МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

КАФЕДРА КІБЕРБЕЗПЕКИ

Василенко М. Д., Слатвінська В. М.

ТЕОРІЯ РИЗИКІВ

НАВЧАЛЬНО-МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

(для студентів факультету кібербезпеки та інформаційних технологій)

Одеса

2020

Рекомендовано навчально-методичною радою
Національного університету «Одеська юридична академія»,
протокол № 2 від 4 грудня 2020 р.

Рецензенти:
Тупкало В.М. – доктор технічних наук, професор, завідувач кафедри менеджменту та інформаційних технологій Інституту інтелектуальної власності та права Національного університету «Одеська юридична академія», м. Київ
Логінова Н.І. – кандидат педагогічних наук, доцент, завідувачка кафедри інформаційних технологій Національного університету «Одеська юридична академія»

Василенко М. Д., Слатвінська В. М.
Т Теорія ризиків : навчально-методичні рекомендації (в допомогу до самостійної роботи для здобувачів вищої освіти ступеня бакалавра факультету кібербезпеки та інформаційних технологій) [Електронне видання]. / М. Д. Василенко, В. М. Слатвінська; кафедра кібербезпеки НУ «Одеська юридична академія». - Одеса : Фенікс, 2020. - 32 с. - Режим доступу: http://dspace.onua.edu.ua/handle/11300/14523
DOI

ISBN

Навчально-методичні рекомендації з курсу «Теорія ризиків» розроблено відповідно до навчального плану, вони складаються з навчальної програми курсу, методичних рекомендацій із проведення практичних занять, питань до самоконтролю, завдань для самостійної роботи, списку рекомендованої літератури. Вивчення дисципліни «Теорія ризиків» допоможе студентам розвинути навички застосування методів та засобів оцінки ризиків в умовах широкого використання сучасних інформаційних технологій; способів оцінювання ризикових ситуацій, методів отримання кінцевого результату і вибору оптимальної стратегії в умовах невизначеності, випадковості та конфлікту.
Матеріали призначено для студентів факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія», які навчаються за спеціальністю «кібербезпека».

УДК

ISBN

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Навчальна дисципліна «Теорія ризиків» призначена для студентів, що навчаються за освітньо-кваліфікаційним рівнем «бакалавр». Вивчення дисципліни «Теорія ризиків» полягає у формуванні у майбутніх спеціалістів умінь та компетенцій для забезпечення ефективної оцінки ризиків в техніці, зокрема в інформаційних технологіях, необхідних для подальшої роботи. Студенти мають ознайомитися із сучасними науковими досягненнями в теоретичних питаннях ризику, опанувати способи оцінювання ризикових ситуацій, методи отримання кінцевого результату і вибору оптимальної стратегії в умовах невизначеності, випадковості та конфлікту. Необхідно навчити студентів застосуванню методів та засобів оцінки ризиків в умовах широкого використання сучасних інформаційних технологій.

Міждисциплінарні зв’язки. Вивчення курсу «Теорія ризиків» передбачає наявність систематичних та ґрунтовних знань із суміжних курсів («Теорія ймовірностей та математична статистика», «Дискретна математика», «Математичний аналіз»), а також розуміння основ програмування на мові Python.

ЗАПЛАНОВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Метою викладання навчальної дисципліни «Теорія ризиків» є формування у майбутніх спеціалістів умінь та компетенцій для забезпечення ефективної оцінки ризиків, необхідних для подальшої роботи, розуміння методів та засобів оцінки ризиків в умовах широкого використання сучасних інформаційних технологій, опанування наукових досягнень в теоретичних питаннях ризику, володіння способами оцінювання ризикових ситуацій, методами отримання кінцевого результату і вибору оптимальної стратегії в умовах невизначеності, випадковості та конфлікту.

Основними завданнями вивчення дисципліни «Теорія ризиків» визначено підготовку фахівців, безпосередньо готових до дослідження ризику, які повинні ідентифікувати небезпеки, оцінювати конкретні ризики, аналізувати і прогнозувати розвиток небезпечних ситуацій, на основі чого виробляти рекомендації щодо ефективних заходів управління ризиком осіб, відповідальних за прийняття рішень.

Згідно з вимогами освітньо-професійної програми студенти повинні:

знати:

класифікацію і види ризиків, способи оцінки ступеню ризику, зміст та управління мірою ризику;

сутність і структуру страхування і перестрахування, їх види і форми;

основні фундаментальні поняття і закони теорії ризиків для їх використання в сучасних кіберсистемах;

принципи побудови алгоритмів оцінки ризиків, основних стандартів оцінки ризиків та їх використання в задачах захисту інформації;

вміти:

використовувати методи та засоби оцінки ризиків в інформаційних технологіях;

використовувати програмні засоби, які реалізують основні функції оцінки ризиків;

проводити дослідження на відповідному рівні, здатність до пошуку, оброблення та аналізу інформації з різних джерел;

вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;

здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів;

впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;

здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку;

впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки;

розробляти моделі загроз та порушника.

шукати, оброблювати та аналізувати інформацію.

бути ознайомленими:

з проєктуванням різного рівня систем оцінки ризиків;

з процедурою управління інцидентами;

з функціонуванням комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

з результатами рекомендацій, що випливають з моделювання ризикових ситуацій, і використовувати їх у практичній діяльності.

СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

№ теми	Види занять	Лекційні заняття (год.)		Практичні заняття (год.)		Самостійна робота (год.)	
	Тема	очна	заоч-на	очна	заоч-на	очна	заоч-на
1	Ризики, їх характеристики. Інформаційні ризики та їх особливості. Методи оцінки ризиків	2	2	2	0	4	4
2	Класифікація ризиків та їх невизначеність	2	2	2	0	4	4
3	Стохастичний ризик, оцінки, критерії	2	0	0	0	4	4
4	Основні поняття теорії випадкових процесів	2	0	1	0	4	4
5	Статистичні методи оцінювання ризиків	2	0	0	0	4	4
6	Якісні методи оцінювання ризиків	2	0	0	0	4	4
7	Матричні методи та критерії прийняття ризикових рішень в умовах невизначеності	2	0	0	0	4	4
8	Застосування теорії ігор в умовах ризику	2	2	0	0	4	4
9	Міжнародна організація зі стандартизації та її стандарти щодо ризиків	2	0	0	2	4	4
10	Основні напрями впливу на ризик	2	0	0	0	4	4
11	Страхування та диверсифікація ризиків	2	0	0	0	4	4
12	Системний аналіз системи "людина - техніка - середовище"	2	0	0	0	4	4
13	Інформаційні ризики, їх характеристики та відмінності	2	0	0	0	4	4
14	Класифікація загроз інформації в інформаційних системах. Загрози безпеки інформації як інформаційні ризики	2	0	0	0	4	4
15	Практичні аспекти оцінювання реалізації загроз в інформаційних системах	2	0	0	0	4	4
	Всього	30	6	5	2	60	60

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Тема 1. Ризики, їх характеристики. Інформаційні ризики та їх особливості. Методи оцінки ризиків

Поняття «ризик», його ймовірнісні характеристики. Суб'єкт та об'єкт ризику. Функції ризику. Причини виникнення ризиків. Характеристика ризиків та методів їх оцінки. Визначення: ризик та теорія ризику. Інформаційні ризики. Кількісні методи оцінки ризику. 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. Методики оцінки та аналізу ризиків: COBRA, RA Software Tool, CRAMM, MethodWare, Гриф. Необхідність використання методів Імітаційного моделювання в задачах управління ризиками. Методологія Монте–Карло в задачах в задачах управління ризиками. Simulink технологія моделювання ризиків. Stateflow моделі управління ризиками.

Тема 2. Класифікація ризиків та їх невизначеність

Поняття кваліфікації і класифікації ризику. Класифікація ризиків за джерелом походження ризику. Об'єктивний і суб'єктивний ризики. Класифікація ризику за мірою прояву: низький, нижче середнього, середній, вище середнього, високий, найвищий. Комплексний ризик. Нульовий ризик. Класифікації за іншими ознаками ризиків. Невизначеність та її джерела. Зв'язок між ризиком і невизначеністю. Фактори, що формують невизначеність. Вплив на ризик об'єктів ризиків. Розмежування ризиків за їх наслідками. Небезпечні явища як ризик.

Тема 3. Стохастичний ризик, оцінки, критерії

Об'єктивні критерії оцінки стохастичного ризику. Середнє, дисперсія. Стохастичне домінування першого й другого порядку. Суб'єктивні критерії оцінки стохастичного ризику. Міра очікуваної корисності. Суб'єктивні ймовірності. Теорія проспектів. Стохастичні процеси з незалежними прирощеннями.

Тема 4. Основні поняття теорії випадкових процесів

Стохастичні процеси з незалежними прирощуваннями. Система та організація управління ризиками. Поняття «ризик-менеджменту». Етапи процесу управління ризиком: збір інформації за аспектами ризику, якісний аналіз, методи кількісного оцінювання ризику, розробка заходів щодо оптимізації ризику, прийняття чи відхилення ризикового рішення. Правила управління ризиками.

Тема 5. Статистичні методи оцінювання ризиків

Дисперсійний метод оцінювання ризику, основні показники варіації. Імовірнісний метод оцінювання ризику. Визначення ймовірності досягнення бажаного результату за інтегральною функцією щільності розподілу ймовірностей. Метод в-коефіцієнта оцінювання системного ризику проекту (бізнесу). Методики побудови систем захисту інформації, що включають етап аналізу ризиків. Методика "Facilitated Risk Analysis Process (FRAP)". Методика оцінка серйозності мережевої атаки, яка використовується SANS / GIAC.

Тема 6. Якісні методи оцінювання ризиків

Сутність та групування якісних методів оцінювання ризику. Метод мозкового штурму. Методика оцінки NIST 800-30. Методика CRAMM. Методика OCTAVE. Обчислення коефіцієнта конкордації Кендала. Загальна характеристика експертних процедур, їх використання для розрахунку рівня ризику проекту. Перевірка узгодженості дій експертів на основі розрахунку коефіцієнта конкордації. Методи асоціацій та аналогій. Постановка задачі прийняття рішень в умовах ризику та невизначеності.

Тема 7. Матричні методи та критерії прийняття ризикових рішень в умовах невизначеності

Використання матриць в оцінюванні альтернативних рішень. Поняття «прийняття рішення», його широкий і вузький сенси. Класична модель прийняття рішення. Метод суду. Метод комісій. Метод Делфі. Метод генерації ідей. Критерії прийняття рішень в умовах високої ентропії: максимінний критерій Вальда, мінімаксний критерій Севіджа, критерій недостатнього обґрунтування Лапласа, критерій узагальненого песимізму-оптимізму Гурвіца.

Тема 8. Застосування теорії ігор в умовах ризику

Методологічні засади теорії ігор. Класифікація ігор. Чиста та змішана стратегії. Засоби розв'язання завдань теорії ігор. Рівновага в домінантних стратегіях. Метод знаходження рівноваги Неша. Метод знаходження оптимумум Паретто. Метод знаходження рішення Штакельберга та рівноваги Штакельберга. Метод знаходження змішаних стратегій. Матриці платежів. Мінімакс, рівновага. Рішення матричних ігор. Біматричні ігри, рівновага Неша, дилема невільника. Оптимальна поведінка в умовах специфічних видів ризику.

Тема 9. Міжнародна організація зі стандартизації та її стандарти щодо ризиків

Міжнародний стандарт ISO 31000. Загальний зміст та зміни, що прийняті в 2018 році. Міжнародний стандарт ISO 31010. Загальна характеристика та основний зміст. Етапи управління інцидентами інформаційної безпеки відповідно до ISO/IEC 27035

Тема 10. Основні напрями впливу на ризик

Методи уникнення ризику. Вирівнювання, збереження, зменшення та передача ризику. Характеристика основних засобів регулювання ризику: резервування засобів, система вибору клієнтів, залучення зовнішніх джерел, здобуття додаткової інформації, диверсифікація, лімітування, біржове хеджування ризиків. Міжнародний стандарт ISO 31000 щодо основних напрямів впливу на ризик.

Тема 11. Страхування та диверсифікація ризиків

Сутність страхування, суб’єкти та об’єкти страхування. Особисте, майнове страхування та страхування відповідальності. Критерії прийняття рішень щодо страхування ризиків. Поняття диверсифікації, сутність політики диверсифікації підприємства, поняття кореляції активів. Причини диверсифікації підприємницької діяльності. Переваги та недоліки диверсифікації. Аналітичний, табличний та графічний методи визначення доцільності диверсифікації.

Тема 12. Системний аналіз системи "людина - техніка - середовище"

Методичні засади визначення небезпечності об’єктів та процесів. Надійність технічних систем. Надійність оператора. Фактори надійності оператора. Фактори середовища. Ергономічні фактори. Міжнародний стандарт ISO 31000 в аналізі системи "людина - техніка - середовище".

Тема 13. Інформаційні ризики, їх характеристики та відмінності

Ризики та їх інформаційна складова. Інформаційний ризик та поняття «загроза безпеки інформації». Інформаційна система та її ризик. Якість інформації. Показники якості інформації. Дія інформаційних ризиків. Причини та чинники інформаційних ризиків. Категорії інформаційних ризиків. Статистичні, експертні, лінгвістичні методи оцінки та аналізу інформаційних ризиків. Мінімізація інформаційних ризиків. Методології для моделювання інформаційних ризиків: STRIDE, PASTA, Trike, VAST, OCTAVE. Правила попередження IT-ризиків. Методи оцінки інформаційних ризиків за міжнародними стандартами: ISO 15408, ISO 27002 (BS7799), BSI, NIST 80030, SAC, COSO, SAS 55/78. Обчислення комплексного інформаційного ризику.

Тема 14. Класифікація загроз інформації в інформаційних системах. Загрози безпеки інформації як інформаційні ризики

Шкідливі програми і віруси як ризики інформації. Класи шкідливих програм. Віруси, їх типи та класифікація. Виявлення вірусів та блокування роботи програм-вірусів, усунення наслідків. Нешкідливі, небезпечні, дуже небезпечні віруси. Профілактика зараження вірусами комп'ютерних систем. Зниження ризиків. Порядок дій користувача при виявленні заражених вірусами комп'ютерних систем. Обчислення узагальнених ризиків на рівні ознак і загроз. Особливості опису та аналізу ризикових ситуацій.

Тема 15. Практичні аспекти оцінювання реалізації загроз в інформаційних системах

Моделювання загроз. Кількісна оцінка моделей загроз. Сучасна методологія SDL. Моделювання загроз як tabula rasa. Загальна характеристика криптографічного захисту інформації. Пріоритизація інформаційних активів за ступенем вразливості. Призначення і загальна класифікація засобів захисту інформації. Особливості захисту інформації в базах даних.

ТЕМИ ПРАКТИЧНИХ ЗАНЯТЬ

Тема 1. Ризики, їх характеристики. Інформаційні ризики та їх особливості. Методи оцінки ризиків

Питання до підготовки:

1. Розкрити поняття ризику та його ймовірнісних характеристик.
2. Встановити суб'єкт та об'єкт ризику та визначити функції ризику.
3. Встановити причини виникнення ризиків. Дайте визначення поняттю "ризик технологічний".
4. Надати характеристики ризикам та методам їх оцінки.
5. Обговорити визначення: «ризик» і «теорія ризику».
6. Розкрити сутність методів оцінки ризиків.
7. Охарактеризувати поняття та особливості інформаційних ризиків, їх мінімізація.

Література:
Основна: 1-18
Допоміжна: 1-15

Тема 2. Класифікація ризиків та їх невизначеність

Питання до підготовки:

1. Поняття класифікації і кваліфікації ризику.
2. Класифікація ризиків за джерелом походження ризику
3. Класифікації за іншими ознаками ризиків
4. Невизначеність та її джерела
5. Зв'язок між ризиком і невизначеністю
6. Фактори, що формують невизначеність
7. Вплив на ризик об'єктів ризиків
8. Розмежування ризиків за їх наслідками
9. Небезпечні явища як ризик

Література:
Основна: 1-18
Допоміжна: 1-15

Тема 3. Стохастичний ризик, оцінки, критерії

Питання до підготовки:

1. Об’єктивні критерії оцінки стохастичного ризику. Середнє, дисперсія.
2. Стохастичне домінування першого й другого порядку.
3. Суб’єктивні критерії оцінки стохастичного ризику.
4. Міра очікуваної корисності.
5. Суб’єктивні ймовірності.
6. Теорія проспектів.
7. Стохастичні процеси з незалежними приростами.

Література:
Основна: 1-18
Допоміжна: 1-15

Тема 4. Основні поняття теорії випадкових процесів

Питання до підготовки:

1. Стохастичні процеси з незалежними приростами.
2. Система та організація управління ризиками.
3. Поняття «ризик-менеджменту».
4. Етапи процесу управління ризиком: збір інформації за аспектами ризику, якісний аналіз, методи кількісного оцінювання ризику, розробка заходів щодо оптимізації ризику, прийняття чи відхилення ризикового рішення.
5. Правила управління ризиками.

Література:
Основна: 1-18
Допоміжна: 1-15

Тема 5. Статистичні методи оцінювання ризиків

Питання до підготовки:

1. Дисперсійний метод оцінювання ризику, основні показники варіації.
2. Імовірнісний метод оцінювання ризику. Визначення ймовірності досягнення бажаного результату за інтегральною функцією щільності розподілу ймовірностей.
3. Метод в-коефіцієнта оцінювання системного ризику проекту (бізнесу).

Література:
Основна: 1-18
Допоміжна: 1-15

Тема 6. Якісні методи оцінювання ризиків

Питання до підготовки:

1. Сутність та групування якісних методів оцінювання ризику.
2. Метод мозкового штурму.
3. Загальна характеристика експертних процедур, їх використання для розрахунку рівня ризику проекту.
4. Перевірка узгодженості дій експертів на основі розрахунку коефіцієнта конкордації.
5. Методи асоціацій та аналогій.

Література:
Основна: 1-18
Допоміжна: 1-15

Тема 7. Матричні методи та критерії прийняття ризикових рішень в умовах невизначеності

Питання до підготовки:

1. Використання матриць в оцінюванні альтернативних рішень.
2. Критерії прийняття рішень в умовах високої ентропії: максимінний критерій Вальда, мінімаксний критерій Севіджа, критері недостатнього обґрунтування Лапласа, критерій узагальненого песимізму-оптимізму Гурвіца.

Література:
Основна: 1-18
Допоміжна: 15

Тема 8. Застосування теорії ігор в умовах ризику

Питання до підготовки:

1. Методологічні засади теорії ігор.
2. Класифікація ігор.
3. Чиста та змішана стратегії.
4. Засоби розв’язання завдань теорії ігор.
5. Оптимальна поведінка в умовах специфічних видів ризику.

Література:
Основна: 1-18
Допоміжна: 1-14

Тема 9. Міжнародна організація зі стандартизації та її стандарти щодо ризиків

Питання до підготовки:

1. Міжнародний стандарт ISO 31000. Загальний зміст та зміни, що прийняті в 2018 році.
2. Міжнародний стандарт ISO 31010. Загальна характеристика та основний зміст.

Література:
Основна: 1-18
Допоміжна: 11

Тема 10. Основні напрями впливу на ризик

Питання до підготовки:

1. Методи уникнення ризику.
2. Характеристика основних засобів регулювання ризику: резервування засобів, система вибору клієнтів, залучення зовнішніх джерел, здобуття додаткової інформації, диверсифікація, лімітування, біржове хеджування ризиків.
3. Міжнародний стандарт ISO 31000 щодо основних напрямів впливу на ризик.

Література:
Основна: 1-18
Допоміжна: 1-13

Тема 11. Страхування та диверсифікація ризиків

Питання до підготовки:

1. Сутність страхування, суб’єкти та об’єкти страхування.
2. Особисте, майнове страхування та страхування відповідальності.
3. Критерії прийняття рішень щодо страхування ризиків.
4. Поняття диверсифікації, сутність політики диверсифікації підприємства, поняття кореляції активів.
5. Причини диверсифікації підприємницької діяльності. Переваги та недоліки диверсифікації.

Література:
Основна: 1-18
Допоміжна: 1-10

Тема 12. Системний аналіз системи "людина - техніка - середовище"

Питання до підготовки:

1. Методичні засади визначення небезпечності об’єктів та процесів.
2. Надійність технічних систем. Надійність оператора.
3. Фактори надійності оператора. Фактори середовища. Ергономічні фактори.
4. Міжнародний стандарт ISO 31000 в аналізі системи "людина - техніка - середовище".

Література:
Основна: 1-18
Допоміжна: 9

Тема 13. Інформаційні ризики, їх характеристики та відмінності

Питання до підготовки:

1. Ризики та їх інформаційна складова.
2. Інформаційний ризик та поняття загроза безпеки інформації.
3. Інформаційна система та її ризик. Якість інформації. Показники якості інформації.
4. Дія інформаційних ризиків. Причини та чинники інформаційних ризиків.
5. Категорії інформаційних ризиків.
6. Методології для моделювання інформаційних ризиків: STRIDE, PASTA, Trike, VAST, OCTAVE.
7. Мінімізація інформаційних ризиків. Правила попередження IT-ризиків.
8. Методи оцінки інформаційних ризиків за міжнародними стандартами: ISO 15408, ISO 27002 (BS7799), BSI, NIST 80030, SAC, COSO, SAS 55/78.

Література:
Основна: 1-18
Допоміжна: 10

Тема 14. Класифікація загроз інформації в інформаційних системах. Загрози безпеки інформації як інформаційні ризики

Питання до підготовки:

1. Шкідливі програми і віруси як ризики інформації. Класи шкідливих програм.

2. Віруси, їх типи та класифікація. Виявлення вірусів та блокування роботи програм-вірусів, усунення наслідків.
3. Нешкідливі, небезпечні, дуже небезпечні віруси. Профілактика зараження вірусами комп'ютерних систем.
4. Зниження ризиків. Порядок дій користувача при виявленні заражених вірусами комп'ютерних систем.
5. Обчислення узагальнених ризиків на рівні ознак і загроз. Особливості опису та аналізу ризикових ситуацій.

Література:
Основна: 1-18
Допоміжна: 1-12

Тема 15. Практичні аспекти оцінювання реалізації загроз в інформаційних системах

Питання до підготовки:

1. Моделювання загроз. Кількісна оцінка моделей загроз.
2. Сучасна методологія SDL.
3. Моделювання загроз як tabula rasa.
4. Загальна характеристика криптографічного захисту інформації.
5. Пріоритизація інформаційних активів за ступенем вразливості.
6. Призначення і загальна класифікація засобів захисту інформації.
7. Особливості захисту інформації в базах даних.

Література:
Основна: 1-18
Допоміжна: 8

ЗАВДАННЯ ДЛЯ САМОСТІЙНОЇ РОБОТИ

Тема 1. Кількісні методи оцінки ризику

1. Підготувати доповіді на теми:
- Переваги і недоліки статистичного методу
- Переваги і недоліки методу експертних оцінок
- Переваги і недоліки методу Монте-Карло
- Переваги і недоліки методу аналогій
- Переваги і недоліки методу аналізу сценаріїв
- Переваги і недоліки методу аналізу чутливості
- Переваги і недоліки методу «дерева рішень»
- Переваги і недоліки методу критичних значень

Тема 2. Небезпечні явища як ризик

1. Підготувати доповіді на теми:
- Кількісний аналіз і моделювання небезпек
- Врахування людського чиннику при моделюванні небезпек
- Техногенний ризик: фактори ризику
- Природний ризик: фактори ризику
- Соціально-політичний ризик: фактори ризику
- Комбінований ризик: фактори ризику

Тема 3. Суб'єктивні критерії оцінки стохастичного ризику

1. Підготувати доповіді на теми:
- Особливості суб'єктивного критерію оцінки стохастичного ризику
- Сутність суб'єктивного критерію оцінки стохастичного ризику
- Характеристика суб'єктивного критерію оцінки стохастичного ризику

Тема 4. Стохастичні процеси з незалежними прирощуваннями

1. Підготувати доповіді на теми:
- Однорідні стохастичні процеси з незалежними приростами.
- Пуассонівський процес.
- Вінерівський процес.
- Стаціонарні випадкові процеси.

Тема 5. Метод в-коефіцієнта оцінювання системного ризику проекту (бізнесу)

1. Підготувати доповіді на теми:

- Характеристика методу в-коефіцієнта оцінювання системного ризику проекту (бізнесу)
- Особливості методу в-коефіцієнта оцінювання системного ризику проекту (бізнесу)
- Сутність методу в-коефіцієнта оцінювання системного ризику проекту (бізнесу)

Тема 6. Методи асоціацій та аналогій

1. Підготувати доповіді на теми:
- Застосування методу аналогій для кількісного оцінювання ризиків
- Сутність методу аналогій
- Сутність методу асоціацій

Тема 7. Критерії прийняття рішень в умовах високої ентропії: максимінний критерій Вальда, мінімаксний критерій Севіджа, критерій недостатнього обґрунтування Лапласа, критерій узагальненого песимізму-оптимізму Гурвіца

1. Підготувати доповіді на теми:
- Моделі прийняття рішень в умовах високої ентропії
- Методи прийняття рішень в умовах високої ентропії
- Проблема прийняття рішень в умовах високої ентропії

Тема 8. Засоби розв'язання завдань теорії ігор

1. Підготувати доповіді на теми:
- Розв'язування матричних ігор двох гравців з нульовою сумою в чистих стратегіях.
- Принципи максиміну і мінімаксу.
- Метод в-коефіцієнта оцінювання системного ризику проекту (бізнесу)

Тема 9. Міжнародний стандарт ISO 31010

1. Підготувати доповіді на теми:
- Оцінка умов виникнення ризиків і визначення їх впливу на безпеку праці стандартними методами і засобами
- Процес подання якісного аналізу ідентифікації ризиків і визначення ризиків, що потребують швидкого реагування

Тема 10. Міжнародний стандарт ISO 31000 щодо основних напрямів впливу на ризик

1. Підготувати доповіді на теми:

- Оцінка умов виникнення ризиків і визначення їх впливу на безпеку праці стандартними методами і засобами
- Процес подання якісного аналізу ідентифікації ризиків і визначення ризиків, що потребують швидкого реагування

Тема 11. Причини диверсифікації підприємницької діяльності

1. Підготувати доповіді на теми:
   - Головні причини щодо прийняття рішення про диверсифікацію
   - Сутність та зміст стратегії диверсифікації підприємницької діяльності
   - Умови диверсифікації підприємницької діяльності
   - Інтегральний метод аналізування диверсифікаційних заходів на підприємствах
   - Види диверсифікації та класифікація диверсифікаційних заходів на підприємствах

Тема 12. Міжнародний стандарт ISO 31000 в аналізі системи "людина - техніка - середовище"

1. Підготувати доповіді на теми:
- Сфера застосування Міжнародного стандарту ISO / IEC 31010
- Методичні засади визначення небезпечності об’єктів та процесів
- Надійність технічних систем
- Глобальний (загальносистемний) ризик відмови системи після модернізації

Тема 13. Інформаційний ризик та поняття «загроза безпеки інформації»

1. Підготувати доповіді на теми:
   - Ризики та їх інформаційна складова.
   - Співвідношення інформаційного ризику та поняття загроза безпеки інформації.
   - Інформаційна система та її ризик.
   - Показники якості інформації.
   - Дія інформаційних ризиків.
   - Категорії інформаційних ризиків.
   - Правила попередження ІТ-ризиків.
   - Шляхи мінімізації інформаційних ризиків.
   - Причини та чинники інформаційних ризиків.
   - Моделювання та оцінка інформаційних ризиків за допомогою методології STRIDE.
   - Методи оцінки інформаційних ризиків за міжнародними стандартами: ISO 15408, ISO 27002 (BS7799), BSI, NIST 80030, SAC, COSO, SAS 55/78.
2. Навести і пояснити математичні зв’язки невизначеності із ризиками.

Скласти схему математичних зв’язків невизначеності із ризиками.
3. Ознайомитися зі стандартом ISO 31000 в частині кваліфікації ризиків. Обробити, узагальнити та інтерпретувати отримані результати на практичному занятті.

Тема 14. Порядок дій користувача при виявленні заражених вірусами комп’ютерних систем

1. Підготувати доповіді на теми:
- Як убезпечитися від зараження «вірусом»?
- Що робити, якщо у вас є підозри, що ви заразилися "вірусом"?
- Найвідоміші антивірусні програми
- Порядок профілактики від комп’ютерного вірусу
- Методи пошуку вірусу і шкідливих програм
2. Перевірити власний комп’ютер на наявність шкідливих програм, змінити паролі для входів у користувацькі профілі, оновити фільтри антивірусної програми.

Тема 15. Сучасна методологія SDL. Моделювання загроз як tabula rasa

1. Підготувати доповіді на теми:
- Модель "небезпека-ризик" як модель породження ризиків
- Модель "невизначеність-ризик" як модель породження ризиків
- Модель "можливості- ризик / шанс" як модель породження ризиків

ТЕМИ РЕФЕРАТІВ

1. Наукові підходи до визначення сутності ризику
2. Оцінка ризиків за моделлю DREAD
3. Невизначеність та ризик: співвідношення понять та специфіка прийняття рішень
4. Страхування як принцип управління ризиками
5. Невизначеність як передумова розвитку ризику
6. Типи аналізу небезпек
7. Концепція дерева відмов
8. Сума під ризиком при нормальній щільності їх розвитку подій
9. Історичне моделювання як метод моделювання небезпек
10. Людський чинник як фактор моделювання небезпек
11. Параметрична оцінка як метод оцінки небезпеки
12. Поняття про припустимий і неприпустимий ризик
13. Метод моделювання Монте-Карло та його характеристика
14. Проблеми впровадження ризик орієнтованого підходу в Україні
15. Види ризиків. Підходи щодо класифікації ризиків
16. Технічні ризики та засоби їх зниження
17. Аналіз впливу людського фактору. Метод HRA.
18. Аналіз прихованих дефектів і аналіз паразитних ланцюгів (SA – Sneak Analysis).

ПИТАННЯ ДО ІСПИТУ

1. Поняття ризику, його ймовірнісні характеристики. Суб’єкт та об’єкт ризику.

2. Функції ризику. Причини виникнення ризиків.

3. Взаємозв’язок понять «ризик» та «невизначеність».

4. Стратегії управління ризиком.

5. Кількісні методи оцінки ризику.

6. Об'єктивні критерії оцінки стохастичного ризику.

7. Середнє, дисперсія. Стохастичне домінування першого і другого порядку.

8. Суб'єктивні критерії оцінки стохастичного ризику.

9. Міра очікуваної корисності.

10. Суб'єктивні ймовірності. Теорія проспектів.

11. Ознаки класифікації та види ризиків.

12. Системні та внутрішні ризики підприємства. Виробничі, транспортні, фінансові, інвестиційні, комерційні (маркетингові) ризики, ризики у соціально-трудових відносинах.

13. Розмежування ризиків за економічними наслідками.

14. Стохастичні процеси з незалежними приростами.

15. Система та організація управління ризиками. Поняття ризик-менеджменту.

16. Етапи процесу управління ризиком: збір інформації за аспектами ризику, якісний аналіз, методи кількісного оцінювання ризику, розробка заходів щодо оптимізації ризику, прийняття чи відхилення ризикового рішення. Правила управління ризиками.

17. Дисперсійний метод оцінювання ризику, основні показники варіації.

18. Імовірнісний метод оцінювання ризику.

19. Визначення ймовірності досягнення бажаного результату за інтегральною функцією щільності розподілу ймовірностей.

20. Сутність та групування якісних методів оцінювання ризику.

21. Метод мозкового штурму.

22. Загальна характеристика експертних процедур, їх використання для розрахунку рівня ризику проєкту.

23. Перевірка узгодженості дій експертів на основі розрахунку коефіцієнта конкордації. Методи асоціацій та аналогій.

24. Використання матриць в оцінюванні альтернативних рішень.

25. Критерії прийняття рішень в умовах високої ентропії: максимінний критерій Вальда, мінімаксний критерій Севіджа, критерій недостатнього обґрунтування Лапласа, критерій узагальненого песимізму-оптимізму Гурвіца.

26. Методологічні засади теорії ігор.

27. Класифікація ігор. Чиста та змішана стратегії. Засоби розв’язання завдань теорії ігор.

28. Оптимальна поведінка в умовах специфічних видів ризику.

29. Методи уникнення ризику.

30. Характеристика основних засобів регулювання ризику: резервування засобів, система вибору клієнтів, залучення зовнішніх джерел, здобуття додаткової інформації, диверсифікація, лімітування, біржове хеджування ризиків.

31. Міжнародний стандарт ISO 31000.

32. Сутність страхування, суб’єкти та об’єкти страхування.

33. Особисте, майнове страхування та страхування відповідальності.

34. Критерії прийняття рішень щодо страхування ризиків.

35. Поняття диверсифікації, сутність політики диверсифікації підприємства, поняття кореляції активів.

36. Причини диверсифікації підприємницької діяльності. Переваги та недоліки диверсифікації.

37. Загальна характеристика використання системного аналізу системи "людина - техніка - середовище".

38. Методичні засади визначення небезпечності об'єктів та процесів.

39. Надійність технічних систем. Надійність оператора.

40. Фактори надійності оператора. Фактори середовища. Ергономічні фактори.

41. Міжнародний стандарт ISO 31000 в аналізі системи "людина - техніка - середовище".

ФОРМИ ПІДСУМКОВОГО КОНТРОЛЮ УСПІШНОСТІ СТУДЕНТІВ

Поточний контроль здійснюється під час проведення практичних занять і має на меті перевірку рівня засвоєння студентом вивченої теми.

При поточному контролі оцінці підлягають: рівень теоретичних знань та вміння працювати з науковою літературою, знання матеріалу, продемонстрованого у виконаних завданнях самостійної роботи; активність та систематичність роботи на заняттях; результати виконання домашніх завдань, тестів, експрес-опитувань, доповідей, рефератів тощо.

Форми проведення поточного контролю: усне опитування студентів, розв’язування практичних завдань, тестові завдання, доповіді, реферати.

Проміжний контроль проводиться після вивчення відповідних тем або блоку тем з метою з`ясування ступеню засвоюваності студентами відповідного об’єму опрацьованого та вивченого матеріалу та подальшої оцінки рівня отриманих знань. Форми проведення проміжного контролю: контрольна робота, тестове опитування, співбесіда (усне спілкування).

Підсумковий контроль здійснюється у формі іспиту.

КРИТЕРІЇ ОЦІНЮВАННЯ

При використанні форми контролю у вигляді заліку враховується поточна, зокрема самостійна робота, наукова діяльність студента. Крім того, студент має надати відповідь на залікове запитання. Оцінка рівня знань виконується за принципом "відповідь вірна" або "відповідь невірна". При вірній відповіді виставляється оцінка "зараховано", при невірній, неповній відповіді виставляється оцінка "не зараховано".

Оцінка з національної шкали переводиться у 100-бальну та шкалу ECTS у відповідності до результатів навчальної успішності студента протягом семестру.

СХЕМА НАРАХУВАННЯ БАЛІВ (СКЛАДОВІ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ)

Пункт оцінки	% підсумкової оцінки або максимальна оцінка в балах	Групове чи індивідуальне оцінювання
Поточний контроль, разом, у т.ч.:	**50**	
доповіді та повідомлення на семінарах	25	Групове та індивідуальне
виконання письмових індивідуальних завдань, рефератів, контрольних робіт	15	Індивідуальне
опитування на семінарських заняттях	10	Групове та індивідуальне
Підсумковий контроль, разом, у т.ч.:	**50**	
письмова компонента	25	Індивідуальне
усна компонента	25	Індивідуальне

ШКАЛА ЗА ECTS

<table>
<tr><th rowspan="2">Сума балів</th><th rowspan="2">Оцінка за 7-бальною шкалою</th><th colspan="2">Оцінка за 4-бальною шкалою</th></tr>
<tr><th>екзамен</th><th>залік</th></tr>
<tr><td>A</td><td>90-100</td><td>Відмінно</td><td rowspan="5">зараховано</td></tr>
<tr><td>B</td><td>82-89</td><td rowspan="2">Добре</td></tr>
<tr><td>C</td><td>75-81</td></tr>
<tr><td>D</td><td>67-74</td><td rowspan="2">Задовільно (достатньо)</td></tr>
<tr><td>E</td><td>60-66</td></tr>
<tr><td>Fx</td><td>35-59</td><td rowspan="2">Незадовільно з можливістю повторного складання</td><td rowspan="2">не зараховано</td></tr>
<tr><td>F</td><td>1-34</td></tr>
</table>

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

ОСНОВНА

1) International Organization for Standardization, 2009. 29 p.
2) Essentials of Risk Management. (Ed by Head G.L.) 1994.
3) Executive Information Systems, Inc. White Paper No. Three, March 27, 1997.
4) Data Warehouses and Marts: A Dynamic View, by Joseph M. Jorion P. Value at risk. - 2000.
5) Chapman C., Ward S. Project risk management: processes, techniques, and insights. - Wiley, 2003.
6) Saunders A., Cornett M. M., McGraw P. A. Financial institutions management: A risk management approach. - New York, NY, USA : McGraw-Hill, 2006.
7) McNeil A. J. et al. Quantitative risk management: Concepts, techniques and tools. - Princeton : Princeton university press, 2005. Т. 3.
8) Power M. The risk management of everything // The Journal of Risk Finance. 2004. V. 5. №. 3. P. 58-65.
9) Гуменюк В. Я. Управління ризиками : навч. посіб. / В. Я. Гуменюк, Г. Ю. Міщук, О. О. Олійник. – Рівне : НУВГП, 2009. 156 с.
10) Машина Н.І. Ризик і методи його вимірювання: Навчальний посібник. - К.: ЦНЛ, 2003. 188 с.
11) Богоявленский С. Б. Теоретические и практические аспекты принятия решений в условиях неопределенности и риска. Учеб. пособие – Санкт-Петербург : Изд-во СПбГЭУ. 2014. 119 с.
12) Антипенко І. В. Онтологічна основа феномену ризику в сучасних методологічних підходах зарубіжної ризикології. Державне управління: удосконалення та розвиток. 2019. № 1. – URL: http://www.dy.nayka.com.ua/?op=1&z=1371 (дата звернення: 04.02.2021). DOI: 10.32702/2307-2156-2019.1.26
13) Василенко М.Д. Кібер-ризики в муніципальному господарстві в період пандемії: збитки та боротьба за кібербезпеку. Наук.-техн. зб. "Комунальне господарство міст". Серія: технічні науки та архітектура. Харків, 2020. Вип. 3 (156). С. 80-87 (в співавторстві). 125 спец.
14) Василенко М.Д. Право в теорії ризиків: ґенеза ризиків від правової до інформаційної складових (інституційний підхід). Юридичний вісник. – О. : ВД «Гельветика». 2019. № 4. С. 43-51 (в співавторстві).
15) Василенко М.Д. Розумне місто» в контексті кібербезпеки: інциденти, ризики, загрози. Науково-технічний зб. «Комунальне господарство міст». Серія: технічні науки та архітектура. Харків, 2020. Вип. 4 (157). С. 184-191 (в співавторстві). 125 спец.

16) Василенко М.Д. Кібербезпека в проявах ризиків у період пандемії: стан та генеза. Вісник Черкаського державного технологічного університету: технічні науки. 2020. №3. С. 30-39. (в співавторстві). 125 спец.
17) Василенко М.Д. Ризики: правова та інформаційна безпека. Правове життя сучасної України : у 3 т. : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 15 трав. 2020 р.) / відп. ред. М. Р. Аракелян. – Одеса : Видавничий дім «Гельветика», 2020. Т. 2. С. 371-374 (в співавторстві).
18) Василенко М.Д. Деякі питання ризиків (інформаційних ризиків) в контексті соціальної інженерії. Безпека та виклики сучасності: ризики та кібербезпека в період пандемії безпека в сучасному світі : матеріали II Всеукраїнської науково-практ. конф. (м. Одеса, 20 листоп. 2020 р.) / за ред. О. В. Дикого. Одеса : Видавничий дім «Гельветика», 2020. С. 53-58 (в співавторстві).

ДОПОМІЖНА

1) Стасюк О. І. та ін. Сучасні стенографічні методи захисту інформації / О. І. Стасюк та ін. // Захист інформації. 2011. Т. 13. № 1 (50). С. 56–63.
2) Ризик-менеджмент суб'єктів енергетичного ринку як складова механізму забезпечення енергетичної безпеки : монографія / Н. В. Караєва, І. І. Гусєва, В. О. Бараннік, А. О. Савицька. К. : Софія-А, 2012. 256 с.
3) Гранатуров В.М. Риск. Сущность, методы измерения, пути снижения. – М.: Дело и Сервис, 2010. 208 с.
4) Балдин К.В., Воробьев С. Н. Модели и методы управления рисками. – М.: МПСИ, МОДЭК, 2009. 432 с.
5) Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: Монографія. – К.: НАУ, 2013. 432 с.
6) Бурячок В.Л., Толубко В.Б., Хорошко В. О., Толюпа С.В. Інформаційна і кібербезпека: соціотехнічний аспект: Підручник. – К.: ДУТ, 2015. 288 с.
7) Бурячок В.Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: Підручник. – К.: ДУТ, 2015. 449 с.
8) Василевич Л.Ф. Юртин І.І. Прийняття рішень за умов конфлікту та невизначеності середовища. Навчальний посібник – К. : Київ. ун-т ім.. Б. Грінченка. 2013. 128с.
9) Henry K. Risk management and analysis / Kevin Henry // Information Security Management Handbook / Edited by Harold F. Tipton, Micki Krauze. – 6th edition. – Boca Raton : Auerbach Publications, 2017. Part 1, Section 1.4, Ch. 28. P. 321-329.
10) Landoll D. The security risk assessment handbook: a complete guide for performing security risk assessments / Douglas J. Landoll. – Boca Raton: Auerbach

Publications, 2016. 504 p.
11) Замула О. А. Аналіз міжнародних стандартів в галузі оцінювання ризиків інформаційної безпеки / О. А. Замула, В. І. Черниш // Системи обробки інформації: збірних наукових праць. – Х.: ХУ ПС, 2014. Вип. 2(92). С. 53-56.
12) Замула А. А., Северинов А. В., Корниенко М. А. Анализ моделей оценки рисков информационной безопасности для построения системы защиты информации. Наука і техніка Повітряних Сил Збройних Сил України, 2017, № 2(15). С. 47-52.
13) Войціховський, А. (2020). Інформаційна безпека як складова системи національної безпеки (міжнародний і зарубіжний досвід). Вісник Харківського національного університету імені В. Н. Каразіна. Серія «Право», (29), 281-288. https://doi.org/10.26565/2075-1834-2020-29-38
14) Правові засади інформаційної безпеки України: монографія / Біленчук П.Д. [та ін.] ; за ред. П.Д. Біленчука. Харків, 2018. 289 с.
15) Sosnovska, O., & Dedenko, L. (2019). Ризик-менеджмент як інструмент забезпечення стійкого функціонування підприємства в умовах невизначеності. Європейський науковий журнал Економічних та Фінансових інновацій, 1(3), 70-79. https://doi.org/10.32750/2019-0106

ІНФОРМАЦІЙНІ РЕСУРСИ

1) http://www.it.inf.od.ua – сайт кафедри інформаційних технологій, на якому розміщено робочі матеріали з курсу
2) Державна служба спеціального зв'язку та захисту інформації України. URL: www.dsszzi.gov.ua.
3) Методи інформаційного захисту простору. Інформаційна безпека України URL: http://ua.textreferat.com/referat-7471.html
4) Інформаційна безпека при роботі у мережі Інтернет URL: https://khm.gov.ua/uk/content/informaciyna-bezpeka-pry-roboti-u-merezhi-internet
5) Марутян Р.Р. Рекомендації щодо вдосконалення політики забезпечення інформаційної безпеки України URL: http://www.dsaua.org/index.php?option=com_content&view=article&id=198%3A2014-08-13-12-55-48&catid=66%3A2010-12-13-08-48-53&Itemid=90&lang=uk
6) Медвідь Ф. Інформаційна безпека України: виклики та загрози URL: https://nato.ru.if.ua/journal/2009-2-28.pdf.
7) Електронний журнал науково-дослідного інституту інформатики і права URL: http://ippi.org.ua/jpage/45
8) Стаття 361-1 Карного Кодексу України. Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут URL: https://web.archive.org/web/20080228124933
9) Огляд різноманітних шкідливих програмних засобів [Електронний ресурс]. — Режим доступу: https://securelist.com

10) Українська антивірусна лабораторія. / Єдиний український розробник інноваційних технологій кіберзахисту URL: https://zillya.ua/antivirusnalaboratoriya
11) Классификация стенографических методов URL: http://networkjournal.mpei.ac.ru/cgibin/main.pl?l=ru&n=9&pa=13&ar=1. — Назва з екрану
12) Внедрение информации в аудио сигнал URL: http://crypts.ru/vnedrenieinformacii-modifikaciej- azyaudiosignala.html. — Назва з екрану
13) Моделювання інформаційно-психологічних операцій в соціотехнічних системах URL: http://antibotan.com/file.html7work id=528730
14) http://dspace.onua.edu.ua – eNUOLAIR – депозитарій (архів) НУ ОЮА

ЗМІСТ

Навчальне видання

Микола Дмитрович Василенко

Валерія Миколаївна Слатвінська

ТЕОРІЯ РИЗИКІВ

Навчально-методичні рекомендації

(для студентів факультету кібербезпеки та інформаційних технологій)

Українською мовою

Підписано до друку ..2021.

Формат 60х84/16. Ум-друк. арк. 1,9.

Наклад 100 прим. Зам. № .

Видано і віддруковано в ПП «Фенікс»

(Свідоцтво суб'єкта видавничої справи ДК № 1044 від 17.09.02).

Україна, м. Одеса, 65009, вул. Зоопаркова, 25.

Тел. +38 050 7775901 +38 048 7959160

e-mail: fenix-izd@ukr.net

www.feniksbooks.com