МАШИННЕ НАВЧАННЯ У КІБЕРБЕЗПЕЦІ

ОПИС КУРСУ

Машинне навчання у кібербезпеці – це вибірковий курс підготовки студентів у сфері інформаційних технологій. Проходження цього курсу дозволяє студентам опанувати і професійно використовувати термінологію машинного навчання (Machine learning, ML), розуміти і пояснювати різні явища і процеси у сфері кібербезпеки, розроблювати програмне забезпечення (ПЗ) для вирішення проблем у сфері кібербезпеки.

У курсі розглядаються основні задачі кібербезпеки, які розв'язуються з використанням методів машинного навчання, наприклад: фільтрація спаму за допомогою методів класифікації та методів обробки природної мови (NLP); виявлення аномалій за даними мережевого трафіку на основі методів неконтрольованого машинного навчання; виявлення зловмисного ПЗ за допомогою штучних нейронних мереж Convolutional Neural Networks та ін.

Дисципліна є вибірковим для вивчення бакалаврами з комп'ютерних наук, оскільки створює додаткову основу для вивчення методів штучного інтелекту та розробки програмного забезпечення у сфері кібербезпеки

є

ВИМОГИ

– базові знання з кібербезпеки, вищої математики, чисельних методів, дослідження операцій, теорії ймовірностей та математичної статистики, з основ штучного інтелекту;

– навички програмування, наприклад мовами Python або Java;

– наявність корпоративного облікового запису @mipolytech.education, Microsoft Teams, Word, Excel;

– наявність особистого логіну та паролю в Moodle (для отримання або поновлення слід звернутися до відповідальної особи на факультеті).

Освітній рівень	Бакалавр
Кількість кредитів	5,0
Назва кафедри, яка пропонує дисципліну	Цифрових технологій та проєктно-аналітичних рішень

МОСКАЛЕНКО Валентина

valentina.moskalenko@mipolytech.education

Доктор технічних наук, професор, фахівець у сфері розробки інформаційних систем, застосування методів, моделей обчислюваного інтелекту та машинного навчання для розв'язання задач управління складними організаційними системами

ПРОГРАМНІ РЕЗУЛЬТАТИ НАВЧАННЯ

- знати та використовувати методи обчислювального інтелекту, машинного навчання, нейромережеві технології для розв'язання задач розпізнавання, прогнозування, класифікації, ідентифікації різних кіберзагроз;
- пояснювати концепцію інформаційної безпеки, принципи безпечного проєктування програмного забезпечення;
- застосовувати методи машинного навчання у задачах класифікації, прогнозування, кластерного аналізу кіберзагроз з використанням технологій DataMining та методів обробки природної мови (NLP);
- демонструвати навички аналізу результатів використання методів машинного навчання, а також вміння обирати ефективні методи для розв'язання задач кібербезпеки;
- використовувати навички розробки ПЗ для створення програмних систем для вирішення проблем у сфері кібербезпеки;
- вміти самостійно працювати, демонструвати критичне, креативне, самокритичне мислення.

ТЕМАТИКА

Застосування штучного інтелекту та машинного навчання у кібербезпеці. Основні відомості про кібербезпеку та особливості сучасних кіберзагроз. Еволюція ШІ для кібербезпеки. Вплив генеративного ШІ на кібербезпеку. Інструменти кібербезпеки на базі ШІ. Сучасні рішення для кібербезпеки на базі ШІ. Класифікація машинного навчання та основні задачі ML. Життєвий цикл машинного навчання та історія використання ML. Кібербезпека ПЗ з ML.

Методи контрольованого навчання для задач кібербезпеки. Використання методів контрольованого навчання (Supervised Learning) для задач кібербезпеки. Загальний опис методів класифікації, регресії для задач кібербезпеки. Дерева рішень (Decision tree) для задач кібербезпеки. Регресія, типи регресії. Алгоритм K-Nearest Neighbors для задач кібербезпеки. Розв'язання задачі фільтрації спаму за допомогою наївного Байєсівського класифікатору (Naïve Bayes); рандомні дерева (Random Forest Classifier); k -найближчих сусідів (K-Neighbors Classifier); машин опорних векторів (Support Vector Machines).

Методи обробки природної мови (NLP) для задач кібербезпеки. Основні компоненти та задачі обробки природної мови (NLP). Методи обробки природної мови (NLP) для задач кібербезпеки. NLP для посилення моделей кібербезпеки. Типи алгоритмів NLP, найкращі для задач кібербезпеки. Інжиніринг ознак у NLP.

Методи неконтрольованого навчання для задач кібербезпеки. Виявлення аномалій з використанням методів машинного навчання Unsupervised Learning. Методи неконтрольованого машинного навчання для вирішення проблем кібербезпеки. Методи кластеризації у кібербезпеці. Методи кластерного аналізу: ієрархічні та дивизимні. Алгоритм k-means та його використання в кібербезпеці. DBSCAN, Mean-shift та інші методи неконтрольованого навчання. Методи машинного навчання для виявлення зловмисного ПЗ.

Виявлення зловмисного ПЗ на основі глибокого навчання. Методи виявлення зловмисного ПЗ. Приклади систем для виявлення зловмисного ПЗ. Використання нейронних мереж у задачах кібербезпеки. Використання згорткових нейронних мереж (Convolutional Neural Networks) для задач кібербезпеки. Системи безпеки мережі. Типи рішень мережевої безпеки. Технології захисту мережевої інфраструктури. Брандмауер, його функції, тенденції змін. Тенденції мережевої безпеки.

ОРГАНІЗАЦІЯ КУРСУ, ФОРМИ ТА МЕТОДИ НАВЧАННЯ

Освітній процес будується як комбінація лекцій та самостійного вивчення навчального матеріалу на платформі Moodle – з одного боку, та проблемно орієнтованих семінарських занять і практичних занять з відпрацювання аналітично-розрахункових навичок – з іншого.

– Відвідування лекційних занять є бажаним, однак не обов'язковим; від студентів очікується ознайомлення з матеріалом перед лекцією, що дозволить побудувати лекційне заняття у вигляді сполучення пояснень викладача та обговорення проблемних питань, які виникли при підготовці до лекції.

– Семінари і практичні заняття передбачають аналіз умовно змодельованих ситуацій та розв'язання задач різних рівнів, розбір реальних кейсів за матеріалами відкритого доступу; їх відвідування є бажаним.

– Від студента потребується виконати індивідуальні завдання та модульні контрольні роботи у терміни, встановлені у розділі «Розподіл балів за контрольними точками та графік їх виконання».

– З урахуванням поточної ситуації від учасників освітнього процесу очікується виконання вимог безпеки при сигналі «Повітряна тривога», санкції за залишення заняття або неявку на заняття не застосовуються.

– Опціонально доступні індивідуальні та групові консультації. З викладачем можна зв'язатися через електронну пошту, в чаті або в персональній розмові в MS Teams.

ПІДХОДИ ДО ОЦІНЮВАННЯ

Розподіл балів за контрольними точками та графік їх виконання

Тижні / Види контр. точок	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	Всього
Робота на практичних заняттях								15							15				30
Виконання індивідуальних завдань									15							15			30
Модульні контрольні роботи										20							20		40
Всього																			100

Зміст та вимоги до контрольних точок

Назва контрольної точки	Опис контрольної точки, порядок її проходження та отримання балів
Робота на практичних заняттях (обговорення виконання ІЗ та його захист)	Оцінка за роботу на практичному (семінарському) занятті оголошується наприкінці заняття і може бути оскаржена одразу ж. Max 15 балів: – студент під час презентації / захисту свого індивідуального завдання та контрольної роботи у вигляді есе демонструє володіння термінологічним апаратом, методами машинного навчання, проєктування

	та розробки ПЗ, відповідає на запитання, здатний швидко адаптувати моделі, методи під зміни в умовах задачі (10 бали); – студент дав пряму і релевантну відповідь на поставлене питання з використанням обґрунтованого посилання на теоретичний матеріал демонструє володіння термінологічним апаратом, методами проєктування ПЗ та методів машинного навчання, здатний адаптувати моделі під зміни завдання, у т.ч. у вигляді додаткових запитань / зміг стисло формалізувати вербально сутність задачі кібербезпеки, визначити ключові складові виконання практичної роботи, критерії якості отриманих результатів (5 бали).
Виконання індивіду-ального завдання	Підготовлене есе у вигляді файлу *docx, або *pdf розміщується у відповідному розділі дисципліни в Moodle і перевіряється протягом тижня після завершення терміну подачі. Оскарження оцінки може бути здійснене на останньому практичному занятті модуля. Max 15 балів: – студент підготував роботу відповідно до поставленого завдання, в якій: правильно визначив задачу, методи, які необхідно застосувати для її розв'язання, обґрунтував своє бачення теоретичними концепціями або моделями, виконав необхідну розробку ПЗ, надав результати роботи ПЗ та провів їх аналіз у разі потреби, представив висновок або власне бачення розв'язання задачі і окреслив можливі перспективи використання отриманих результатів, обмеженість отриманого рішення, навів за необхідності обґрунтування використання інших методів; робота структурована, викладена діловим, науковим або діловим стилем (10 балів); – робота містить комплексну, логічну і оригінальну пропозицію щодо використання методів розв'язання задачі індивідуального завдання аж до міждисциплінарного підходу; використання штучного інтелекту (ШІ) не забороняється, оскільки пропозиції відомих застосунків ШІ суттєво залежать від обміркованої постановки питання і уточнюючих питань; однак у разі, якщо відповідь, отримана з використанням ШІ, не є комплексною або не відповідає за стилем і викладеними позиціями іншим частинам роботи або завдання, містить очевидно неправдиву інформацію, то оцінка за цим критерієм знижується (5 балів)
Модульні контрольні роботи	МКР виконуються як есе у вигляді файлу *docx, або *pdf розміщується у відповідному розділі дисципліни в Moodle і перевіряється протягом тижня після завершення терміну подачі Кількість спроб не обмежується. Кожна модульна контрольна робота включає блок завдань з матеріалу модуля (max 20 балів). Завдання передбачають обґрунтування вибору методів машинного навчання для розв'язання конкретної задачі кібербезпеки, розробку ПЗ згідно завдання, відповіді на теоретичні питання з тем модуля. При оцінюванні МКР враховується логіка та обґрунтованість представленого матеріалу – знання та вибір методів машинного навчання для розв'язання задач кібербезпеки, аналіз отриманих результатів та правильність формування висновків.

Додаткові зауваження:

– студент може оскаржити отримані оцінки в порядку, передбаченому Положенням про організацію освітнього процесу (Нормативні документи : Polytechnic (metinvest.university))та Положенням про політику та процедури врегулювання конфліктних ситуацій (Академічні політики : Polytechnic (metinvest.university))

– оцінки, отримані за роботу на практичних заняттях не можуть бути відпрацьовані або покращені, окрім процедури оскарження, оцінки за інші види поточного контролю можуть бути покращені за індивідуальною домовленістю з викладачем;

– викладач не має права знижувати оцінку за індивідуальне завдання або модульну контрольну роботу, якщо вони не були складені вчасно, однак в разі, якщо така робота була оцінена пізніше, ніж момент завершення теоретичного навчання у семестрі, то відповідна оцінка не враховується у рейтингу здобувачів освіти.

Форма підсумкового контролю. Порядок визначення підсумкової оцінки

Форма підсумкового контролю	Залік, тобто підсумкова оцінка вставляється як сума оцінок поточного контролю без проведення додаткових контрольних заходів,
Умови допуску до підсумкового контролю	Якщо сума оцінок за поточний контроль за семестр становить менше 60 балів, необхідно відпрацювати відповідні види контролю поточної успішності до звершення теоретичного навчання
Порядок визначення підсумкової оцінки	Для заліку: – якщо протягом семестру за результатами поточного контролю здобувач освіти набрав менше 60 балів, то під час екзаменаційної сесії йому надається змога отримати/покращити власний результат з усіх видів поточного контролю, крім активності на навчальних заняттях; – в разі, якщо протягом семестру за результатами поточного контролю або в процесі покращення власних результатів здобувач освіти набрав більше 60 балів, йому виставляється фактична сума балів і оцінка «залік», в іншому випадку – «незалік».

Відповідність між прийнятими в університеті шкалами оцінки наведена в таблиці

Бальна шкала	**Рівні**	**Характеристика**	**Традиційні шкали**	
			Іспит	**Залік**
90-100	A	Студент демонструє видатний рівень досягнення запланованих результатів вивчення навчальної дисципліни, що засвідчують його безумовну готовність до подальшого навчання та/або професійної діяльності за фахом	Відмінно	Залік
82-89	B	Студент виявляє вищий за середній рівень досягнення запланованих результатів вивчення навчальної дисципліни та готовності до подальшого навчання та/або професійної діяльності за фахом, в його знаннях або діях присутні незначні помилки	Добре	
75-81	C	Студент виявляє середній рівень досягнення запланованих результатів вивчення навчальної дисципліни та готовності до подальшого навчання та/або професійної діяльності за фахом, в його знаннях або діях присутні деякі значущі помилки		
67-74	D	Студент виявляє задовільний рівень досягнення запланованих результатів вивчення навчальної дисципліни та готовності до подальшого навчання та/або професійної діяльності за фахом, в його знаннях або діях наявні суттєві помилки	Задовільно	
60-66	E	Наявні мінімально достатні для подальшого навчання та/або професійної діяльності за фахом результати вивчення навчальної дисципліни		
35-59	FX	Низка запланованих результатів навчання не досягнуті. Рівень наявних результатів навчання є недостатнім для подальшого навчання та/або професійної діяльності за фахом	Незадовільно	Незалік
0-34	F	Результати навчання відсутні або критично низькі		

ОСОБЛИВІ ПІДХОДИ ДО ВИЗНАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

– у разі, якщо здобувач освіти засвоїв повністю або частково відповідні програмні результати навчання під час отримання освіти на попередніх кваліфікаційних рівнях або інших дисциплінах, то кредити та оцінка з даної дисципліни може бути перезарахована у порядку, передбаченому Положенням про організацію освітнього процесу (Нормативні документи: Polytechnic (metinvest.university)). Консультацію з даного питання можна отримати у викладача, куратора або гаранта освітньої програми, завідувача кафедри, за якою закріплено цю дисципліну;

– у разі, якщо здобувач освіти обрав цю дисципліну як дисципліну вільного вибору, не зважаючи на той факт, чи вивчалася вона раніше, оцінка та кредити з цієї дисципліни не перезараховуються;

– у разі, якщо здобувач освіти хотів би самостійно вивчити певні курси з методів бізнес-аналізу для проєктування систем цифрового інтелекту (наприклад, Coursera, Udemy або інших платформ, в т.ч. платформ відкритих курсів вітчизняних та/або закордонних університетів), то 1) доцільно звернутися до списку рекомендованих вебресурсів або проконсультуватися з викладачем на предмет релевантності самостійно знайденого освітнього ресурсу програмі дисципліни; 2) у разі успішності опанування такого курсу, яке підтверджується сертифікатом або іншим способом, такому здобувачу у порядку, визначеному Положенням про визнання результатів навчання, набутих у неформальній/інформальній освіті Нормативні документи : Polytechnic (metinvest.university), такі результати можуть бути зараховані замість оцінки з певного виду поточного контролю;

– у разі, якщо здобувач освіти реалізував певний вид наукової роботи (тези, стаття, результативна участь у студентській олімпіаді тощо), то у порядку, визначеному Положенням про визнання результатів навчання, набутих у неформальній/інформальній освіті Нормативні документи : Polytechnic (metinvest.university), такі результати можуть бути зараховані замість оцінки з певного виду поточного або навіть підсумкового контролю; консультацію з питань визнання результатів неформальної та інформальної освіти можна отримати в уповноваженої особи; перелік таких осіб можна знайти за посиланням Студентам : Polytechnic (metinvest.university).

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1 Deisenroth M. P., Faisal A. A., Ong C. S. Mathematics for Machine Learning. Cambridge University Press, 2020. 412 p. URL: https://mml-book.github.io/book/mml-book.pdf.
2 Sarker IH. Machine Learning: Algorithms, Real-World Applications. Springer, 2021. URL: https://www.researchgate.net/publication/350297716_Machine_Learning_Algorithms_Real-World_Applications_and_Research_Directions.
3 Crowe, R. H., Hannes, Caveness, Emily, Zhu, Di Machine Learning Production Systems. 1st Ed.Print. O'Reilly Media Inc., 2024. 475 p. URL: https://read.kortext.com/library/books/3166214.
4 Younes, L. Introduction to machine learning. arXiv preprint arXiv:2409.02668. 2024. URL: https://arxiv.org/pdf/2409.02668.
5 Jo, T. Machine Learning Foundations. Supervised, Unsupervised, and Advanced Learning. Springer Nature Switzer-land AG, 2021. 391 p. DOI:10.1007/978-3-030-65900-4
6 Aggarwal, Charu C. Neural Networks and Deep Learning 2nd Ed. Springer Nature, 2023. 677 p. URL: https://read.kortext.com/library/books/2380843.
7 Sarker IH. Machine Learning: Algorithms, Real-World Applications. Springer, 2021. URL: https://www.researchgate.net/publication/350297716_Machine_Learning_Algorithms_Real-World_Applications_and_Research_Directions.
8 Nielsen M. Neural Networks and Deep Learning. URL: https://static.latexstudio.net/article/2018/0912/neuralnetworksanddeeplearning.pdf.
9 Russell St., Norvig P. Artificial Intelligence: A Modern Approach, 4th US ed.. Pearson, 2020. 1136 p URL: https://dl.ebooksworld.ir/books/Artificial.Intelligence.A.Modern.Approach.4th.Edition.Peter.Norvig.%20Stuart.Russell.Pearson.9780134610993.EBooksWorld.ir.pdf.
10 Email Spam Detection with Machine Learning: A Comprehensive Guide. URL: https://medium.com/@azimkhan8018/email-spam-detection-with-machine-learning-a-comprehensive-guide-b65c6936678b/

АКАДЕМІЧНІ ПОЛІТИКИ

Як член спільноти Технічного університету «МЕТІНВЕСТ ПОЛІТЕХНІКА» Ви маєте дотримуватися певних стандартів та академічної політики:

– ***Академічна недоброчесність*** вигляді академічного плагіату; фабрикації; фальсифікації; списування обману; хабарництва; необ'єктивного оцінювання; надання здобувачам освіти під час проходження ними оцінювання результатів навчання допомоги чи створення перешкод, не передбачених умовами та/або процедурами проходження такого оцінювання; впливу у будь-якій формі (прохання, умовляння, вказівка, погроза, примушування тощо) на педагогічного (науково-педагогічного) працівника з метою здійснення ним необ'єктивного оцінювання результатів навчання – прямо заборонено (докладніше про це – у Положенні про академічну доброчесність здобувачів вищої освіти та науково-педагогічних працівників ТОВ ТЕХНІЧНОГО УНІВЕРСИТЕТУ «МЕТІНВЕСТ ПОЛІТЕХНІКА»); і в разі виявлення – ***відповідний захід контролю (контрольну точку) буде оцінено в 0 балів за з наступним повідомленням декану факультету та голові комісії з академічної доброчесності Університету***.

– У разі випадку надання здобувачам освіти під час проходження ними оцінювання результатів навчання допомоги чи створення перешкод, не передбачених умовами та/або процедурами проходження такого оцінювання; впливу у будь-якій формі (прохання, умовляння, вказівка, погроза, примушування тощо) на педагогічного (науково-педагогічного) працівника з метою здійснення ним необ'єктивного оцінювання результатів навчання студент може оскаржити процедури оцінювання за процедурами, передбаченими Положенням про організацію освітнього процесу (розділ 10).

– Матеріали в рамках курсу, захищені авторським правом, можуть бути використані лише тільки здобувачами освіти, яким призначено даний курс і для цілей, пов'язаних з цим курсом і не можуть поширюватися.

– Спілкування з однокурсниками та викладачем має бути професійним та ввічливим.

– Очікується, що Ви перевірятимете всі Ваші письмові повідомлення, включаючи поштові повідомлення та повідомлення у MS Teams на коректність змісту та мови.

– Університет прагне підтримувати середовище, вільне від дискримінації або дискримінаційних домагань, спрямованих на будь-яку людину або групу в межах своєї спільноти - здобувачів освіти, співробітників або відвідувачів.

Докладніше про академічні політики стосовно етичності поведінки, академічної доброчесності та протидію булінгу можна дізнатися за посиланням: Академічні політики - Polytechnic (metinvest.university)