МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Кафедра кібербезпеки та програмного забезпечення

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Теорія ризиків

першого рівня вищої освіти

КРОПИВНИЦЬКИЙ

1. Загальна інформація

Назва дисципліни	**Теорія ризиків**
Розробники	**– Коваленко Анна Степанівна**, кандидат технічних наук, доцент кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету – **Lead .Net Engineer Україна м. Львів «Vodworks» Голубець Р.О.**
Викладач	Лектор – **Коваленко Анна Степанівна**, кандидат технічних наук, доцент, https://scholar.google.com.ua/citations?user=jEfDXi0AAAAJ&hl=ru https://www.scopus.com/authid/detail.uri?authorId=57219410986
Контактний телефон	службовий: (0522)390-449 – робочі дні з 8^{30} до 14^{20}
E-mail:	annasun911@gmail.com
Консультації	*очні* – відповідно до затвердженого графіку консультацій; *онлайн* – е-листування, у месенджері (Telegram), вебінари на платформах Zoom, Discord

2. Анотація дисципліни

Навчальний курс «Теорія ризиків» призначений для набуття теоретичних знань та практичних навичок роботи з основами ризик-менеджменту, оволодіння практикою застосування методів кількісної оцінки ризику в сфері інформаційної безпеки та прийняття ефективних управлінських рішень в ситуаціях невизначеності та ризику.

3. Мета і завдання дисципліни

Метою викладання навчальної дисципліни «Теорія ризиків» є забезпечення здобувачів вищої освіти комплексом знань, умінь та навичок, необхідних для застосування в професійній діяльності у сфері ризик-менеджменту.

Завданням вивчення дисципліни є формування компетентностей:

– Вміння виявляти, ставити та вирішувати проблеми.

– Здатність проектувати системи та їхні компоненти з урахуванням усіх аспектів їх життєвого циклу та поставленої задачі, включаючи створення, налаштування, експлуатацію, технічне обслуговування та утилізацію.

– Здатність аргументувати вибір методів розв’язування спеціалізованих задач, критично оцінювати отримані результати, обґрунтовувати та захищати прийняті рішення.

4. Формат дисципліни

Для денної форми навчання:

Викладання курсу передбачає для засвоєння дисципліни традиційні лекційні заняття із застосуванням мультимедійних презентацій, у поєднанні з лабораторними заняттями.

Формат очний (*Face to face*)

Для заочної форми навчання:

Під час сесії формат очний (*Face to face*), у міжсесійний період – дистанційний (*online*).

5. Результати навчання

У результаті вивчення навчальної дисципліни студент буде:

Знати:

– Мати знання основ економіки та управління

Вміти:

– Вміти оцінювати отримані результати та аргументовано захищати прийняті рішення.

Набувати навичок автономії і відповідальності:

– Здатність адаптуватись до нових ситуацій, обґрунтовувати, приймати та реалізовувати у межах компетенції рішення.

6. Обсяг дисципліни

Ознака дисципліни, вид заняття	Кількість годин
Кількість кредитів / годин	4/120
Кількість змістових модулів	2
Нормативна / вибіркова	вибіркова
Вид підсумкового контролю :	залік

7. Технічне і програмне забезпечення / обладнання

Лекційні заняття проводяться в аудиторіях обладнаних мультимедійним проектором. Лабораторні роботи виконуються у аудиторіях кафедри кібербезпеки та програмного забезпечення, обладнаних відповідним апаратним та програмним забезпеченням (ауд. 501, 507, 508, 517), з відкритою бездротовою мережею Wi-Fi, вільним доступом до Інтернету. Оскільки при вивченні дисципліни використовуються інформаційні технології навчання, система дистанційної освіти Moodle, студенту необхідно мати комп'ютерну техніку (з виходом у Internet) та оргтехніку для комунікації з викладачами, виконання тестових завдань в системі дистанційної освіти. Застосовується матеріально-технічна база кафедри кібербезпеки та програмного забезпечення.

8. Політика дисципліни

Організація освітнього процесу. Учасники освітнього процесу повинні дотримуватися вимог Положення про організацію освітнього процесу ЦНТУ, Кодексу академічної доброчесності ЦНТУ, Положення про дотримання академічної доброчесності НПП та здобувачами вищої освіти, інших нормативних актів університету http://www.kntu.kr.ua/?view=univer&id=4.

Академічна доброчесність:

Очікується, що студенти будуть дотримуватися принципів академічної доброчесності, усвідомлювати наслідки її порушення. Детальніше за посиланням URL : http://www.kntu.kr.ua/doc/dobro.pdf

Відвідування занять

Є важливою складовою навчання. Очікується, що всі студенти відвідають лекції і лабораторні заняття курсу.

Пропущені заняття повинні бути відпрацьовані не пізніше, ніж за тиждень до залікової сесії.

Поведінка на заняттях

Недопустимість: запізнень на заняття, списування та плагіат, несвоєчасне виконання поставленого завдання.

При організації освітнього процесу в Центральноукраїнському національному технічному університеті студенти, викладачі та адміністрація діють відповідно до:

– Положення про організацію освітнього процесу;
– Положення про організацію вивчення навчальних дисциплін вільного вибору;
– Положення про рубіжний контроль успішності і сесійну атестацію студентів ЦНТУ;
– Кодексу академічної доброчесності ЦНТУ.

9. Навчально-методична карта дисципліни

Лекція 1. Сутність поняття "ризик".
Основні компоненти ризику. Інформаційна складова ризику

Лекція 2. Поняття інформаційного ризику.
Вплив інформаційних ризиків на процес функціонування підприємства. Мінімізація IT ризиків.

Лекція 3. Основні методи кількісної оцінки ризиків.
Виправданий ризик. Переваги та недоліки основних методів кількісної оцінки ризиків. Статистичні методи.

Лекція 4. Методи кількісної оцінки ризиків інвестиційних проектів.
Аналіз чутливості. Критерії обґрунтування рішень при виборі інвестиційного проекту. Метод сценаріїв. «Дерево» рішень. Метод коригування норми дисконту.

Лекція 5. Моделювання у сфері управління ризиками інформаційної безпеки.
ISO/IEC 27005. Процесна модель. Методика Facilitated Risk Analysis Process. Методика OCTAVE. Методика RiskWatch.

Лекція 6. Сучасні моделі ідентифікації, оцінки та обробки ризиків інформаційної безпеки. Гіперграфи та мережі Петрі.
Модель оцінки ризиків інформаційної безпеки. Модель обробки ризиків інформаційної безпеки. Модель виявлення уразливостей в процесі експлуатації системи. Інкрементна модель побудови системи забезпечення інформаційної безпеки.

Лекція 7. Система управління ризиками ІТ-проектів.

Управління ризиками проектної діяльності. Елементи управління в проблемних ситуаціях. Системи підтримки прийняття рішень. Моделювання ситуацій.

Лекція 8. Інструментальні засоби та практики моніторингу ризиків інформаційної безпеки.

Безперервне вдосконалення та аудит ефективності контролів. KRI та KPI для ризик-менеджменту, побудова ризикових дашбордів і реєстру ризиків, автоматизація збору подій (SIEM/SOAR), контроль відповідності (ISO/IEC 27001), регулярний перегляд ризик-апетиту, тестування планів реагування на інциденти та підготовка управлінської звітності для прийняття рішень.

Лабораторна робота 1. Сутність та основні поняття теорії ризиків. Визначення ризику, невизначеності та ймовірності; класифікація ризиків, базові метрики та інтерпретація ризикових подій у прикладних задачах.

Лабораторна робота 2. Методологічні засади та інструментарій кількісної оцінки ризику. Формування моделі ризику, вибір показників і шкал оцінювання, побудова матриці ризиків та застосування базових кількісних методів для порівняння альтернатив.

Лабораторна робота 3. Прийняття рішень в умовах ризику. Застосування критеріїв вибору (очікувана корисність, мінімакс, Байєсівські підходи), оцінка компромісів між виграшем і ризиком та обґрунтування управлінського рішення.

Лабораторна робота 4. Статистичний метод кількісної оцінки ризиків. Збір і підготовка статистичних даних, оцінювання параметрів розподілів, розрахунок імовірностей настання подій, дисперсійних показників та статистичне обґрунтування рівня ризику.

Лабораторна робота 5. Експертні методи оцінювання ризиків. Організація експертного опитування, узгодження думок та формування інтегральної оцінки ризику.

Лабораторна робота 6. Аналіз чутливості та сценарний підхід. Побудова альтернативних сценаріїв, оцінка впливу факторів і визначення критичних параметрів ризику.

Лабораторна робота 7. Імітаційне моделювання ризиків (Monte Carlo). Формування розподілів вхідних параметрів, моделювання результатів та інтерпретація ймовірнісних характеристик.

Лабораторна робота 8. Управління ризиками та план реагування. Розроблення стратегії зниження ризиків, вибір заходів контролю, моніторинг та оцінка ефективності управлінських рішень.

10. Система оцінювання та вимоги

Види контролю: поточний, підсумковий.
Методи контролю: спостереження за навчальною діяльністю, усне опитування, письмовий контроль, тестовий контроль.
Форма підсумкового контролю: залік.

Контроль знань і умінь здобувачів (поточний і підсумковий) здійснюється згідно з кредитною трансферно-накопичувальною системою організації освітнього процесу в ЦНТУ. Рейтинг студента із засвоєння дисципліни визначається за 100-бальною шкалою. Він складається із рейтингу з поточної навчальної роботи впродовж семестру, для оцінювання якої призначається 100 балів (по 50 балів за кожен змістовний модуль).

Критерії оцінювання. Еквівалент оцінки в балах для кожної окремої теми може бути різний, загальну суму балів за тему визначено в навчально-методичній карті. Розподіл балів між видами занять (лекції, лабораторні заняття, самостійна робота) можливий шляхом спільного прийняття рішення викладача і студентів на першому занятті.

При виставленні оцінки враховуються результати навчальної роботи студента протягом семестру

Критерії оцінки заліку:

– «зараховано» – студент має стійкі знання про основні поняття дисципліни, може сформулювати взаємозв'язки між поняттями.

– «незараховано» – студент має значні пропуски в знаннях, не може сформулювати взаємозв'язку між поняттями, що вивчаються в курсі, не має уявлення про більшість основних понять дисципліни, що вивчається.

11. Рекомендована література й джерела

Базова

1. A.S. Kovalenko, O.V. Kovalenko, O.A. Smirnov, Jamil Al-Azzeh, S.A. Smirnov Qualitative risk analysis of software development. Asian Journal of Information Technology. – Volume 17(3). – Medwell Journals. DOI: ajit.2018.218.230. – 2018. – P. 218-230. Режим доступу: http://medwelljournals.com/abstract/?doi=ajit.2018.218.230 (**Закордонне фахове видання**)
2. Коваленко А.С., Смірнова Т.В., Буравченко К.О., Щербань А.В., Багдасарян Е.К., «Проектування та оптимізація структурованих кабельних систем для автоматизації виробничих процесів підприємства» Сучасні інформаційні системи. 2022. Т. 6, № 1. С. 129-133. Режим доступу: http://ais.khpi.edu.ua/article/view/254256/251522 **(Фахове видання. Категорія «Б»)**
3. Коваленко А.С., Смірнова Т.В., Янков М.О., Грудік В.В., Горбов В.О. «Планування радіопокриття та моделювання поширення радіосигналів мобільних мереж 5G для автоматизації виробничих процесів». Електронне моделювання, № 3, т. 44. С. 113-122. 2022. Режим доступу: https://www.emodel.org.ua/uk/archive-ukr/2022/44-3-u/c-113-122 **(Фахове видання. Категорія «Б»)**
4. Kovalenko A., Khudov H., Symkanych O., Kabus N., Lysytsya V., Khudov R. “The comparative assessment of the quality of cytological drugs image processing”. International Journal of Advanced Trends in Computer Science and Engineering, 2020, 9(5), стр. 8645–8653. Режим доступу:https://www.researchgate.net/publication/344924358_The_Comparative_Assessment_of_the_Quality_of_Cytological_Drugs_Image_Processing (**Закордонне фахове видання**)
5. Коваленко А.С., Гнатюк С.О., Кавун С.В., Терейковський І.А., Жмурко Т.О., Смірнов О.А., Смірнов С.А., Основи безпеки в комп’ютерних мережах, **Навчальний посібник** – Кропивницький: вид. Лисенко В.Ф. 2018. – 177 с.

Допоміжна

6. International standard BS ISO/IEC 27005:2008, 2008-06-15.
7. Ronald A. Beghetto Beautiful Risks: Having the Courage to Teach and Learn Creatively. Rowman & Littlefield Publishers. 2018. 128 c.
8. Marvin Rausand, Stein Haugen Risk Assessment: Theory, Methods, and Applications (Statistics in Practice). Wiley. 2020. 784 c.
9. Georg Hodosi, Lazar Rusu Risks, Relationships and Success Factors in IT Outsourcing: A Study in Large Companies (SpringerBriefs in Information Systems). Springer. 2019. 71 c.
10. Daemon Behr IT Architect Series: Designing Risk in IT Infrastructure. 2018. 474 c.

11. Carl S. Young Risk and the Theory of Security Risk Assessment (Advanced Sciences and Technologies for Security Applications). Springer. 2020. 302 с.
12. Portfolio Theory and Risk Management. Cambridge University Press. 2014. 169 с.
13. Griselda Deelstra, Guillaume Plantin Risk Theory and Reinsurance (EAA Series). Springer. 2013. 86 с.
14. Maciej J. Capiński, Ekkehard Kopp Hanspeter Schmidli Risk Theory (Springer Actuarial). Springer. 2018. 254 с.
15. Gary Stoneburner. Risk Management Guide for Information Technology Systems / Stoneburner G., Goguen1 A., Feringa1 A. - Gaithersburg: National Institute of Standards and Technology, 2002. - 55 p.
16. Юдін О.І., Корченко О.Г., Конахович Г.Ф., Захист інформації в мережах передачі даних – К.: Вид-во ТОВ "НВП"Інтерсервіс", 2009.– 716 с.
17. Martina Raue, Eva Lermer, Bernhard Streicher Psychological Perspectives on Risk and Risk Analysis: Theory, Models, and Applications. Springer. 2018. 402 с.
18. J. Stephen Wormith, Leam A. Craig, Todd E. Hogue The Wiley Handbook of What Works in Violence Risk Management: Theory, Research, and Practice. Wiley-Blackwell. 2020. 608 с.
19. Harry Markowitz, Kenneth Blay Risk-Return Analysis: The Theory and Practice of Rational Investing. McGraw Hill. 2013. 272 с.
20. Kimmo Soramaki, Samantha Cook Network Theory and Financial Risk. Risk Books. 2016. 228.

Методичне забезпечення

21. Коваленко А.С., Коваленко О.В., Оришака О.В. «Теорія ризиків». Методичні вказівки до виконання лабораторних робіт для студентів денної форми навчання галузі 12 Інформаційні технології. – Кропивницький: ЦНТУ – 2022. – 59 с.
22. Коваленко А.С., Коваленко О.В., Оришака О.В. «Теорія ризиків». Методичні вказівки до виконання контрольних робіт для студентів заочної форми навчання галузі 12 Інформаційні технології. – Кропивницький: ЦНТУ – 2022. – 59 с.

Інформаційні ресурси

23. Онлайн-курси UDEMY. – URL: https://www.udemy.com/ –платформа онлайн-курсів різних ІТ тематик.
24. Онлайн-курси Prometheus. – URL: https://prometheus.org.ua/ – українська платформа безкоштовних онлайн-курсів
25. Онлайн-курси Coursera. – URL: https://www.coursera.org –платформа онлайн-курсів різних ІТ тематик.
26. https://habr.com – колективний блог з новинами та аналітичними статтями про інформаційні технології та програмування.
27. http://stackoverflow.com/ – система питань і відповідей для професійних програмістів та новачків у програмуванні.
28. https://dou.ua/ – український веб-сайт з елементами колективного блогу, створений для розповсюдження новин, аналітичних статей та свіжої інформації пов'язаної із інформаційними технологіями.
29. https://www.google.com/ – основна пошукова платформа.
30. https://www.youtube.com – Відеохостинг, що надає користувачам послуги зберігання, доставки та показу відео. На платформі розміщено багато курсів ІТ спрямованості.
31. https://biblprog.org.ua/ua/programming/ – каталог безкоштовних середовищ розроблення ПЗ.