МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Кафедра кібербезпеки та програмного забезпечення

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Теорія ризиків

Освітньо-професійна програма «Кібербезпека»

першого рівня вищої освіти

за спеціальністю 125 Кібербезпека

галузі знань 12 Інформаційні технології

кваліфікація Бакалавр з кібербезпеки

Розглянуто на засіданні кафедри
Протокол №13 від 31 березня 2022 р.

КРОПИВНИЦЬКИЙ – 2022

ЗМІСТ

1. Загальна інформація

Назва дисципліни	**Теорія ризиків**
Рік викладання	2022-2023 календарний рік
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. (**https://jobs.dou.ua/companies/vodworks/)
Викладач	Лектор – **Коваленко Анна Степанівна**, кандидат технічних наук, доцент, http://kbpz.kntu.kr.ua/kovalenko-anna/ https://scholar.google.com.ua/citations?user=jEfDXi0AAAAJ&hl=ru https://www.scopus.com/authid/detail.uri?authorId=57219410986 Асистент – **Оришака Олег Володимирович**, доцент, http://kbpz.kntu.kr.ua/orishaka-oleg/ https://scholar.google.com/citations?user=genCf08AAAAJ&hl=ru https://orcid.org/0000-0002-2712-106X
Контактний телефон	службовий: (0522)390-449 – робочі дні з 8^{30} до 14^{20} Мобільні телефони / Viber / Telegram надано у описі курсу «Теорія ризиків» на сервері дистанційної освіти ЦНТУ. –URL: http://moodle.kntu.kr.ua/course/view.php?id=668
E-mail:	У описі курсу «Теорія ризиків» на сервері дистанційної освіти ЦНТУ. – URL: http://moodle.kntu.kr.ua/course/view.php?id=668
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 моніторингу процесів функціонування інформаційно-телекомунікаційних систем з основами ризик-менеджменту, оволодіння практикою застосування методів кількісної оцінки ризику, аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору в сфері інформаційної безпеки та прийняття ефективних управлінських рішень в ситуаціях невизначеності.

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.

Основними **завданнями** вивчення навчальної дисципліни є формування наступних компетенцій бакалавра з кібербезпеки:

– КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

– КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

– КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

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 забезпечити наступні програмні результати:

– забезпечувати процеси моніторингу доступу до ресурсів і процесів інформаційно□телекомунікаційних систем;

– забезпечувати конфігурування та функціонування систем моніторингу ресурсів та процесів в інформаційно телекомунікаційних системах;

– виконувати впровадження та підтримку систем виявлення вторгнень та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних, інформаційно□телекомунікаційних (автоматизованих) системах;

– аналізувати ефективність систем виявлення та протидії несанкціонованому доступу до ресурсів і процесів в інформаційно□телекомунікаційних системах;

– аналізувати та впроваджувати системи захисту від зловмисних програмних кодів.

6. Обсяг дисципліни

Ознака дисципліни, вид заняття	**Кількість годин**
Рекомендації щодо семестру вивчення	6 семестр
Спеціальність	125 «Кібербезпека»
Кількість кредитів / годин	3/90
Кількість змістових модулів	2
Нормативна / вибіркова	вибіркова
лекції	14
лабораторні	14
самостійна робота	32
Вид підсумкового контролю :	екзамен

7. Пререквізити

Враховуючи послідовність накопичення знань і набуття вмінь, для опанування навчальної дисципліни необхідні знання й вміння, здобуті під час вивчення навчальних дисциплін «Вища математика», «Базові методології та технології програмування», «Алгоритми та методи обчислень».

8. 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.

9. Політика дисципліни

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.

10. Навчально-методична карта дисципліни

Тиждень, дата, академічні години	**Тема, основні питання** *(розкривають зміст і є орієнтирами для підготовки до модульного і підсумкового контролю)*	**Форма діяльності (заняття) /формат**	**Матеріали**	**Література, інформаційні ресурси**	**Завдання, години**	**Вага оцінки**	**Термін виконання**
Змістовний модуль 1. Основні компоненти ризику							
Тиж.1 (за розкладом) (2 год.)	**Тема лекції 1. Сутність поняття "ризик".** Основні компоненти ризику. Інформаційна складова ризику	Лекція / *Face to face*	Презентація	1-5, 13-17, 23	Самостійно опрацювати теоретичний матеріал теми 1. (2 год.)	5 балів	Самостійна робота до 2 тижня включно
Тиж.2 (за розкладом) (2 год.)	**ЛР 1. Сутність та основні поняття теорії ризиків.**	Лабораторна робота / *Face to face*	Методичні рекомендації	6-14, 18-22, 23-32	Самостійно опрацювати теоретико-практичні питання до виконання лабораторної роботи 1. (2 год.)	5 балів	Самостійна робота до 3 тижня включно
Тиж.3 (за розкладом) (2 год.)	**Тема лекції 2. Поняття інформаційного ризику.** Вплив інформаційних ризиків на процес функціонування підприємства. Мінімізація ІТ ризиків.	Лекція / *Face to face*	Презентація	1-5, 13-17, 23	Самостійно опрацювати теоретичний матеріал теми 2. (2 год.)	5 балів	Самостійна робота до 4 тижня включно
Тиж.4 (за розкладом) (2 год.)	**ЛР 2. Методологічні засади та інструментарій кількісної оцінки ризику. Часина 1.**	Лабораторна робота / *Face to face*	Методичні рекомендації	6-14, 18-22, 23-32	Самостійно опрацювати теоретико-практичні питання до виконання лабораторної роботи 2. (2 год.)	5 балів	Самостійна робота до 5 тижня включно

Тиж.5 (за розкладом) (2 год.)	**Тема лекції 3. Основні методи кількісної оцінки ризиків.** Виправданий ризик. Переваги та недоліки основних методів кількісної оцінки ризиків. Статистичні методи.	Лекція / *Face to face*	Презентація	1-5, 13-17, 23	Самостійно опрацювати теоретичний матеріал теми 3. (2 год.)	5 балів	Самостійна робота до 6 тижня включно
Тиж.6 (за розкладом) (2 год.)	**ЛР 2. Методологічні засади та інструментарій кількісної оцінки ризику. Часина 2.**	Лабораторна робота / *Face to face*	Методичні рекомендації	6-14, 18-22, 23-32	Самостійно опрацювати теоретико-практичні питання до виконання лабораторної роботи 2. (2 год.)	5 балів	Самостійна робота до 7 тижня включно
Максимальна кількість балів за змістовим модулем 1						30 балів	
Змістовний модуль 2. Оцінки ризиків							
Тиж.7 (за розкладом) (2 год.)	**Тема лекції 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 / *Face to face*	Презентація	1-5, 13-17, 23	Самостійно опрацювати теоретичний матеріал теми 4. (2 год.)	3 бал	Самостійна робота до 8 тижня включно
Тиж.8 (за розкладом) (2 год.)	**ЛР 3. Прийняття рішень в умовах ризику. Часина 1.**	Лабораторна робота / *Face to face*	Методичні рекомендації	6-14, 18-22, 23-32	Самостійно опрацювати теоретико-практичні питання до виконання лабораторної роботи 3. (2 год.)	4 балів	Самостійна робота до 9 тижня включно

Тиж.9 (за розкладом) (2 год.)	**Тема лекції 5** Моделювання у сфері управління ризиками інформаційної безпеки. ISO/IEC 27005. Процесна модель. Методика Facilitated Risk Analysis Process. Методика OCTAVE. Методика RiskWatch.	Лекція / *Face to face*	Презентація	1-5, 13-17, 23	Самостійно опрацювати теоретичний матеріал теми 5. (2 год.)	3 бал	Самостійна робота до 10 тижня включно
Тиж.10 (за розкладом) (2 год.)	**ЛР 3. Прийняття рішень в умовах ризику. Часина 2.**	Лабораторна робота / *Face to face*	Методичні рекомендації	6-14, 18-22, 23-32	Самостійно опрацювати теоретико-практичні питання до виконання лабораторної роботи 3. (2 год.)	4 балів	Самостійна робота до 11 тижня включно
Тиж.11 (за розкладом) (2 год.)	**Тема лекції 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 / *Face to face*	Презентація	1-5, 13-17, 23	Самостійно опрацювати теоретичний матеріал теми 6. (2 год.)	3 бал	Самостійна робота до 12 тижня включно
Тиж.12 (за розкладом) (2 год.)	**ЛР 4. Статистичний метод кількісної оцінки ризиків. Часина 1.**	Лабораторна робота / *Face to face*	Методичні рекомендації	6-14, 18-22, 23-32	Самостійно опрацювати теоретико-практичні питання до виконання лабораторної роботи 4. (4 год.)	5 балів	Самостійна робота до 13 тижня включно

Тиж.13 (за розкладом) (2 год.)	**Тема лекції 7. Система управління ризиками ІТ-проектів** Управління ризиками проектної діяльності. Елементи управління в проблемних ситуаціях. Системи підтримки прийняття рішень. Моделювання ситуацій.	Лекція / *Face to face*	Презентація	1-5, 13-17, 23	Самостійно опрацювати теоретичний матеріал теми 7. (2 год.)	3 бал	Самостійна робота до 14 тижня включно
Тиж.14 (за розкладом) (2 год.)	**ЛР 4. Статистичний метод кількісної оцінки ризиків. Часина 2.**	Лабораторна робота / *Face to face*	Методичні рекомендації	6-14, 18-22, 23-32	Самостійно опрацювати теоретико-практичні питання до виконання лабораторної роботи 4. (4 год.)	5 бали	Самостійна робота до 14 тижня включно
Максимальна кількість балів за змістовим модулем 2						30 балів	
Максимальна кількість балів за екзамен						40 балів	

11. Система оцінювання та вимоги

Види контролю: поточний, підсумковий.

Методи контролю: спостереження за навчальною діяльністю, усне опитування, письмовий контроль, тестовий контроль.

Форма підсумкового контролю: екзамен.

Контроль знань і умінь (поточний і підсумковий) з дисципліни «Теорія ризиків» здійснюється згідно з кредитною трансферно-накопичувальною системою організації навчального процесу. Рейтинг студента із засвоєння дисципліни визначається за 100-бальною шкалою. Він складається з рейтингу навчальної роботи (засвоєння теоретичного матеріалу під час аудиторних занять та самостійної роботи, виконання лабораторних завдань), для оцінювання якої призначається 60 балів, та екзамену, максимальна оцінка за який складає 40 балів.

Розподіл балів, які отримують студенти при вивченні дисципліни «Теорія ризиків»

Поточний контроль та самостійна робота															
Змістовий модуль 1						Змістовий модуль 2								Екзамен	Сума
Т1		Т2		Т3		Т4		Т5		Т6		Т7			
Л1	ЛР1	Л2	ЛР2	Л3	ЛР2	Л4	ЛР3	Л5	ЛР3	Л6	ЛР4	Л7	ЛР4		
5	5	5	5	5	5	3	4	3	4	3	5	3	5	40	100
30						30									

Примітка: Т1, Т2,…,Т7 – тема, Л – теоретичні (лекційні) заняття, ЛР – лабораторні заняття

Шкала оцінювання: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою
		залік
90-100	A	зараховано
82-89	B	
74-81	C	
64-73	D	
60-63	E	
35-59	FX	не зараховано з можливістю повторного складання
1-34	F	не зараховано з обов'язковим повторним вивченням дисципліни

Критерії оцінювання знань і вмінь здобувачів визначені Положенням про організацію освітнього процесу в ЦНТУ (*стор. 32-33*).

12. 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.
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.

Допоміжна

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. Курс «Теорія ризиків» на сервері дистанційної освіта ЦНТУ. – URL: http://moodle.kntu.kr.ua/course/view.php?id=668
24. Онлайн-курси UDEMY. – URL: https://www.udemy.com/ –платформа онлайн-курсів різних ІТ тематик.
25. Онлайн-курси Prometheus. – URL: https://prometheus.org.ua/ – українська платформа безкоштовних онлайн-курсів
26. Онлайн-курси Coursera. – URL: https://www.coursera.org –платформа онлайн-курсів різних ІТ тематик.
27. https://habr.com – колективний блог з новинами та аналітичними статтями про інформаційні технології та програмування.
28. http://stackoverflow.com/ – система питань і відповідей для професійних програмістів та новачків у програмуванні.
29. https://dou.ua/ – український веб-сайт з елементами колективного блогу, створений для розповсюдження новин, аналітичних статей та свіжої інформації пов'язаної із інформаційними технологіями.
30. https://www.google.com/ – основна пошукова платформа.
31. https://www.youtube.com – Відеохостинг, що надає користувачам послуги зберігання, доставки та показу відео. На платформі розміщено багато курсів ІТ спрямованості.
32. https://biblprog.org.ua/ua/programming/ – каталог безкоштовних середовищ розроблення ПЗ.