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 "Оцінка ризиків в кібербезпеці", що викладається в межах ОПП "Кібербезпека" першого (бакалаврського) рівня вищої освіти для здобувачів з спеціальності 125 Кібербезпека та захист інформації

Львів - 2023

Назва дисципліни	Оцінка ризиків в кібербезпеці
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	Пархуць Любомир Теодорович, д.т.н., професор, професор кафедри кібербезпеки 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 liubomyr.parkhuts@lnu.edu.ua 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	
Інформація про дисципліну	Дисципліна "Оцінка ризиків в кібербезпеці" є нормативною дисципліною із спеціальності 125 Кібербезпека та захист інформації для освітньої програми першого (бакалаврського) рівня вищої освіти "Кібербезпека", яка викладається у 6 семестрі в обсязі 4 кредити (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 ризику. Стохастичне моделювання ризику, методи розрахунку показників ризику. Економічна оцінка ризику та ефективності інвестицій у системи захисту інформації. Неперервність бізнесу та інформаційна безпека. Планування аварійного відновлення інформаційних систем.
Мета та цілі дисципліни	Метою викладання дисципліни є навчити студентів методів аналізу та оцінювання ризиків, методів забезпечення неперервності функціонування та аварійного відновлення інформаційних систем, 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. Hubbard D. W., Seiersen R. How to Measure Anything in Cybersecurity Risk. Wiley, 2023. 345 p. **Додаткова література** 5. Корченко О. Г., Казмірчук С.В., Ахметов Б.Б. Прикладні системи оцінювання ризиків. Київ: ЦП "Компринт", 2017. 435 с. 6. Заболоцький М. В. Основи фінансової математики: навч. посібник / М. В. Заболоцький, І. А. Прокопишин. Львів: ЛНУ ім. Івана Франка, 2016. 144 с. 7. Пархуць Л., Хома Т., Хмиз О. Організаційно-технічне забезпечення процесу відновлення інформаційно-комунікаційних систем після аварії // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2012, вип. 1(23). – С. 76-83. 8. Положення про плани відновлення діяльності банків України та банківських груп. Постанова Правління Національного банку України 18.07.2019 № 95. 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. ISO 22301:2019 Societal security – Business continuity management systems – Requirements. 12. ISO 22316:2017 Security and resilience – Organizational resilience – Principles and attributes. 13. NIST Special Publication 800-84. Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities. – NIST, 2006. – https://csrc.nist.gov/publications/detail/sp/800-84/final **Інформаційні ресурси** 14. Державна служба спеціального зв'язку та захисту інформації України. http://www.dstszi.gov.ua 15. Український цент інформаційної безпеки. http://www.bezpeka.com 16. Інститут спеціального зв'язку та захисту інформації НТУУ "КПІ". http://iszzi.kpi.ua

	17. Information System Audit and Control Association (ISACA). http://www.isaca.org , http://www.isaca.org.ua 18. The European Union Agency for Cybersecurity, ENISA. www.enisa.europa.eu 19. International Information System Security Certification Consortium (ISC)^2. https://www.isc2.org
Обсяг курсу	Всього 120 годин. З них 32 години лекцій, 32 годин лабораторних занять та 56 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 оцінювання ризиків інформаційної безпеки; - етапи загального процесу оцінювання ризиків інформаційної безпеки; - основи стохастичного моделювання ризику, економічні показники ризику та методи їх розрахунку; - основні принципів забезпечення неперервності бізнесу на основі ризик-орієнтованого підходу Підготовлений фахівець повинен **вміти**: - ідентифікувати ризики, вимірювати величину ризиків та встановлювати їх значущість, оцінювати залишковий ризик; - оцінювати економічний ризик та ефективність інвестицій у системи захисту інформації засобами електронних таблиць; - вміти планувати аварійне відновлення інформаційних систем. **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, консервативні системи захисту, ефективність інвестицій, умовно збережені кошти, планування відновлення.
Формат курсу	Очний. Проведення лекцій, лабораторних занять і консультацій.
Теми	**1. Оцінювання ризиків інформаційної безпеки** [1-5, 9, 10] Поняття ризику. Ймовірнісний та економічний аспекти ризику. Ризики інформаційної безпеки. Міжнародні стандарти оцінювання ризиків ІБ. Загальний процес управління ризиками ІБ. Основні етапи оцінки ризиків: ідентифікація, вимірювання, оцінювання. Ідентифікація ризиків інформаційної безпеки: ідентифікація активів, загроз, існуючих засобів захисту, вразливостей, наслідків. Вимірювання ризиків інформаційної безпеки: оцінка наслідків, вимірювання ймовірностей, визначення величини ризику.

	Встановлення значущості ризиків. Методи обробки ризиків. Прийняття ризиків, залишковий ризик. **2. Економічний ризик для систем захисту** [6, 9, 10] Показники фінансової ефективності інвестицій. Економічна ефективність систем захисту. Стохастичне моделювання економічного ризику. Когерентні міри ризику. Показник ризику на основі нерівності Кантеллі. Міра ризику Value at Risk та її розрахунок. Структурно-логічний опис консервативних систем захисту: об'єкти захисту, канали для атак, засоби захисту. Дискретна ймовірнісна модель втрат. Оцінка економічного ризику та ефективності систем захисту. Інтервальна арифметика. Інтервальна оцінка ризику для консервативних систем захисту. Інтервальний аналіз найпростіших моделей визначення величини ризику **3. Планування відновлення інформаційних систем** [7,8,11-13] Неперервністю бізнесу та інформаційна безпека. Планування відновлення після аварій. Стандарти та кращі практики з управління неперервністю бізнесу та відновлення. Планування аварійного резервування та відновлення даних. Планування аварійного відновлення мережевих сервісів. Сценарії аварійного відновлення для хмарних сервісів.
Підсумковий контроль, форма	Залік
Пререквізити	Для вивчення курсу студенти потребують базових знань з: - Основи математичного аналізу та застосування; - Застосування теорії ймовірності у кібербезпеці; - Програмування; - Прикладна статистика; - Основи кібербезпеки; - Менеджмент 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; • контрольний тест: по 20% семестрової оцінки; кількість балів – 20; • заліковий тест: 20% семестрової оцінки; максимальна кількість балів –

	20; • додаткові бали за активну участь у лекціях і лабораторних роботах 10% семестрової оцінки; максимальна кількість балів – 10. 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.
Питання до заліку	Залік – за результатами поточного контролю протягом семестру і заліковий тест. Питання відповідають темам курсу.
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.

Схема курсу "Оцінка ризиків в кібербезпеці "

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. Ризики інформаційної безпеки. Міжнародні стандарти оцінювання ризиків ІБ.	2	Фінансові ренти та їх застосування. Показники фінансової ефективності інвестицій. Економічна ефективність систем захисту.	2	4

2	Загальний процес управління ризиками ІБ. Основні етапи оцінки ризиків: ідентифікація, вимірювання, оцінювання.	2	Фінансові розрахунки засобами електронних таблиць. Пояснення ЛР №1 "Оцінка ефективності інвестиційних проектів".	2	4
3	Ідентифікація ризиків інформаційної безпеки: ідентифікація активів, загроз, існуючих засобів захисту, вразливостей, наслідків.	2	Консультації з ЛР №1. Здача ЛР №1.	2	4
4	Вимірювання ризиків інформаційної безпеки: оцінка наслідків, вимірювання ймовірностей, визначення величини ризику.	2	Консультації з ЛР №1. Здача ЛР №1.	2	4
5	Встановлення значущості ризиків. Методи обробки ризиків. Прийняття ризиків, залишковий ризик.	2	Якісні та кількісні моделі визначення величини ризику	2	3
6	Стохастичне моделювання економічного ризику. Когерентні міри ризику. Показник ризику на основі нерівності Кантеллі.	2	Найпростіші ймовірнісні задачі про ураження об’єкта захисту.	2	4
7	Міра ризику Value at Risk та її розрахунок	2	Тест 1.	2	4
8	Структурно-логічний опис консервативних систем захисту: об’єкти захисту, канали для атак, засоби захисту.	2	Розрахунок показників ризику.	2	4
9	Дискретна ймовірнісна модель втрат. Оцінка економічного ризику та ефективності систем захисту.	2	Пояснення ЛР №2 "Оцінка економічної ефективності та ризику для консервативних систем захисту"	2	4
10	Інтервальна арифметика. Інтервальна оцінка ризику для консервативних систем захисту.	2	Консультації з ЛР №2	2	3
11	Інтервальний аналіз найпростіших моделей визначення величини ризику	2	Здача ЛР №2	2	4

12	Неперервністю бізнесу та інформаційна безпека Планування відновлення після аварій.	2	Аналіз стандартів ISO 22301, ISO 22316	2	3
13	Стандарти та кращі практики з управління неперервністю бізнесу та відновлення	2	Настанова "NIST Special Publication 800-84. Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities"	2	3
14	Планування аварійного резервування та відновлення даних	2	Рекомендації "RedLegg Tabletop Exercise. The Complete Guide To Validating Your Incident Response Plan Source"	2	3
15	Планування аварійного відновлення мережевих сервісів.	2	Положення НБУ про неперервність бізнесу та відновлення.	2	3
16	Сценарії аварійного відновлення для хмарних сервісів.	2	Залік	2	2
Всього		***32***		***32***	***56***