться в усній формі. Залік проходить у письмовій формі.

Шкала оцінювання знань здобувачів освіти з освітніх компонентів, де формою контролю є залік	Оцінка в балах	Лінгвістична оцінка
	90–100	Зараховано
	82–89	
	75–81	
	67–74	
	60–66	
	1–59	Незараховано (необхідне перескладання)

VI. Рекомендована література та інтернет-ресурси

Основна література

1. Melanie Mitchell. Artificial Intelligence. A Guide for Thinking Humans, London. Penguin 2020. — 448 p. — ISBN 978-0-241-40483-6 . (укр.)
2. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.
3. ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.
4. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.
5. ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення.
6. AI. https://uk.wikipedia.org/wiki/%D0%A8%D1%82%D1%83%D1%87%D0%BD%D0%B8%D0%B9_%D1%96%D0%BD%D1%82%D0%B5%D0%BB%D0%B5%D0% BA%D1%82
7. Розпорядження Кабінету міністрів України від 2 грудня 2020 р. № 1556-р. Київ «Про схвалення Концепції розвитку штучного інтелекту в Україні» https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text
8. Асоціація штучного інтелекту - http://www.raai.org
9. Stamp, M., & Jureček, M. (Eds.). (2025). *Machine Learning, Deep Learning and AI for Cybersecurity*. Springer. https://link.springer.com/book/9783031831560
10. Abou El Houda, Z., & Zouheir, A. (2025). Deep learning for intrusion detection in emerging technologies: A comprehensive survey and new perspectives. *Artificial Intelligence Review*. https://doi.org/10.1007/s10462-025-11346-z
11. Singh, R., Alqahtani, M., & Ferrag, M. A. (2024). Advancing cybersecurity: A comprehensive review of AI-driven detection techniques. *Journal of Big Data, 11*(67). https://doi.org/10.1186/s40537-024-00957-y
12. Sarker, I. H., Kayes, A. S. M., & Watters, P. (2021). Artificial intelligence in cyber security: Research advances, challenges, and opportunities. *Artificial Intelligence Review, 54*(6), 4273–4310. https://doi.org/10.1007/s10462-021-09976-0
13. Ferrag, M. A., Alwahedi, F., Battah, A., & Maglaras, L. (2024). Generative AI in cybersecurity: A comprehensive review of LLM applications and vulnerabilities. *arXiv preprint arXiv:2405.12750*. https://arxiv.org/abs/2405.12750
14. AlSharman, S. A., Al-Khaleel, O., & Al-Ayyoub, M. (2024). A detailed inspection of machine learning-based intrusion detection systems for software defined networks. *Computers, 5*(4), 34. https://www.mdpi.com/2624-831X/5/4/34.