**Силабус освітнього компонента**
Програма навчальної дисципліни

# Основи машинного навчання для кібербезпеки

**Шифр та назва спеціальності**
F5 – Кібербезпека та захист інформації

**Інститут**
ННІ комп`ютерних наук та інформаційних технологій

**Спеціалізація**

**Кафедра**
Кібербезпеки (328)

**Освітня програма**
Кібербезпека

**Тип дисципліни**
Обов'язкова

**Рівень освіти**
Перший (бакалаврський)

**Форма навчання**
Денна, заочна

**Семестр**
8

**Мова викладання**
Українська, англійська

## Викладачі, розробники

**МІЛЕВСЬКИЙ Станіслав Валерійович**

stanislav.milevskyi@khpi.edu.ua
Доктор технічних наук, доцент, професор кафедри кібербезпеки НТУ «ХПІ».

Автор понад 100 наукових та навчально-методичних праць. Гарант освітньо-наукової програми «Кібербезпека» другого (магістерського) рівня вищої освіти. Провідний лектор з дисциплін: «Основи математичного моделювання систем безпеки», «Основи машинного навчання для кібербезпеки», «Англійська мова в академічних застосунках», «Моделювання кіберфізичних дій», «Математичні моделі управління ІТ-проєктами» у студентів бакалавріата та магістратури, «Моделювання механізмів кібербезпеки», «Математичні методи, моделі та інформаційні технології у наукових дослідженнях» у аспірантів .

Детальніше про викладача на сайті кафедри

## Загальна інформація

### Анотація

Навчальна програма дисципліни “Основи машинного навчання для кібербезпеки” визначає зміст і обсяг знань, необхідних для фахівця з кібербезпеки. Дисципліна обіймає проблематику вивчення сучасного стану технологій машинного навчання, що використовуються для формалізації та обробки даних в технологіях функціонування систем безпеки, вивчення сучасних програмних

засобів машинної обробки даних, технологій їх проектування, реалізації, налагодження і дослідження. Машинне навчання застосовують в ряді обчислювальних задач, в яких розробка та програмування явних алгоритмів з доброю продуктивністю є складною або нездійсненною задачею. Для практичного засвоєння навчальних матеріалів ряд тем дисципліни поглиблено вивчається на лабораторних заняттях.

## Мета та цілі дисципліни

Метою вивчення дисципліни є формування у майбутніх фахівців знань та вмінь застосування сучасних методів та засобів розробки, дослідження та використання сучасних технологій обробки даних для вирішення задач класифікації, регресійного аналізу, прогнозування та прийняття рішень.

## Формат занять

Лекції, лабораторні заняття, самостійна робота, консультації. Підсумковий контроль – диференційований залік.

## Компетентності

ЗК1. Здатність застосовувати знання у практичних ситуаціях.
ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності.
ЗК5. Здатність вчитися і оволодівати сучасними знаннями.
ЗК8. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
СК2. Здатність використовувати інформаційні технологій, сучасні методи і моделей кібербезпеки та систем захисту інформації.
СК4. Здатність забезпечувати захист інформації в інформаційних системах згідно встановленої політики кібербезпеки та захисту інформації.
СК5. Здатність відновлювати функціонування інформаційних систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.
СК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо).
СК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.
СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

## Результати навчання

РН4. 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.
РН5. 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.
РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.
РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення та передачі сигналів тощо, принципи, методи і поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.

РН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.
РН10. Вміти використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.
РН12. Застосовувати методи захисту інформації в інформаційних системах згідно встановленої політики інформаційної безпеки.
РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних та програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних систем та\або інфраструктури організації в цілому.
РН14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних систем з використанням процедур резервування згідно встановленої політики безпеки та забезпечувати функціонування спеціального програмного забезпечення, щодо захисту та відновлення інформації.
РН15. Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.
РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.
РН17. Забезпечувати функціонування системи управління кібербезпекою та захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.
РН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору та інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

### Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 24 год., лабораторні роботи – 24 год., самостійна робота – 72 год.

### Передумови вивчення дисципліни (пререквізити)

Вища математика.

### Особливості дисципліни, методи та технології навчання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, індивідуальні групові проєкти, майстер-класи.

## Програма навчальної дисципліни

### Навчальні заняття

#### Лекції

| Теми лекцій | Кількість годин |
|---|---|
| **Тема 1. Вступ до машиного навчання.**<br>Що таке машинне навчання. Типи навчання. Як працює навчання із учителем. Чому модель здатна працювати з новими даними? | 3 |
| **Тема 2. Позначення та визначення.**<br>Позначення. Випадкова величина. Незміщені оцінки. Правило Байєса. Оцінка параметрів. Параметри та гіперпараметри. Класифікація та регресія. Навчання | 3 |

| | |
|---|---|
| на основі моделей та на основі прикладів. Поверхневе та глибоке навчання. | |
| **Тема 3. Фундаментальні алгоритми.**<br>Лінійна регресія. Логістична регресія. Навчання дерева рішень. Спосіб опорних векторів. Метод k найближчих сусідів. | 3 |
| **Тема 4. Анатомія алгоритмів навчання. Будівельні блоки алгоритмів навчання. Градієнтний спуск.**<br>Як працюють інженери, котрі займаються машинним навчанням. Особливості алгоритмів навчання. | 3 |
| **Тема 5. Практичні засади.**<br>Проектування ознак. Вибір алгоритму навчання. Три набори. Недонавчання та перенавчання. Регуляризація. Оцінка ефективності моделі. Налаштування гіперпараметрів. | 2 |
| **Тема 6. Нейронні мережі та глибоке навчання.**<br>Нейронні мережі. Глибоке навчання. | 2 |
| **Тема 7. Проблеми та рішення.**<br>Ядерна регресія. Багатокласова класифікація. Однокласова класифікація. Класифікація з багатьма мітками. Навчання ансамблю. Навчання маркування послідовностей. Навчання перетворення послідовностей у послідовності. Активне навчання. Навчання із частковим залученням вчителя. Навчання з першого разу. Навчання без підготовки. | 2 |
| **Тема 8. Просунуті методики.**<br>Робота з незбалансованими наборами даних. Об'єднання моделей. Навчання нейронних мереж. Просунута регуляризація. Обробка кількох входів. Обробка кількох виходів. Перенесення навчання. Ефективність алгоритмів. | 2 |
| **Тема 9. Навчання без учителя.**<br>Оцінка густини. Кластеризація. Скорочення розмірності. Виявлення аномалій. | 2 |
| **Тема 10. Інші форми навчання.**<br>Визначення метрик. Визначення рангу. Навчання робити рекомендації. Самонавчання з учителем: вкладення слів. | 2 |
| **Загальна кількість годин** | **24** |

## Лабораторні заняття

| Теми лабораторних занять | Кількість годин | Вагові коефіцієнти $a$ |
|---|---|---|
| **Тема 1. Передобробка даних.**<br>Виявлення та обробка пропусків у даних. Кодування категоріальних змінних (Label Encoding, One-Hot Encoding). Видалення та обробка викидів. Балансування даних (oversampling, undersampling). | 3 | 0,1 |
| **Тема 2. Важливість Ознак.**<br>Використання Random Forest для визначення важливості ознак. Перестановочна важливість (Permutation Importance). Аналіз впливу ознак на точність моделі. Використання SHAP та LIME для пояснення моделей. | 3 | 0,1 |
| **Тема 3. Нормалізація Ознак.**<br>Масштабування (MinMaxScaler, StandardScaler, RobustScaler). Вплив нормалізації на алгоритми класифікації. Нормалізація для | 3 | 0,1 |

| | | |
|---|---|---|
| алгоритмів на основі відстаней (k-NN, SVM). Практика використання в sklearn. | | |
| **Тема 4. Вибір числа сусідів, вибір метрики (k-NN).** Критерії вибору оптимального k. Використання різних метрик (Euclidean, Manhattan, Cosine). Перевірка якості моделі через крос-валідацію. Вплив параметрів на точність класифікації у задачах кібербезпеки. | 3 | 0,1 |
| **Тема 5. Опорні Об'єкти (SVM).** Основи роботи алгоритму SVM. Лінійне та нелінійне розділення даних. Використання ядерних функцій (Radial, Polynomial). Практика застосування SVM для виявлення аномалій у трафіку. | 2 | 0,1 |
| **Тема 6. Аналіз текстів.** Побудова словникової моделі (Bag of Words). Використання TF-IDF для аналізу текстів. Методи векторизації текстів (Word2Vec, GloVe). Виявлення фішингових повідомлень і спаму. | 2 | 0,1 |
| **Тема 7. Логістична регресія.** Основи ймовірнісної класифікації. Реалізація моделі у sklearn. ROC-крива та AUC-метрика. Використання логістичної регресії для задач виявлення вторгнень. | 2 | 0,1 |
| **Тема 8. Лінійна регресія.** Побудова моделі регресії та інтерпретація коефіцієнтів. Метод найменших квадратів. Виявлення мультиколінеарності ознак. Використання регресії для прогнозу кіберзагроз. | 2 | 0,1 |
| **Тема 9. Розмір випадкового лісу (Random Forest).** Вибір кількості дерев у моделі. Балансування між bias та variance. Визначення стабільності прогнозу. Практика використання Random Forest для класифікації мережевого трафіку. | 2 | 0,1 |
| **Тема 10. Метод найшвидшого бустінгу над вирішальними деревами (XGBoost / LightGBM / CatBoost).** Основи градієнтного бустінгу. Порівняння XGBoost, LightGBM, CatBoost. Налаштування гіперпараметрів (learning rate, depth, estimators). Практика застосування для виявлення шкідливих дій у системах. | 2 | 0,1 |
| **Загальна кількість годин** | **24** | $\sum_{i=1}^{n} a_i = 1$ |

## Контрольні роботи

| Теми контрольних робіт | Вагові коефіцієнти $b$ |
|---|---|
| **Тема 1. Методи передобробки та нормалізації даних у машинному навчанні для задач кібербезпеки.** Робота з пропущеними даними та викидами. Масштабування та нормалізація ознак. Вплив підготовки даних на якість класифікації. | 1,5 |
| **Тема 2. Застосування алгоритмів машинного навчання для виявлення кіберзагроз.** Логістична регресія, k-NN, SVM. Використання Random Forest і методів бустінгу. Приклади виявлення аномалій у мережевому трафіку. | 1,5 |

| | |
|---|---|
| **Загалом** | $\sum_{i=1}^{m} b_i=3$ |

### Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

#### Опрацювання теоретичного матеріалу

| Теми для самостійного вивчення | Кількість годин |
|---|---|
| **Тема 1. Основні етапи життєвого циклу машинного навчання у сфері кібербезпеки.** Збір та попередня обробка даних. Вибір моделі та алгоритму. Навчання та тестування. Валідація та оптимізація. Завдання: скласти схему життєвого циклу ML у кібербезпеці. | 11 |
| **Тема 2. Методи відбору ознак та їх вплив на точність класифікації атак.** Відбір ознак на основі статистичних методів. Використання важливості ознак у Random Forest. Методи PCA та LDA. Завдання: порівняти точність моделі з усіма ознаками та після відбору. | 11 |
| **Тема 3. Порівняння методів нормалізації та стандартизації даних.** MinMaxScaler, StandardScaler, RobustScaler. Вплив нормалізації на роботу k-NN та SVM. Практичні приклади на реальному датасеті. Завдання: провести експеримент із різними методами масштабування. | 10 |
| **Тема 4. Застосування алгоритму k-NN для виявлення вторгнень у мережі.** Вибір числа сусідів (k). Використання різних метрик (евклідова, косинусна, мангеттенська). Балансування даних при навчанні k-NN. Завдання: побудувати класифікатор для мережевого трафіку. | 10 |
| **Тема 5. SVM у задачах виявлення аномалій у кібербезпеці.** Лінійне та нелінійне розділення даних. Використання ядерних функцій. Приклади застосування для IDS (Intrusion Detection System). Завдання: реалізувати модель SVM та протестувати на датасеті KDD Cup. | 10 |
| **Тема 6. Методи обробки текстових даних для виявлення фішингу та спаму.** Bag of Words та TF-IDF. Word2Vec, FastText, GloVe. Використання ML для класифікації листів. Завдання: побудувати модель для виявлення фішингових email. | 10 |
| **Тема 7. Порівняльний аналіз ансамблевих методів: Random Forest, XGBoost, LightGBM.** Основи ансамблевого навчання (bagging, boosting). Сильні та слабкі сторони кожного алгоритму. Приклади застосування у кібербезпеці (виявлення DDoS, спаму). Завдання: провести експеримент на одному датасеті з трьома алгоритмами та порівняти результати. | 10 |
| **Загальна кількість годин** | **72** |

## Неформальна освіта

Здобувач має можливість перезарахувати окремі теми або курс шляхом: проходження професійних курсів чи тренінгів, онлайн-освіти, професійних стажувань, у сфері, що відповідає навчальним цілям дисципліни.

Для зарахування необхідно надати: сертифікат (електронний або друкований) про проходження курсу/стажування, опис програми тренінгу із зазначенням змісту тем, обсягу та тривалості..

### Рекомендовані курси, тренінги, стажування

1. Онлайн-курс CISCO «AI Fundamentals with IBM SkillsBuild, Learning Collection: AI with Intel» https://www.netacad.com/catalogs/learn?category=course

## Література, навчальні матеріали та інформаційні ресурси

### Основна література

1. Bishop, Christopher M. Pattern Recognition and Machine Learning. Springer; 1st ed. 2006. Corr.; 2nd printing ed. 2007.
http://users.isr.ist.utl.pt/~wurmd/Livros/school/Bishop%20-%20Pattern%20Recognition%20And%20Machine%20Learning%20-%20Springer%20%202006.pdf
2. Hastie, Trevor, Robert Tibshirani, and Jerome Friedman. The Elements of Statistical Learning. Springer, 2009.
https://www.sas.upenn.edu/~fdiebold/NoHesitations/BookAdvanced.pdf
3. Gelman, Andrew, and Jennifer Hill. Data Analysis Using Regression and Multilevel/ Hierarchical Models. Cambridge University Press, 2006.
https://moodle2.units.it/pluginfile.php/706395/mod_resource/content/1/gelman%20hill%202007.pdf
4. Jones, Owen, Robert Maillardet, and Andrew Robinson. Introduction to Scientific Programming and Simulation Using R. Chapman and Hall, 2009.
https://nyu-cdsc.github.io/learningr/assets/simulation.pdf
5. Segaran, Toby. Programming Collective Intelligence: Building Smart Web 2.0 Applications. O'Reilly Media, 2007.
https://axon.cs.byu.edu/~martinez/classes/778/Papers/GP.pdf

### Додаткова література

6. A. Rukhin, and J. Soto. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22, 09.2000, 164 p.
https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-22r1a.pdf

## Система оцінювання

Підсумкова оцінка з освітнього компонента визначається відповідальним лектором за темами, видами занять, тощо у відповідності до силабусу і є інтегральною оцінкою результатів усіх вид навчальної діяльності здобувача вищої освіти. Підсумкова оцінка повинна відображати всі оцінки за складовими навчального процесу з урахуванням їх вагових показників $k$:

| Поточний контроль (практичні, семінарські, лабораторні заняття), $k_1$ | Контрольні роботи (за наявності), $k_2$ | Індивідуальне завдання (за наявності), $k_3$ | Підсумковий контроль (для ОК з іспитом), $k_4$ |
|---|---|---|---|
| 0,7 | 0,3 | | |

Сума коефіцієнтів повинна складати одиницю: $k_1 + k_2 + k_3 + k_4 = 1$. Підбір вагових коефіцієнтів підсумкової оцінки здійснює розробник курсу.
Розрахунок підсумкової оцінки проводиться за формулою:

$$О = П \cdot k_1 + К \cdot k_2 + І \cdot k_3 + Пк \cdot k_4$$

де: П – середньозважена середня оцінка за поточний контроль
І – оцінка за виконання індивідуального завдання

$K$ – середньозважена оцінка за контрольні роботи
Пк – оцінка за підсумковий контроль

$$П = \frac{П_1 \cdot a_1 + П_2 \cdot a_2 + ... + П_n \cdot a_n}{\sum_{i=1}^{n} a_i}$$

де: $a_i$ - ваговий коефіцієнт за кожне практичне (семінарське) або лабораторне заняття.

$$K = \frac{K_1 \cdot b_1 + K_2 \cdot b_2 + ... + K_m \cdot b_m}{\sum_{i=1}^{m} b_i}$$

де: $b_i$ - ваговий коефіцієнт за кожну контрольну роботу.

Поточні оцінки за кожну складову (П, $K$, І,... ) виставляються за 100-бальною шкалою згідно з положенням «Про критерії та систему оцінювання знань та вмінь і про рейтинг здобувачів вищої освіти» НТУ «ХПІ».

Підсумкова оцінка виставляється відповідно до розрахованої О з округленням до найближчого цілого числа в більшу сторону.

**Шкала оцінювання**

| Сума балів | Національна оцінка | ECTS |
|---|---|---|
| 90–100 | Відмінно | A |
| 82–89 | Добре | B |
| 75–81 | Добре | C |
| 64–74 | Задовільно | D |
| 60–63 | Задовільно | E |
| 35–59 | Незадовільно (потрібне додаткове вивчення) | FX |
| 1–34 | Незадовільно (потрібне повторне вивчення) | F |

## Норми академічної етики і політика курсу

Здобувач вищої освіти повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту.
Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

## Погодження

| | | | |
|---|---|---|---|
| Силабус погоджено | 30.08.2025 | | **Завідувач кафедри**<br>Сергій ЄВСЕЄВ |
| | 30.08.2025 | | **Гарант ОП**<br>Сергій ЄВСЕЄВ |