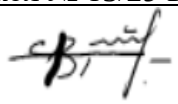
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Львівський національний університет імені Івана Франка
Факультет прикладної математики та інформатики
Кафедра кібербезпеки

Затверджено
На засіданні кафедри кібербезпеки
факультету прикладної математики та інформатики
Львівського національного університету імені Івана Франка
(Протокол № 15/23 від 29 серпня 2023 р.)



Завідувач кафедри _____ П. С. Венгерський

Силабус з навчальної дисципліни
"Управління ризиками",
що викладається в межах ОПП
"Кібербезпека"
першого (бакалаврського) рівня вищої освіти для здобувачів з спеціальності 125 Кібербезпека та захист інформації

Львів - 2023

Назва дисципліни	Управління ризиками
Адреса викладання дисципліни	Головний корпус ЛНУ ім. І. Франка м. Львів, вул. Університетська 1
Факультет та кафедра, за якою закріплена дисципліна	Факультет прикладної математики та інформатики Кафедра кібербезпеки
Галузь знань, шифр та назва спеціальності	12 Інформаційні технології 125 Кібербезпека та захист інформації
Викладачі дисципліни	Прокопишин Іван Анатолійович, канд. фіз.-мат. наук, доцент, доцент кафедри математичної економіки, економетрії, фінансової та страхової математики
Контактна інформація викладачів	Головний корпус ЛНУ ім. І. Франка, каб. 376, м. Львів, вул. Університетська, 1 http://new.mmf.lnu.edu.ua/employee/prokopyshyn-i-a ivan.prokopyshyn@lnu.edu.ua
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 "Управління ризиками" є вибірковою дисципліною із спеціальності 125 Кібербезпека та захист інформації для освітньої програми першого (бакалаврського) рівня вищої освіти "Кібербезпека", яка викладається у 6 семестрі в обсязі 5 кредитів (за Європейською Кредитно-Трансферною Системою ECTS)
Коротка анотація дисципліни	Основні концепції та принципи інформаційної безпеки. Поняття ризику. Аналіз ризиків: активи, вразливості, загрози, захист. Якісна та кількісна оцінка інформаційного ризику. Вибір контрзаходів та управління ризиками. Стандарти управління інформаційною безпекою та ризиками. Методики та програмні засоби оцінки, моніторингу та управління ризиками. Стохастичне моделювання ризику, методи розрахунку показників ризику. Економічна оцінка ризику та ефективності інвестицій в консервативні системи захисту інформації.
Мета та цілі дисципліни	Метою викладання дисципліни є навчити студентів методів аналізу, оцінювання та управління ризиками, 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	**Основна література** 1. ДСТУ ISO/IEC 27005:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки. 2. ДСТУ EN IEC 31010:2022. Керування ризиками – методи оцінки ризиків. 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. 4. Управління ризиками: Навчальний наочний посібник / М. О. Кравченко, К. О. Бояринова, К.О. Копішинська. Київ : КПІ ім. Ігоря Сікорського, 2021. 432 с. 5. Hubbard D. W., Seiersen R. How to Measure Anything in Cybersecurity Risk. Wiley, 2023. 345 p. 6. Kuzminykh I., Ghita B., Sokolov V., Bakhshi T. Information Security Risk Assessment // Encyclopedia 2021, 1. P.602–617. **Додаткова література** 7. Заболоцький М. В. Основи фінансової математики: навч. посібник / М. В. Заболоцький, І. А. Прокопишин. Львів: ЛНУ ім. Івана Франка, 2016. 144 с. 8. Корченко О. Г., Казмірчук С.В., Ахметов Б.Б. Прикладні системи оцінювання ризиків. Київ: ЦП "Компринт", 2017. 435 с. 9. Ромака В. А. Менеджмент у сфері захисту інформації: підручник / В. А. Ромака, Р. О. Корж, Ю. Р. Гарасим. Львів: ЗУКЦ, 2013. 462 с. 10. 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. 11. Chapple M., Stewart J.M., Gibson D. (ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide. 9th edition. Wiley, 2021. 1250 p. 12. Chapple M., Seidl D. (ISC)2 CISSP Certified Information Systems Security Professional Official Practice Tests. 3rd edition. Wiley, 2021. 499 p. 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 14. Tess Hanna. The 12 Best Risk Management Software and Programs for 2024 https://solutionsreview.com/backup-disaster-recovery/the-best-risk-management-software/ **Методичні вказівки** 15. Прокопишин І.А. Методичні рекомендації до проведення

	лабораторної роботи "Показники фінансової ефективності інвестицій". – В електронній формі. – 15 с. 16. Прокопишин І.А. Методичні рекомендації до проведення лабораторної роботи "Оцінка економічної ефективності та ризику для консервативних систем захисту". – В електронній формі. – 18 с. **Інформаційні ресурси** 17. Державна служба спеціального зв'язку та захисту інформації України. http://www.dstszi.gov.ua 18. Український цент інформаційної безпеки. http://www.bezpeka.com 19. Інститут спеціального зв'язку та захисту інформації НТУУ "КПІ". http://iszzi.kpi.ua 20. Information System Audit and Control Association (ISACA). http://www.isaca.org , http://www.isaca.org.ua 21. The European Union Agency for Cybersecurity, ENISA. www.enisa.europa.eu 22. International Information System Security Certification Consortium $(ISC)^2$. https://www.isc2.org
Обсяг курсу	Всього 150 годин. З них 32 годин лекцій, 32 годин лабораторних занять та 86 годин самостійної роботи.
Очікувані результати навчання	В результаті вивчення дисципліни фахівець повинен **знати:** - основні положення та принципи інформаційної безпеки, законодавчі та нормативні акти, які регламентують управління ризиками інформаційної безпеки; - етапи загального процесу управління ризиками інформаційної безпеки; - основи стохастичного моделювання ризику, економічні показники ризику та методи їх розрахунку. Підготовлений фахівець повинен **вміти**: - аналізувати вразливості та загрози, оцінювати відповідні ризики, вибирати засоби захисту; - застосовувати методи обробки ризиків, оцінювати залишковий ризик; - оцінювати економічний ризик та ефективність інвестицій у системи захисту інформації засобами електронних таблиць. **Курс забезпечує набуття таких фахових компетентностей:** **ІК, КЗ 2, КЗ 3, КЗ 4, КЗ 5, КФ 1, КФ 7, КФ 9;** **та програмних результатів навчання:** **ПРН 1 – ПРН 8, ПРН 16, ПРН 28, ПРН 29, ПРН 33, ПРН 34, ПРН 44, ПРН 45, ПРН 46 .**
Ключові слова	Інформаційна безпека, системи управління інформаційною безпекою, ризик, якісне оцінювання ризику, кількісне вимірювання ризику, міри ризику, нерівність Кантеллі, управління ризиками, консервативні системи захисту, ефективність інвестицій, умовно збережені кошти.
Формат курсу	Очний.

Теми	**1. Ризики у сфері інформаційної безпеки** [1-7, 9, 10] **2. Фінансово-економічні розрахунки у сфері захисту** [8, 11, 16, 17] **3. Економічна оцінка ризику та ефективності захисту** [11, 17] **4. Управління ризиками інформаційної безпеки (ІБ)** [1-7,9, 10, 12-15]
Підсумковий контроль, форма	Залік
Пререквізити	Для вивчення курсу студенти потребують базових знань з: - Основи математичного аналізу та застосування; - Теорії ймовірностей та математичної статистики; - Програмування - Основи кібербезпеки - Менеджменту інформаційної безпеки;
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Презентації, лекції, лабораторні роботи, індивідуальні завдання, індивідуальні доповіді, самостійна робота. Лекційні та лабораторні: інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу. Самостійна робота: репродуктивний метод, дослідницький метод.
Необхідне обладнання	Комп'ютер із програмним забезпеченням, необхідним для виконання лабораторних робіт (електронні таблиці), доступ до мережі Internet.
Методи оцінювання	Поточне опитування на лекційних та лабораторних заняттях, захист лабораторних робіт, здача тесту. Залік – за результатами поточного контролю протягом семестру і усне опитування.
Критерії оцінювання (окремо для кожного виду навчальної діяльності)	Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням: • лабораторні роботи: 50% семестрової оцінки; максимальна кількість балів – 50; • реферат і доповідь: 20% семестрової оцінки; максимальна кількість балів – 20; • контрольний тест: по 30% семестрової оцінки; кількість балів – 30. Підсумкова максимальна кількість балів – 100. **Академічна доброчесність**: Роботи студентів повинні бути їх оригінальними дослідженнями чи міркуваннями. Відсутність посилань на використані джерела, фабрикування джерел, списування, втручання в роботу інших студентів кваліфікуються як прояви академічної недоброчесності. **Відвідування занять** є важливою складовою навчання. Усі студенти зобов'язані відвідувати усі лекції, практичні та лабораторні зайняття курсу, дотримуватися термінів виконання усіх видів робіт та індивідуальних завдань. **Література.** Уся література, яку студенти не зможуть знайти самостійно, буде надана викладачем виключно в освітніх цілях без права її передачі третім особам. Студенти також заохочуються до використання інших літературних джерел, яких немає серед рекомендованих. **Політика виставлення балів.** Враховуються бали набрані при поточному опитуванні, виконанні самостійних робіт, бали проміжкових та

	підсумкових тестування. Обов'язково враховуються активність студентів під час занять, своєчасність виконання поставлених завдань, не допускається списування та плагіат. Жодні форми порушення академічної доброчесності не толеруються.
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.

Схема курсу "Управління ризиками "

Тижні	Лекції		Практичні заняття		Самост. робота
	Тема заняття	К-ть годин	Тема заняття	К-ть годин	К-ть годин
1	Поняття ризику. Ймовірнісний та економічний аспекти ризику. Системи управління інформаційною безпекою (СУІБ). Роль та місце аналізу та управління ризиками в СУІБ.	4	Фінансові ренти та їх застосування у фінансовому аналізі.	2	4
2			Фінансові розрахунки засобами електронних таблиць. Розрахунок показників фінансової ефективності інвестицій.	2	8
3	Грошові потоки, фінансові ренти. Показники фінансової ефективності інвестицій. Економічна ефективність систем захисту	4	Пояснення ЛР №1 "Оцінка ефективності інвестиційних проектів".	2	4
4			Консультації з ЛР №1. Здача ЛР №1.	2	4
5	Стохастичне моделювання економічного ризику. Когерентні міри ризику. Показник ризику на основі нерівності Кантеллі.	4	Найпростіші ймовірнісні задачі про ураження об'єкта захисту.	2	8
6			Тест 1.	2	4
7	Структурно-логічний опис консервативних систем захисту: об'єкти захисту, канали для атак, засоби захисту. Дискретна ймовірнісна модель втрат.	4	Пояснення ЛР №2 "Оцінка економічної ефективності та ризику для консервативних систем захисту"	2	4

	Оцінка економічного ризику та ефективності систем захисту. Раціональний вибір засобів захисту. Багатокритеріальне оцінювання ризику.				
8			Консультації з ЛР №2	2	8
9	Міжнародні стандарти СУІБ та управління ризиками ІБ. Загальний процес управління ризиками ІБ. Встановлення контексту. Оцінка ризиків (ідентифікація, вимірювання, встановлення значущості). Методи обробки ризиків (зниження, збереження, уникнення, перенесення).	4	Здача ЛР №2	2	4
10			Оцінювання ризику. Якісна оцінка ризику. Кількісне вимірювання ризику	2	4
11	Прийняття ризиків, залишковий ризик. Обмін інформацією щодо ризиків, комунікація. Моніторинг і перегляд показників ризику, вдосконалення процесу управління ризиками. Інструменти аналізу ризиків базового рівня (COBRA, RA Software Tool).	4	Оброблення ризиків ІБ. Вибір контрзаходів та управління ризиками.	2	4
12			Методики та програмні засоби оцінки та управління ризиками ІБ	2	4
13	Засоби повного аналізу ризиків (CRAMM, MethodWare, RiskWatch, Авангард). Аналіз захищеності інформаційних систем, засоби аналізу захищеності.	4	Підготовка реферату про методики та програмні засоби управління ризиками інформаційної безпеки	2	10
14			Доповідь за рефератом.	2	4
15	Мережеві атаки. Мережеві екрани. Виявлення атак.	4	Доповідь за рефератом.	2	8

	Мережеві сканери, засоби контролю захищеності системного рівня. Системи виявлення атак (IDS) та запобігання вторгненням (IPS) як засіб управління ризиками.				
16			Підсумкове заняття. Залік	2	4
Всього		***32***		***32***	***86***