**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

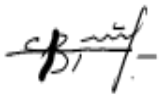
**Львівський національний університет імені Івана Франка**

**Факультет прикладної математики та інформатики**

**Кафедра кібербезпеки**

**Затверджено**
На засіданні кафедри кібербезпеки
факультету прикладної математики
та інформатики
Львівського національного університету
імені Івана Франка
(Протокол №9/24 від 29 серпня 2024 р.)

Завідувач кафедри



Петро ВЕНГЕРСЬКИЙ

# Силабус з навчальної дисципліни

# "Методи ШІ в управлінні ризиками кібербезпеки",

# що викладається в межах ОПП Технології штучного інтелекту в кібербезпеці другого (магістерського) рівня вищої освіти для здобувачів з спеціальності 125 Кібербезпека та захист інформації

**Львів - 2024**

| | |
|---|---|
| **Назва дисципліни** | Методи ШІ в управлінні ризиками кібербезпеки |
| **Адреса викладання дисципліни** | м. Львів, вул. Університетська 1 |
| **Факультет та кафедра, за якою закріплена дисципліна** | Факультет прикладної математики та інформатики<br>Кафедра кібербезпеки |
| **Галузь знань, шифр та назва спеціальності** | 12 – інформаційні технології<br>125 – кібербезпека та захист інформації |
| **Викладачі дисципліни** | Пархуць Любомир Теодорович, д.т.н.,<br>професор кафедри кібербезпеки,<br>Прокопишин Іван Анатолійович,<br>доцент кафедри математичної економіки, економетрії, фінансової та страхової математики |
| **Контактна інформація викладачів** | Liubomyr.Parkhuts@lnu.edu.ua ,<br>https://ami.lnu.edu.ua/employee/parkhuts-l-t<br>ivan.prokopyshyn@lnu.edu.ua<br>http://new.mmf.lnu.edu.ua/employee/prokopyshyn-i-a<br>Головний корпус ЛНУ ім. І. Франка, каб. 376<br>м. Львів, вул. Університетська, 1 |
| **Консультації з питань навчання по дисципліні відбуваються** | Консультація проводиться за розкладом консультацій викладача. Можливі дистанційні консультації за попередньою домовленістю. |
| **Сторінка курсу** | https://ami.lnu.edu.ua/admission/specializations |
| **Інформація про дисципліну** | Дисципліна "Методи ШІ в управлінні ризиками кібербезпеки" є вибірковою дисципліною з спеціальності 125 Кібербезпека та захист інформації для освітньої програми "Технології штучного інтелекту в кібербезпеці", яка викладається в 3-му семестрі в обсязі 3-ох кредитів (за Європейською Кредитно-Трансферною Системою ECTS). |
| **Коротка анотація дисципліни** | Поняття ризику. Аналіз ризиків ІБ: активи, вразливості, загрози, захист. Якісна та кількісна оцінка інформаційного ризику, вибір контрзаходів та управління ризиками. Стохастичне моделювання ризику, економічна оцінка ризику та ефективності інвестицій в системи захисту інформації. Онтологічна модель систем управління ризиками інформаційної безпеки, декомпозиція проблеми управління ризиками. Методи ШІ виявлення потенційних ризиків ІБ. Прогнозне моделювання та аналіз ризиків. Обробка ризиків з використанням систем прийняття рішень на основі ШІ, оптимізації ресурсів у системах ІБ. Методики управління інформаційною безпекою та ризиками, програмні засоби оцінки, моніторингу та управління ризиками. |
| **Мета та цілі дисципліни** | Метою викладання дисципліни є навчити студентів методів аналізу, оцінювання та управління ризиками з використанням методів ШІ, а |

| | |
|---|---|
| | також сформувати у студентів уміння структурно-логічного опису систем захисту та стохастичного моделювання можливих втрат, кількісної оцінки ризиків та економічної ефективності систем захисту. |
| **Література для вивчення дисципліни** | **Базова**<br>1. ДСТУ ISO/IEC 27005:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки.<br>2. ДСТУ EN IEC 31010:2022. Керування ризиками – методи оцінки ризиків.<br>3. Потій О.В. Аналіз методів оцінки і управління ризиками кібер- і інформаційної безпеки / О. В. Потій, Ю. І. Горбенко, О. А. Замула, К. В. Ісірова // Всеукраїнський міжвідомчий науково-технічний збірник "Радіотехніка". Вип. 206. Харків : ХНУРЕ, 2021. С. 1-25.<br>4. Allen B, Babst B., Hicks T. A. Building a Cyber Risk Management Program. O'Reilly, 2024. 204 p.<br>5. Brij B. Gupta, Quan Z. Sheng. Machine Learning for Computer and Cyber SecurityPrinciple, Algorithms, and Practices, 2019, 364 p.<br>6. Clarence Chio, David Freeman. Machine Learning and Security: Protecting Systems with Data and Algorithms 1st Edition, 2019, 386 p.<br>7. Sarker I.H. Machine Learning: Algorithms, Real-World Applications and Research Directions. *SN COMPUT. SCI.* 2, 160 (2021). https://doi.org/10.1007/s42979-021-00592-x<br>8. Sirag H., Awadelkariem S.D. (2022) A Review on Intrusion Detection System Using Machine Learning Algorithms. Proceedings of International Conference on Emerging Technologies and Intelligent Systems. ICETIS 2021. Lecture Notes in Networks and Systems, vol 322. Springer, Cham.<br>**Допоміжна**<br>9. Корченко О. Г., Казмірчук С.В., Ахметов Б.Б. Прикладні системи оцінювання ризиків. Київ: ЦП "Компринт", 2017. 435 с.<br>10. Засоби штучного інтелекту: навч. посіб. / Р. О. Ткаченко, Н. О. Кустра, О. М. Павлюк, У. В. Поліщук. Львів: Вид-во Львів. політехніки, 2014. 204 с.<br>11. Системи штучного інтелекту: навч. посіб. / Ю. В. Нікольський, В. В. Пасічник, Ю. М. Щербина. Львів: Магнолія-2006, 2013. 279 с.<br>12. A multicriterial analysis of the efficiency of conservative information security systems / Dudykevych V., Prokopyshyn I., Chekurin V., Opirskyy I., Lakh Yu., Kret T., Ivanchenko Ye., Ivanchenko I. // Eastern-European Journal of Enterprise Technologies. 2019. Vol. 3, Issue 9 (99). P. 6–13.<br>13. Jemimah Rodriguez. The 7 Best Free and Open Source Risk Management Software. https://www.goodfirms.co/risk-management-software/blog/best-free-open-source-risk-management-software<br>14. Tess Hanna. The 12 Best Risk Management Software and Programs for 2024 https://solutionsreview.com/backup-disaster-recovery/the-best-risk-management-software/<br>15. Artificial Intelligence (AI) Applied to Risk Management // The |

| | |
|---|---|
| | Federation of European Risk Management Associations (FERMA). https://www.ferma.eu/publication/artificial-intelligence-ai-applied-to-risk-management/<br><br>16. AI and Machine Learning for Risk Management // Visure Solutions, Inc. https://visuresolutions.com/uk/blog/ai-and-machine-learning-for-risk-management/#elementor-toc__heading-anchor-1 |
| **Обсяг курсу** | Загальний обсяг: 90 годин. Аудиторних занять: 48 год., з них 16 год. лекцій та 32 год. лабораторних робіт. Самостійної роботи: 42 год. |
| **Очікувані результати навчання** | В результаті вивчення дисципліни фахівець повинен **знати:**<br>– етапи загального процесу управління ризиками інформаційної безпеки;<br>– основи стохастичного моделювання ризику, економічні показники ризику та методи їх розрахунку;<br>– алгоритми машинного навчання та часових рядів для виявлення закономірностей та аномалій інформаційних потоків;<br>– методи прогнозного моделювання та аналізу ризиків з використанням нейронних мереж та часових рядів<br>– Підготовлений фахівець повинен **вміти**:<br>– аналізувати вразливості та загрози, оцінювати відповідні ризики, вибирати засоби захисту;<br>– оцінювати економічний ризик та ефективність інвестицій у системи захисту;<br>– застосовувати алгоритми машинного навчання та часові ряди для ідентифікації ризиків, аналізу та прогностичного моделювання ризиків. |
| **Ключові слова** | Ризики, якісне оцінювання ризику, кількісне вимірювання ризику, міри ризику, ефективність інвестицій, управління ризиком, штучний інтелект, нейронні мережі, машинне навчання, часові ряди. |
| **Формат курсу** | Очний.<br>Проведення лекцій, лабораторних занять і консультацій. |
| **Теми** | Теми подані у Схемі курсу нижче |
| **Підсумковий контроль, форма** | Залік в кінці 3-го семестру |
| **Пререквізити** | Для вивчення курсу студенти потребують базових знань з курсів :<br>– Теорія ймовірностей та математична статистика<br>– Машинне навчання та адаптивний інтелект<br>– Нейронні мережі в задачах кібербезпеки |
| **Навчальні методи та тех.-ніки, які бу-** | Презентації, лекції, лабораторні роботи, індивідуальні завдання, індивідуальні доповіді, самостійна робота.<br>Лекційні та лабораторні: інформаційно-рецептивний метод, |

| | |
|---|---|
| **дуть використовуватися під час викладання курсу** | репродуктивний метод, евристичний метод, метод проблемного викладу. Самостійна робота: репродуктивний метод, дослідницький метод. |
| **Необхідне обладнання** | Комп'ютерний клас із вільно-доступним програмним забезпеченням, локальна комп'ютерна мережа, доступ до Internet мережі. |
| **Критерії оцінювання (окремо для кожного виду навчальної діяльності)** | Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням:<br>• лабораторні роботи: 48% семестрової оцінки; максимальна кількість балів – 48;<br>• реферат і доповідь: 20% семестрової оцінки; максимальна кількість балів – 20;<br>• контрольний тест: по 20% семестрової оцінки; кількість балів – 20.<br>• додаткові бали за поточне опитування на лекціях і лабораторних заняттях 12% семестрової оцінки; максимальна кількість балів – 12.<br>Підсумкова максимальна кількість балів – 100.<br>**Академічна доброчесність:** очікується, що роботи студентів будуть оригінальними дослідженнями чи міркуваннями. Списування та втручання в роботу інших студентів становлять, але не обмежують, приклади можливої академічної недоброчесності. Виявлення ознак академічної недоброчесності в написанні завдань є підставою для її незарахуванння викладачем, незалежно від масштабів плагіату чи обману. Жодні форми порушення академічної доброчесності не толеруються.<br>**Відвідання занять** є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції та лабораторні заняття курсу. Студенти повинні інформувати викладача про неможливість відвідати заняття. У будь-якому випадку студенти зобов'язані дотримуватися термінів визначених для виконання всіх видів робіт, передбачених курсом.<br>**Література.** Уся література, яку студенти не зможуть знайти самостійно, буде надана викладачем виключно в освітніх цілях без права її передачі третім особам. Студенти заохочуються до використання також й іншої літератури та джерел, яких немає серед рекомендованих.<br>**Політика виставлення балів.** Враховуються бали, набрані при поточному контролі та бали за виконання лабораторних робіт. При цьому обов'язково враховуються присутність на заняттях та активність студента під час лабораторного заняття; недопустимість пропусків та запізнень на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття в цілях не пов'язаних з навчанням; списування та плагіат; несвоєчасне виконання поставленого завдання і т. ін.<br>**Оцінювання на лекційних заняттях:** поточне опитування по 1-2 бали за правильну відповідь, сумарно – до 6 балів.<br>**Оцінювання роботи на лабораторних заняттях:**<br>1) поточне опитування по 1-2 бали за правильну відповідь, сумарно – до 6 балів;<br>2) виконання 6-ти лабораторних робіт по 8 балів, сумарно – 48 балів. Бали оцінювання лабораторної роботи нараховуються пропорційно кількості виконаних завдань з лабораторної роботи з урахуванням відповідей на поставлені запитання. За оригінальне виконання |

| | |
|---|---|
| | лабораторної роботи може додаватися 1-2 бали.<br>**Оцінювання самостійної роботи.** За рахунок годин самостійної роботи студенти освоюють теоретичний матеріал, виконують лабораторні роботи, готують реферат а також здійснюють підготовку до контрольної роботи. Спеціальне оцінювання не проводиться.<br><br>**Оцінювання контрольної роботи:** 20 тестових теоретичних та практичних запитань 5 – по 1 балу, 3 – по 2 бали і 3 – по 3 бали. Максимальна оцінка – 20 балів.<br>**Оцінювання реферату.** Студент подає на захист роздрукований реферат і виголошує доповідь, розподіл балів: зміст і оформлення реферату – до 10 балів, виступ за матеріалом реферату – до 5 балів, відповідь на додаткові запитання – до 5 балів. Максимальна оцінка – 20 балів. За зразково підготовлений реферат, який змістовно та вичерпно висвітлює тему може буди додано до 3 додаткових балів.<br><br>**Критерії оцінювання результатів неформальної освіти:**<br>Нарахування балів відбувається за публікацію студентом тез доповідей на конференціях, наукових статей, за участь студента у діяльності наукових гуртків, семінарів, круглих столів, конкурсів, участь у заходах неформальної освіти, за отримання сертифікатів про проходження навчання на різних освітніх платформах (Coursera, Prometheus тощо). Кількість балів визначається відсотком покриття результатів відповідної активності до вимог результатів навчання з навчальної дисципліни. |
| **Питання до контрольної роботи. Залік.** | Питання контрольної роботи відповідають темам курсу.<br>Залік – за результатами поточного контролю протягом семестру і, за потреби, додаткове усне опитування за тематикою курсу. |
| **Опитування** | Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу. |

## Схема курсу

| Тиж. | Тема, план, короткі тези | Форма діяльності (заняття) | Література | Завдання, год. | Термін виконання |
|---|---|---|---|---|---|
| 1 | **1. Ризики у сфері інформаційної безпеки**<br>Поняття ризику. Ймовірнісний та економічний аспекти ризику. Системи управління інформаційною безпекою (СУІБ). Роль та місце аналізу та управління ризиками в СУІБ. Міжнародні стандарти СУІБ та управління ризиками інформаційної безпеки (ІБ). | лекція,<br>лаб.,<br>самостійна робота | [1-3, 6, 11,12] | 2<br>2<br>5 | 1 тиждень |

| | | | | | |
|---|---|---|---|---|---|
| 2 | **2. Управління ризиками інформаційної безпеки**<br>Загальний процес управління ризиками ІБ. Встановлення контексту, оцінка ризиків (ідентифікація, вимірювання, встановлення значущості). Методи обробки ризиків (зниження, збереження, уникнення, перенесення). | лекція,<br>лаб.,<br>самостійна робота | [1-3, 6, 11,12] | 2<br>4<br>5 | 1 тиждень |
| 3 | **3. Економічна оцінка ризику та ефективності захисту**<br>Стохастичне моделювання економічного ризику, випадкова велична втрат. Міри ризику, аксіоматика когерентних мір ризику. Структурно-логічний опис консервативних систем захисту, об'єкти захисту, вразливості, засоби захисту. Дискретна ймовірнісна модель втрат, оцінка економічного ризику, раціональний вибір засобів захисту. | лекція,<br>лаб.,<br>самостійна робота | [2, 3, 11, 12] | 2<br>6<br>6 | 1 тиждень |
| 4 | **4. Методи штучного інтелекту в кібербезпеці**<br>Поняття штучного інтелекту (ШІ). Низхідний та висхідний підходи до побудови систем штучного інтелекту. ШІ в задачах кібербезпеки. Переваги ШІ в управлінні ризиками. Онтологічна модель систем управління ризиками інформаційної безпеки (СУРІБ). Декомпозиція проблеми управління ризиками. | лекція,<br>лаб.,<br>самостійна робота | [4, 5, 7, 10, 15, 16] | 2<br>4<br>5 | 1 тиждень |
| 5 | **5. Ідентифікація ризиків ІБ**<br>Методи ШІ виявлення потенційних ризиків ІБ. Алгоритми виявлення аномалій в інформаційних потоках. Машинне навчання та часові ряди для виявлення закономірностей та аномалій. | лекція,<br>лаб.,<br>самостійна робота | [7, 8, 10] | 2<br>4<br>5 | 1 тиждень |
| 6 | **6. Прогнозне моделювання та аналіз ризиків**<br>Створення прогностичних моделей ризику методами машинного навчання. Нейронні мережі для прогнозування ймовірності кібератак на основі даних про | лекція,<br>лаб.,<br>самостійна робота | [4, 8, 9, 15, 16] | 2<br>4<br>5 | 1 тиждень |

| | | | | | |
|---|---|---|---|---|---|
| | мережний трафік. Методи прогнозування часових рядів. Корпоративні платформи прогнозної аналітики з використанням методів штучного інтелекту. | | | | |
| 7 | **7. ШІ в задачах обробки моніторингу та комплаєнсу ризиків ІБ**<br>Обробка ризиків ІБ з використанням систем прийняття рішень на основі ШІ. Проблема оптимізації ресурсів у системах ІБ. Автоматизація комплаєнсу та документування ризиків. | лекція,<br>лаб.,<br>самостійна робота | [4, 8, 9, 13-16] | 2<br>4<br>5 | 1 тиждень |
| 8 | **8. Інструментальні засоби управління ризиками**<br>Методики управління інформаційною безпекою та ризиками, програмні засоби оцінки, моніторингу та управління ризиками. | лекція,<br>лаб.,<br>самостійна робота | [11, 13-16] | 2<br>4<br>6 | 1 тиждень |