СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«ТЕОРІЯ РИЗИКІВ»

Національний технічний університет ДНІПРОВСЬКА ПОЛІТЕХНІКА 1899	**Ступінь освіти**	бакалавр
	Галузь знань	12 Інформаційні технології
	Тривалість викладання	9,10 чверті
	Заняття:	Осінній семестр
	лекції:	2 години
	практичні заняття:	1година
	Мова викладання	українська

Сторінка курсу в СДО НТУ «ДП»:
https://do.nmu.org.ua/enrol/index.php?id=3459

Кафедра, що викладає Безпеки інформації та телекомунікацій

Інформація про викладачів

Ткач Максим Олександрович	к.т.н., доцент
Персональна сторінка	https://bit.nmu.org.ua/ua/pro_kaf/prepods/tkach.php
E-mail:	tkach.m.ol@nmu.one

1.Анотація до курсу

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.

2. Мета та завдання курсу

Мета дисципліни – формування компетентностей щодо застосування ризик-орієнтованого підходу до управління інформаційною та кібербезпекою. Формування у здобувачів поглиблених знань, умінь і навичок в області теорії ризику як феномену відповідно до сучасних наукових уявлень, що сприятиме вирішенню широкого спектру задач в різних напружених і екстремальних ситуаціях у сфері професійної освіти.

Завдання курсу набуттям знань і вмінь щодо проведення об'єктивної оцінки рівня ризиків інформаційноїбезпеки. Насамперед, це знання та вміння, які дають змогу виявляти,враховувати, реагувати і аналізувати ризики інформаційної безпеки. Безреалізації цих процесів неможливо забезпечити рівень захищеності, адекватнийсучасним стандартам і галузевим нормам.

3. Результати навчання

Володіти основнними відомостями про принципи та методи оцінки ризиків, прийняття рішень при невизначеності.

Знати: основні характеристики ризику та їх вимірювання; числові показники(характеристики) ризику; основні методи оцінки інформаційних ризиків;найпоширеніші методики оцінки інформаційних ризиків; основні принципипобудови математичних моделей інформаційних систем в умовах ризику таневизначеності; поріг ризику, поріг безпеки, їх зв'язок; зони ризику; ризики вуправлінні інформаційною безпекою; особливості управління інформаційнимиризиками.

Вміти: оцінити надійність систем захисту;визначити ризики інформаційноїсистеми; обирати рішення при невизначеності; управляти інформаційнимиризиками; проводити аудит системи інформаційної безпеки.

4. Структура курсу

ЛЕКЦІЇ

Змістовний модуль №1

1. Розвиток загальної теорії ризиків в історичному аспекті.

1.1 Фактори, що зумовлюють підвищення ролі теорії ризиків в сучасному світі.

1.2 Об'єкти дослідження загальної теорії ризиків. Концепції ризику.

1.3 Основні визначення. Ризик. Ризик інформаційної безпеки. Загроза. Уразливість. Актив. Аналіз, оцінка та оцінювання ризику.

1.4 Управління ризиком. Властивості, що визначають поняття і прояв ризику.

2. Поняття невизначеності. Класифікація невизначеностей.

2.1 Класифікація ризиків. Концепції аналізу ризику (за сферами прояву).

2.2 Методи аналізу ризику в рамках технократичної концепції.

2.3Основні національні та міжнародні стандарти в сфері аналізу, оцінки та управління ризиками.

2.4 Основні міжнародні стандарти в сфері управління ризиками інформаційної безпеки

Змістовний модуль №2

3 Система управління інформаційними ризиками. Структура.

3.1 Процесна модель управління ризиками.

3.2 Процес управління ризиками інформаційної безпеки відповідно до ISO 27005.

3.3 Процес управління ризиками інформаційної безпеки відповідно до ISO 27005. 2.4 Характеристика етапу «Встановлення контексту».

3.4 Процес управління ризиками інформаційної безпеки відповідно до ISO 27005.

Характеристика етапу «Встановлення контексту». Область застосування і кордони.

3.5 Оцінка ризиків інформаційної безпеки. Основні методики. Аналіз ризиків інформаційної безпеки відповідно до ISO 27005. Етап ідентифікації ризиків.

4 Ідентифікація активів.

4.1Ідентифікація загроз.

4.2 Ідентифікація контролів.

4.3 Ідентифікація вразливостей.

4.4 Ідентифікація наслідків.

5 Оцінка ризиків інформаційної безпеки відповідно до ISO 27005.

5.1 Методології. Оцінка ймовірності. Оцінка наслідків.

5.2 Обробка ризиків інформаційної безпеки відповідно до ISO 27005.

5.2 Комунікації ризику інформаційної безпеки відповідно до ISO 27005.

5.3 Моніторинг та перегляд ризику інформаційної безпеки відповідно до ISO 27005.

ПРАКТИЧНІ ЗАНЯТТЯ

1.Програмне моделювання процесу управління ризиками інформаційної безпеки.

2.Оцінка ризиків невідповідності вимогам ДСТУ ISO/IEC 27001.

3.Оцінка ризиків із застосуванням моделювання інформаційних потоків.

4.Оцінка ризиків із застосуванням моделювання загроз та вразливостей

5.Оцінка ризиків із застосуванням методики FAIR

5. Технічне обладнання та/або програмне забезпечення

Необхідний доступ до системи дистанційного навчання НТУ «ДП». Активований акаунт університетської пошти (student.i.p.@nmu.one) на Офіс365. Дистанційна платформа Moodle. Система MS Office 365.

6. Система оцінювання та вимоги

6.1. Навчальні досягнення здобувачів вищої освіти за результатами вивчення курсу оцінюватимуться за шкалою, що наведена нижче:

Рейтингова шкала	Інституційна шкала
90 – 100	відмінно
74 -89	добре
60-73	задовільно
0-59	незадовільно

6.2. Здобувачі вищої освіти можуть отримати **підсумкову оцінку** з навчальної дисципліни на підставі поточного оцінювання знань за умови, якщо набрана кількість балів з поточного тестування та самостійної роботи складатиме не менше 60 балів.

Максимальне оцінювання:

Теоретична частина	Практична частина		Бонус	**Разом**
	При своєчасному складанні	При несвоєчасному складанні		
55	45	30	0	**100**

Практичні роботи приймаються за контрольними запитаннями до кожної з роботи. Теоретична частина оцінюється за результатами здачі іспиту. Кожний білет містить 2 питання.

6.3. Критерії оцінювання підсумкової роботи

Робота повинна містити розгорнуті відповіді на два питання білету. Якщо робота виконується у дистанційному режимі, то видача номеру білета проходить через систему MS Teams у зазначеній викладачем групі спілкування. В такому режимі виконана робота пишеться вручну, фотографується та відсилається не електронну пошту викладача у впродовж встановленого викладачем часу. За виконану роботу нараховуються бали:

55 бали – дана розгорнута відповідь на два питання;

40 балів – дана розгорнута відповідь на одне питання, але є помилки при розгляді іншого питання, або є несуттєві помилки у відповідях на два питання;

25 балів – дана повна відповідь на одне питання або на два питання зі значними помилками;

15 балів – відповідь на одне питання із значними помилками;

0 балів – відповіді на питання відсутні або повністю невірні, або робота здана несвоєчасно.

6.4. Критерії оцінювання практичної роботи

З кожної практичної роботи здобувач вищої освіти отримує запитання з переліку контрольних запитань до роботи.

15 балів – Достатня зрозумілість відповіді

10 бали – Добра зрозумілість відповіді

7 бали – Задовільна зрозумілість відповіді

0 балів – Незадовільна зрозумілість відповіді

7. Політика курсу

7.1. Політика щодо академічної доброчесності

Академічна доброчесність здобувачів вищої освіти є важливою умовою для опанування результатами навчання за дисципліною і отримання задовільної оцінки з поточного та підсумкового контролів. Академічна доброчесність базується на засудженні практик списування (виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання), плагіату (відтворення опублікованих текстів інших авторів без зазначення авторства), фабрикації (вигадування даних чи фактів, що використовуються в освітньому процесі). Політика щодо академічної доброчесності регламентується положенням "Положення про систему запобігання та виявлення плагіату у Національному технічному університеті "Дніпровська політехніка". https://cutt.ly/IBesJEc.

У разі порушення здобувачем вищої освіти академічної доброчесності (списування, плагіат, фабрикація), робота оцінюється незадовільно та має бути виконана повторно. При цьому викладач залишає за собою право змінити тему завдання.

7.2.Комунікаційна політика

Здобувачі вищої освіти повинні мати активовану університетську пошту.

Усі письмові запитання до викладачів стосовно курсу мають надсилатися на університетську електронну пошту.

7.3. Політика щодо перескладання

Роботи, які здаються із порушенням термінів без поважних причин оцінюються на нижчу оцінку. Перескладання відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).

7.4 Політика щодо оскарження оцінювання

Якщо здобувач вищої освіти не згоден з оцінюванням його знань він може опротестувати виставлену викладачем оцінку у встановленому порядку.

7.5. Відвідування занять

Для здобувачів вищої освіти денної форми відвідування занять є обов'язковим. Поважними причинами для неявки на заняття є хвороба, участь в університетських заходах, академічна мобільність, які необхідно підтверджувати документами. Про відсутність на занятті та причини відсутності здобувач вищої освіти має повідомити викладача або особисто, або через старосту.

За об'єктивних причин (наприклад, міжнародна мобільність) навчання може відбуватись в он-лайн формі за погодженням з керівником курсу.

8 Рекомендовані джерела інформації

8.1. Основні

1. Архипов О. Є. Вступ до теорії ризиків: інформаційні ризики : моногр. / О. Є. Архипов. – К. : Нац. акад. СБУ, 2015. – 248 с.

2. ДСТУ ISO/IEC 27005:2015 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2011, IDT).

3. ДСТУ EN 50600-2-5:2022 Інформаційні технології. Засоби й інфраструктури центрів оброблення даних. Частина 2-5. Системи безпеки (EN 50600-2-5:2016, IDT).

4. ДСТУ CLC/TR 50174-99-2:2022 Інформаційні технології. Монтаж кабелів. Частина 99-2. Зменшення негативних наслідків та захист від електричних перешкод (CLC/TR 50174-99-2:2020, IDT).

5. ДСТУ 8961:2019 Інформаційні технології. Криптографічний захист інформації. Алгоритми асиметричного шифрування та інкапсуляції ключів.

6. ДСТУ ISO 31000:2018 Менеджмент ризиків. Принципи та керівні вказівки (ISO 31000:2018, IDT) (Національний стандарт України).

7. ДСТУ IEC/ISO 31010:2013 Керування ризиком. Методи загального оцінювання ризику (IEC/ISO 31010:2009, IDT) (Національний стандарт України).

8.2. Допоміжні

1. ДСТУ 4145-2002 Інформаційні технології. Криптографічний захист

інформації. Цифровий підпис, що грунтується на еліптичних кривих. Формування та перевіряння.

2. ДСТУ ISO Guide 73:2013 Керування ризиком. Словник термінів (ISO Guide 73:2009, IDT).