

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ТЕОРІЯ РИЗИКІВ»

Лектор курсу		Тищенко Віталій Сергійович, старший викладач кафедри “Управління інформаційною та кібернетичною безпекою”		Контактна інформація лектора (e-mail), сторінка курсу в Moodle		e-mail: tvs5vetal@gmail.com сторінка курсу в Classroom – https://classroom.google.com/c/Njg1MjYzNTYxMDQ4?cjc	
Галузь знань		12 «Інформаційні технології»		Рівень вищої освіти		бакалавр	
Спеціальність		125 Кібербезпека		Семестр		3	
Освітня програма		Кібербезпека		Тип дисципліни		Загальної підготовки	
Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	3	90	18	-	18	-	54

АНОТАЦІЯ КУРСУ

Взаємозв’язок у структурно-логічній схемі

Мета курсу: формування у студентів необхідної системи знань у сфері аналізу категорії інформаційного ризику на підґрунті використання фінансового аналізу, якісних підходів, економіко-математичних методів і моделей.

Компетентності відповідно до освітньої програми

Soft- skills / Загальні компетентності (ЗК)

ЗК 2. Знання та розуміння предметної області та розуміння професії.
ЗК 5. Здатність до пошуку, оброблення та аналізу інформації.

Hard-skills / Спеціальні компетентності (СК)

СК 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

Програмні результати навчання (ПР)

ПР 4. Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

ПР 12. Розробляти моделі загроз та порушника.

ПР 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

ПР 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

ОРГАНІЗАЦІЯ НАВЧАННЯ

Тема, опис теми	Вид заняття	Оцінювання за тему	Форми і методи навчання/питання до самостійної роботи
Розділ 1. Теоретичні основи управління ризиками.			
Тема 1. Загальні відомості щодо ризиків та управління ризиками			
Рекомендовані джерела: 1,3,5,6,9,11			

Заняття 1.1 Базові поняття ризиків.	Лекція 1 2 год		Пояснювально-ілюстративний, лекція-візуалізація
Заняття 1.2 Базові поняття ризику в інформаційній безпеці	Практичне заняття 1 2 год	5 балів	Тестування, навчальна дискусія, обговорення ситуаційного завдання
Заняття 1.3. Базові поняття управління ризиками.	Лекція 2 2 год		Пояснювально-ілюстративний, лекція-візуалізація
Заняття 1.4 Базові поняття ризик-менеджменту	Практичне заняття 2 2 год	5 балів	Усне опитування, навчальна дискусія, обговорення ситуаційного завдання
Заняття 1.5. Прогнозування розвитку	Лекція 3 2 год		Лекція-візуалізація
Заняття 1.6 Прогнозування розвитку	Практичне заняття 3 2 год	5 балів	Усне опитування, виконання завдань на практичне застосування знань і вмінь.
Заняття 1.7 Системний підхід до управління ризиками	Лекція 4 2 год		Лекція-візуалізація
Заняття 1.8 Функціонально-вартісний аналіз	Практичне заняття 4 2 год	5 балів	Усне опитування, навчальна дискусія, обговорення ситуаційного завдання
Тема 2. Створення систем управління інформаційною безпекою відповідно до вимог стандартів в сфері ІБ <u>Рекомендовані джерела:</u> 1,2,4,7,8,10.			
Заняття 2.1 Базові показники ймовірностей	Лекція 5 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 2.2. Базові показники ймовірностей	Практичне заняття 5 2 год	5 балів	Усне опитування, виконання завдань на практичне застосування знань і вмінь, тестування
Заняття 2.3. Ймовірнісні міри ризику	Лекція 6 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування

Заняття 2.4. Ймовірнісні міри ризику	Практичне заняття 6 2 год	5 балів	Усне опитування, виконання завдань на практичне застосування знань і вмінь, тестування
Заняття 2.5 Міри корисності	Лекція 7 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 2.6 Одноетапні процедури прийняття рішень	Практичне заняття 7 2 год	5 балів	Усне опитування, виконання завдань на практичне застосування знань і вмінь, тестування
Розділ 2. Використання стандартів при перевірці і оцінці систем управління інформаційної безпеки..			
Тема 3. Кількісний аналіз ризиків Рекомендовані джерела: 1,2,3,5,6,8,9.			
Заняття 3.1. Методології управління ризиками	Лекція 8 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 3.2. Норма доходу	Практичне заняття 8 2 год	5 балів	Усне опитування, виконання завдань на практичне застосування знань і вмінь.
Заняття 3.3. Планування, ідентифікація, якісний аналіз	Лекція 9 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 3.4. Кількісний аналіз, реагування, моніторинг та управління ризиками. Робота з SimpleRisk	Практичне заняття 9 2 год	5 балів	Усне опитування, виконання завдань на практичне застосування знань і вмінь.
Тема 1. Загальні відомості щодо ризиків та управління ризиками Тема 2. Ймовірнісні міри ризику Тема 3. Кількісний аналіз ризиків	Самостійна робота		
	4 год	1 бал	1. Порівняльна характеристика ризиків вірусних атак
	4 год	1 бал	2. Порівняльна характеристика засобів антивірусного захисту
	4 год	1 бал	3. Засоби захисту від мережевих атак
	4 год	1 бал	4. Класифікація комп'ютерних немережевих атак
	4 год	1 бал	5. Засоби захисту від комп'ютерних немережевих атак
	4 год	1 бал	6. Класифікація загроз інформаційної безпеці державного підприємства
2 год	1 бал	7. Класифікація загроз інформаційної безпеці приватного	

			підприємства
4 год	1 бал		8. Взаємодія служби інформаційної безпеки з іншими безпековими службами
4 год	1 бал		9. Тенденції розвитку мережевих атак
4 год	1 бал		10. Тенденції розвитку вірусних атак
4 год	1 бал		11. Тенденції розвитку інформаційних атак в державному секторі
2 год	1 бал		12. Тенденції розвитку інформаційних атак в приватному секторі
4 год	1 бал		13. Тенденції розвитку засобів інформаційної протидії
2 год	1 бал		14. Статистичні оцінки ефективності засобів інформаційної протидії
4 год	1 бал		15. Оцінка економічних втрат приватного підприємства від інформаційних атак

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

- Мультимедійний проєктор;
- Комп'ютерний клас для проведення практичних занять

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management
2. IEC 31010:2019 Risk management — Risk assessment techniques
3. ISO 31000:2018 Risk management — Guidelines. URL: https://nobelcert.com/DataFiles/FreeUpload/ISO_31000_2018.pdf
4. NIST Risk Management Framework. URL: <https://src.nist.gov/projects/risk-management/about-rmf>
5. What is Information Security Risk Management?

URL: [https://www.rapid7.com/fundamentals/information-security-](https://www.rapid7.com/fundamentals/information-security-risk-)

[management/#:~:text=Information%20security%20risk%20management%2C%20or,availability%20of%20an%20organization's%20assets.](https://www.rapid7.com/fundamentals/information-security-risk-management/#:~:text=Information%20security%20risk%20management%2C%20or,availability%20of%20an%20organization's%20assets.)

6. Alex Sidorenko, Elena Demidenko. Guide to Effective Risk Management 3.0. 2017

URL: https://www.researchgate.net/publication/323254437_FREE_RISK_MANAGEMENT_BOOK_GUIDE_TO_EFFECTIVE_RISK_MANAGEMENT_30

7. Security Risk Management: Building an Information Security Risk Management Program from the Ground Up. 2011.

URL: <https://www.everand.com/book/287529238/Security-Risk-Management-Building-an-Information-Security-Risk-Management-Program-from-the-Ground-Up>

8. Malcolm W.Harkins. Managing Risk and Information Security: Protect to Enable. 2016. URL: <https://library.oapen.org/bitstream/id/6002f5f4-dbf6-4d1a-a436-5dd908db2f0b/1002072.pdf>

9. Julian Talbot, Miles Jakeman. Security Risk Management. Body of Knowledge. 2019. URL: https://www.csr.ruma.rs/upload/6faae8f1ec8cc14577ee8975a4c8ac2f/security_risk_management_body_of_knowledge.pdf

10. Risk Identification tools and techniques. URL: <https://www.greycampus.com/opencampus/certified-associate-in-project-management/risk-identification-tools-and-techniques-in-capm>

11. Dennis Evans. Risk Mitigation Strategies. 2019. URL: https://www.researchgate.net/publication/335664777_Risk_Mitigation_Strategies

ПОЛІТИКА КУРСУ («ПРАВИЛА ГРИ»)

- Курс передбачає роботу в колективі.
- Середовище в аудиторії є дружнім, творчим, відкритим до конструктивної критики.
- Освоєння дисципліни передбачає обов'язкове відвідування лекцій і практичних занять, а також самостійну роботу.
- Самостійна робота включає в себе теоретичне вивчення питань, що стосуються тем лекційних занять, які не ввійшли в теоретичний курс, або ж були розглянуті коротко, їх поглиблена проробка за рекомендованою літературою.
- Усі завдання, передбачені програмою, мають бути виконані у встановлений термін.
- Якщо студент відсутній з поважної причини, він презентує виконані завдання під час самостійної підготовки та консультації викладача.
- Під час роботи над завданнями не допустимо порушення академічної доброчесності: при використанні Інтернет ресурсів та інших джерел інформації студент повинен вказати джерело, використане в ході виконання завдання. У разі виявлення факту плагіату студент отримує за завдання 0 балів.
- Студент, який спізнився, вважається таким, що пропустив заняття з неповажної причини з виставленням 0 балів за заняття, і при цьому має право бути присутнім на занятті.
- За використання телефонів і комп'ютерних засобів без дозволу викладача, порушення дисципліни студент видаляється з заняття, за заняття отримує 0 балів.

КРИТЕРІЙ ТА МЕТОДИ ОЦІНЮВАННЯ

Умовою допуску до підсумкового контролю є виконання всіх практичних робіт і виконання самостійних завдань, які передбачені структурою освітньої компоненти Дослідження операцій.

Якщо студента не допущено до складання заліку, як такого, що не виконав індивідуальний план, йому надається час до перескладання для виконання всіх вимог допуску. Студент має право на два перескладання. При повторному перескладанні екзамену його у студента може приймати комісія, яка створюється директором ННІТ. Оцінка комісії є остаточною. У випадку отримання студентом 0 балів (неприйнятно), що тягне відрахування за невиконання навчального плану.

Оцінювання студентів здійснюється за накопичувальною 100-бальною системою і складається із двох основних оцінкових блоків і розподіляється в певних пропорціях 60 (бали напрацьовані під час вивчення дисципліни – Поточний контроль), 40 (підсумкове оцінювання - Залік):

Форми контролю	Види навчальної роботи	Оцінювання
ПОТОЧНИЙ КОНТРОЛЬ	• Виконання практичних робіт	45 бали
	• Самостійна робота	15 балів
ПІДСУМКОВЕ ОЦІНЮВАННЯ Екзамен	Екзамен проходить у письмовій формі.	40 балів

Додаткова оцінка

Види навчальної роботи	Оцінювання
Участь у наукових конференціях, підготовка наукових публікацій за тематикою освітньої компоненти:	
- Тези доповіді на фаховій конференції	3 бали
- Стаття у фаховому виданні	5 балів
- Стаття в іноземному рецензованому виданні	10 балів

Максимальна кількість додаткових балів, які можуть бути зараховані здобувачу освіти - 10 балів.

ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ

бали	Критерії оцінювання	Рівень компетентності	Оцінка /запис в екзаменаційній відомості
90-100	Студент демонструє повні й міцні знання навчального матеріалу в обсязі, що	Високий	Відмінно / Зараховано (А)

	<p>відповідає робочій програмі дисципліни, правильно й обґрунтовано приймає необхідні рішення в різних нестандартних ситуаціях.</p> <p>Вміє реалізувати теоретичні положення дисципліни в практичних розрахунках, аналізувати та співставляти дані об'єктів діяльності фахівця на основі набутих з даної та суміжних дисциплін знань та умінь.</p> <p>Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань проявив вміння самостійно вирішувати поставлені завдання, активно включатись в дискусії, може відстоювати власну позицію в питаннях та рішеннях, що розглядаються. Зменшення 100-бальної оцінки може бути пов'язане з недостатнім розкриттям питань, що стосується дисципліни, яка вивчається, але виходить за рамки об'єму матеріалу, передбаченого робочою програмою, або студент проявляє невпевненість в тлумаченні теоретичних положень чи складних практичних завдань.</p>	<p>Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни. Власні пропозиції студента в оцінках і вирішенні практичних задач підвищує його вміння використовувати знання, які він отримав при вивченні інших дисциплін, а також знання, набуті при самостійному поглибленому вивченні питань, що відносяться до дисципліни, яка вивчається.</p>	
82-89	<p>Студент демонструє гарні знання, добре володіє матеріалом, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати теоретичні положення при вирішенні практичних задач, але допускає окремі неточності. Вміє самостійно виправляти допущені помилки, кількість яких є незначною.</p> <p>Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, дає вичерпні пояснення.</p>	<p>Достатній</p> <p>Забезпечує студенту самостійне вирішення основних практичних задач в умовах, коли вихідні дані в них змінюються порівняно з прикладами, що розглянуті при вивченні дисципліни</p>	Добре / Зараховано (B)
75-81	<p>Студент в загальному добре володіє матеріалом, знає основні положення матеріалу, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати при вирішенні типових практичних завдань, але допускає окремі неточності. Вміє пояснити основні положення виконаних завдань та дати правильні відповіді при зміні результату при заданій зміні вихідних параметрів. Помилки у відповідях/ рішеннях/ розрахунках не є системними. Знає характеристики основних положень, що мають визначальне значення при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, в межах дисципліни, що вивчається.</p>	<p>Достатній</p> <p>Конкретний рівень, за вивченим матеріалом робочої програми дисципліни.</p> <p>Додаткові питання про можливість використання теоретичних положень для практичного використання викликають утруднення.</p>	Добре / Зараховано (C)
64-74	<p>Студент засвоїв основний теоретичний матеріал, передбачений робочою програмою дисципліни, та розуміє постанову стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень. Розуміє основні положення, що є визначальними в курсі, може вирішувати подібні завдання тим, що розглядалися з викладачем, але допускає значну кількість неточностей і грубих помилок, які може усувати за допомогою викладача.</p>	<p>Середній</p> <p>Забезпечує достатньо надійний рівень відтворення основних положень дисципліни</p>	Задовільно / Зараховано (D)
60-63	<p>Студент має певні знання, передбачені в робочій програмі дисципліни, володіє основними положеннями, що вивчаються на рівні, який визначається як мінімально допустимий. З використанням основних теоретичних положень, студент з труднощами пояснює правила вирішення практичних/розрахункових завдань</p>	<p>Середній</p> <p>Є мінімально допустимим у всіх складових навчальної програми з дисципліни</p>	Задовільно / Зараховано (E)

	дисципліни. Виконання практичних / індивідуальних / контрольних завдань значно формалізовано: є відповідність алгоритму, але відсутнє глибоке розуміння роботи та взаємозв'язків з іншими дисциплінами.		
35-59	Студент може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни студент виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у студента відсутні.	Низький Не забезпечує практичної реалізації задач, що формуються при вивченні дисципліни	Незадовільно з можливістю повторного складання) / Не зараховано (FX) В залікову книжку не представляється
1-34	Студент повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Студент не допущений до здачі екзамену/заліку.	Незадовільний Студент не підготовлений до самостійного вирішення задач, які окреслює мета та завдання дисципліни	Незадовільно з обов'язковим повторним вивченням / Не допущений (F) В залікову книжку не представляється

ПОЛІТИКА ДОБРОЧЕСНОСТІ

Здобувач вищої освіти виконуючи самостійну або індивідуальну роботу повинен дотримуватись політики доброчесності. У разі наявності плагіату в будь-яких видах робіт здобувача, він отримує незадовільну оцінку і повинен повторно виконати завдання, які передбачені у Силабусі.