СИЛАБУС
Кафедра кібербезпеки та математичного моделювання

Назва курсу	**Управління ризиками інформаційної безпеки**
Мова викладання	українська
Викладач (-і)	Ткач Ю.М., завкафедри кібербезпеки та математичного моделювання, д.пед.н., професор
Профайл викладача (-ів)	https://mmi.stu.cn.ua/personal-kafedry/ ORCID 0000-0002-8565-0525
Контакти викладача	(063) 594 22 94 tkachym79@gmail.com

1. **Анотація курсу** -

Предметом навчальної дисципліни "Управління ризиками інформаційної безпеки" є основні поняття, принципи, методи та засоби управління ризиками інформаційної безпеки, а також процедури управління ризиками інформаційної безпеки відповідно до вимог найбільш поширених міжнародних стандартів.

Об'єкт навчальної дисципліни – ризики інформаційної безпеки.

Організаційні форми, методи й засоби забезпечення високої фундаментальної, професійної і практичної спрямованості та диференційованого підходу навчання студентів: для ефективної організації навчальних занять використовуються такі форми роботи, як розповідь, навчальна лекція, практична робота, дискусія, робота з книгою та в Інтернеті, постановка завдання, планування процесу виконання, ілюстрування, демонстрування, регулювання й контроль, аналіз підсумків практичної роботи.

Практична та професійна спрямованість дисципліни зумовлена набуттям знань і вмінь щодо проведення об'єктивної оцінки рівня ризиків інформаційної безпеки. Насамперед, це знання та вміння, які дають змогу виявляти, враховувати, реагувати і аналізувати ризики інформаційної безпеки. Без реалізації цих процесів неможливо забезпечити рівень захищеності, адекватний сучасним стандартам і галузевим нормам.

Модуль 1 Моделювання інформаційних систем в умовах ризику та невизначеності.

Тема 1. Місце дисципліни в системі підготовки фахівця із організації інформаційної безпеки. . Історичні аспекти поняття ризику. Місце і роль інформаційних ризиків в управлінні діяльністю організацій.

Предмет дисципліни, її цілі та задачі. Структура, завдання і форми контролю, основна література. Ризик у повсякденому житті. Побутове розуміння ризику. Історичні аспекти поняття ризику. Ризик у галузях знань. Ризикологія як точна наука. Теорія рішень як основа прийняття оптимальних рішень в умовах ризику і невизначеності. Місце і роль інформаційних ризиків в управлінні діяльністю організацій.

Тема 2. Формування та формалізація поняття ризику.

Поняття ризику, оцінка ризику, аналіз ризику, методи та методики управління ризиками. Основні характеристики ризику та їх вимірювання: індекс ризику, ентропія, напруженість ризикового середовища (поля). Поняття безпеки, його формування та математична формалізація. Поріг ризику, поріг безпеки, їх зв'язок. Вибір і рішення при невизначеності. Теорія вибору при відсутності об'єктивно відомих ймовірностей подій. Різниця з теорією прийняття рішень в умовах ризику. Суб'єктивний аналіз введення ймовірностей при повній невизначеності.

Тема 3. Ризики, кризи та катастрофи.

Елементи ризикології криз і катастроф. Динаміка ризик-факторів, як інформаційний індикатор ризик-кризовості. IT-ризики. Виявлення IT-ризиків. Моніторинг та управління. Зона ризиків. Види ризиків в інформаційній системі. Уподобання, вибір в умовах ризику і стохастичне домінування. Аксіоматичний підхід до побудови критеріїв вибору в умовах ризику. Огляд принципів побудови математичних моделей ризиків. Нормальні моделі. Введення в принципи побудови динамічних стохастичних моделей. Прогнозування ризиків. Методи соціально-економічного прогнозування. Статистичні методи прогнозування. Експертні методи прогнозування. Проблеми застосування методів прогнозування в умовах ризику. Прийняття рішень і сучасні комп'ютерні технології прогнозування. Підходи до обліку невизначеності при описі ризиків.

Модуль 2. Методи аналізу та оцінки ризиків

Тема 4. Методи аналізу та оцінки ризиків.

Основні операції над ризиками. Зона ризиків. Алгебра ризиків. Числові показники (характеристики) ризику. Числові характеристики ризику процесу функціонування інформаційної системи в натуральному вираженні. Оцінювання ризику через математичні сподівання і дисперсії. Випадок нормальних розподілів. Основні методи оцінки та аналізу інформаційних ризиків. Методи аналізу ризику та невизначеності в управлінні інформаційною безпекою.

Тема 5. Методи оцінки інформаційних ризиків за міжнародними стандартами.

Підходи до оцінювання ризиків. Резонанс ризик-факторів. Застосування ідентифікації ризик-факторів. Ризик і безпека процесу функціонування інформаційної системи. Числові характеристики ризику процесу функціонування інформаційної системи у відносному вираженні: коефіцієнт варіації, коефіцієнт семі варіації, коефіцієнт сподіваних збитків при запланованому доході

Тема 6. Числові характеристики ризику процесу функціонування інформаційної системи у відносному вираженні.

Підходи до управління ризиками. Ризику в управлінні інформаційною безпекою. Керування ризиками. Технологія керування ризиками. Оцінка рівня загроз та уразливостей. Системний підхід в управління ризиками. Технології оцінки та аналізу ризиків. Методи вирішення багатокритеріальних завдань управління ризиками. Поняття аудиту. Види аудиту. Аудит системи інформаційної безпеки. Прийняття рішень в умовах ризику (стохастичної невизначеності).

Тема 7. Методики аналізу та оцінки ризиків.

Формалізація аналізу та синтез ризику. Якісні та кількісні методики управління інформаційними ризиками. Методики оцінки та аналізу ризиків: COBRA, RA Software Tool, CRAMM, MethodWare, Гриф.

Тема 8. Управління інформаційними ризиками.

Статистичні, експертні, лінгвістичні методи оцінки та аналізу інформаційних ризиків. Методи оцінки інформаційних ризиків за міжнародними стандартами: ISO 15408, ISO 27002 (BS7799), BSI, NIST 80030, SAC, COSO, SAS 55/78.

Тема 9. Ризик-менеджмент в управлінні інформаційною безпекою.

Реєстр інформаційних ресурсів. Реєстр вимог безпеки. Критерії оцінки збитків. Узагальнена схема процесу управління IT-ризиками. План аудиту безпеки. План оцінки ризиків. Методологія оцінки ризиків інформаційної безпеки. Сучасні концепції управління інформаційними ризиками.

2. Мета та цілі курсу -

Основна мета дисципліни надати основні відомості про принципи та методи оцінки ризиків, прийняття рішень при невизначеності.

Під час вивчення дисципліни здобувач вищої освіти (ЗВО) має набути або розширити наступні загальні (КЗ) та фахові (КФ) компетентності, передбачені освітньою програмою:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 2. Знання та розуміння предметної області та розуміння професії.

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

КФ 5. Здатність розробляти, планувати, аналізувати та впроваджувати систему доступу до інформаційних ресурсів, а також систему аудиту і контролю ефективності функціонування інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації.

КФ 6. Здатність розробляти та впроваджувати заходи протидії кіберінцидентам, а також аналізувати, здійснювати процедури управління та контролю інцидентами, організовувати та проводити розслідування, надавати рекомендації щодо заходів їх попередження та протидії.

Завдання вивчення навчальної дисципліни є:

- моделювання інформаційних систем в умовах ризику та невизначеності;
- оцінка ризиків інформаційної безпеки;
- управління ризиками інформаційної безпеки.

На базі здобутих знань фахівець зможе вирішувати професійні задачі, що базуються на управлінні ризиками в інформаційній безпеки та аудити системи інформаційної безпеки.

3. Результати навчання –

Під час вивчення дисципліни ЗВО має досягти або вдосконалити наступні програмні результати навчання (ПРН), передбачені освітньою програмою:

ПРН 2 - планувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;

ПРН 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;

ПРН 5- реалізовувати процеси постійної самоосвіти і професійної сертифікації, критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності;

ПРН 7- проектувати, впроваджувати, та супроводжувати інформаційно-комунікаційні системи, а також забезпечувати захист інформаційних ресурсів мереж (мережева безпека) та всієї інфраструктури установи на базі сучасних моделей, методів і засобів передачі даних в комутативних або без комутативних каналах зв’язку, хмарного простору, протоколів обміну даними, мережного устаткування, тощо.

В результаті вивчення дисципліни студент повинен:

Знати: основні характеристики ризику та їх вимірювання; числові показники (характеристики) ризику; основні методи оцінки інформаційних ризиків; найпоширеніші методики оцінки інформаційних ризиків; основні принципи побудови математичних моделей інформаційних систем в умовах ризику та невизначеності; поріг ризику, поріг безпеки, їх зв'язок; зони ризику; ризики в управлінні інформаційною безпекою; особливості управління інформаційними ризиками.

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

4. Обсяг курсу.

Вид заняття	Загальна к-сть годин
лекції	16
практичні	14
самостійна робота (РГР)	90

5. Пререквізити – взаємозв'язок із суміжними дисциплінами: вивчення навчальної дисципліни "Аудит та управління інцидентами інформаційної безпеки" поглиблює знання студентів отримані під час вивчення дисциплін "Менеджмент інформаційної безпеки" (при підготовці фахівців освітньо-кваліфікаційного рівня "бакалавр" за напрямом "Кібербезпека") та "Забезпечення безперервності бізнесу".

6. Система оцінювання та вимоги

Оцінювання проводиться за 100-бальною шкалою.

Бали нараховуються за наступним співвідношенням:

• практичні заняття : 20% семестрової оцінки;

• домашні завдання: 20% семестрової оцінки;

•РГР: 20% семестрової оцінки;

• іспит: 40% семестрової оцінки.

Загальна система оцінювання курсу	Управління ризиками інформаційної безпеки
Вимоги до РГР	**Критерії оцінювання написання** 1. Повнота розкриття. 2. Авторський внесок. 3. Актуальність. 4. Практична значимість. 5. Відповідність вимогам оформлення. **Вимоги оформлення** Об'єм 15-25 сторінок. 14 шрифт. Times New Roman. Одинарний інтервал. Робота складається з: - титул – 1 с.; - зміст – 2 с.; - вступ: актуальність, об'єкт, предмет, мета та завдання дослідження. - основна частина: не менше 2 розділів. - висновки формуються відповідно до завдань. **Критерії оцінювання захисту РГР.** *Стартовий бал 15.* Захист РГР триває не більше 10 хвилин. Якщо при захисті доповідач вклався в час, але не розкрив тему, нараховуються мінус бали (залежно від повноти розкриття). За неправильну відповідь на запитання мінус 2 бали, а за неповну відповідь мінус 1 бал. За відсутність презентації мінус 2 бали.
Практичні заняття	**Критерії оцінювання практичних занять** 1. Підготовленість до практичних занять. 2. Самостійність виконання практичних робіт. 3. Повнота розкриття теми. 4. Своєчасність виконання практичних робіт
Умови допуску до підсумкового контролю	Позитивна оцінка за всіма обов'язковими видами робіт (практичні заняття та РГР)

7. Політики курсу -

Політика щодо академічної доброчесності: Списування під час контрольних робіт заборонені. Мобільні пристрої дозволяється використовувати лише під час онлайн-тестування та підготовки практичних завдань.

Жодні форми порушення академічної доброчесності не толеруються. У випадку таких подій – реагування відповідно до Положення про академічну доброчесність студентів та науково-педагогічних працівників Чернігівського національного технологічного університету та Методичних рекомендацій для закладів вищої освіти з підтримки принципів академічної доброчесності.

Правила перезарахування кредитів у випадку мобільності, правила перескладання або відпрацювання пропущених занять тощо: відбувається згідно з Положенням про організацію освітнього процесу в ЧНТУ.

Політика щодо дедлайнів та перескладання: роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (75% від можливої максимальної кількості балів за вид діяльності).

Перескладання модулів відбувається за наявності поважних причин (наприклад, лікарняний).

Політика щодо відвідування: Відвідування занять є обов'язковим компонентом оцінювання. За об'єктивних причин (наприклад, хвороба, працевлаштування, міжнародне стажування) навчання може відбуватись в онлайн-формі за погодженням.

8. Рекомендована література

Базова:

1. Математические основы теории риска / В.Ю.Королев, В.Е Бенинг, С.Я. Шоргин. – Учебн. пособ. - М.: Физматлит, 2007, 544 с.
2. Шоломицкий А. Г. Теория. риска. Выбор при неопределенности и моделирование риска – М.: Изд. Дом ГУ ВШЭ, 2005. – 380с.
3. Риск-менеджмент. / В.Н. Вяткин, И.В. Вяткин, В.А. Гамза, Ю.Ю. Екатеринославский, Дж.Дж Хэмптон; И. Юргенс, ред. Учебник. - М: Дашков и К, 2003. - 494 с.
4. Інформаційна безпека та сучасні мережеві технології: Англо-українсько-російський словник термінів / В.П. Бабак, О.Г. Корченко. – К.: НАУ, 2003. – 670с.
5. Надійнісне проектування технічних систем і оцінка риску. / Хенлі Ернест Джон, Кумамото Хиромицу; пер. з англ. О.Ю. Зареніна, В.Ф.Хмеля; під ред. Ю.Г.Зареніна. - К: Вища школа, 1987. - 544 с.
6. Основи системного аналізу / М.З. Згуровський, Н.Д. Панкратова. – К.: Видавнича група BHV, 2007. – 544 с.
7. Хохлов Н.В. Управление риском: Учебное пособие для вузов. - М.: "ЮНИТИ", 1999. - 240с.
8. Корченко О.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения. – К.: «МК-Пресс», 2006. – 320с.
9. Энциклопедия безопасности авиации / Н.С. Кулик, В.П. Харченко, М.Г. Луцкий и др.; Под. ред. Н.С. Кулика. – К.: Техніка, 2008. – 1000с.; ил. – Библиогр.: с. 977-999.

Додаткова література:

10. Мониторинг и оценка риска систем "защита - объект - среда" / Ю. В. Есипов, Ф. А. Самсонов, А. И. Черемисин – М.: ЛКИ, 2008. – 138с.
11. Макдональд Д. Промышленная безопасность, оценка риска и системы аварийного останова. – М.: ИДТ, 2007. – 416с.

Інформаційні ресурси

1. www.me.gov.ua – Міністерство економіки України
2. zet.in.ua – актуальна економічна статистика та аналітика економіки України
3. www.cia.gov – The Central Intelligence Agency (CIA)
4. http://www.ukrstat.gov.ua – Державний комітет статистики
5. http://www.ukrstat.gov.ua/operativ/operativ2005/vvp/vvp_ric/vvp_u.htm - Валовий внутрішній продукт