МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

**ЗАТВЕРДЖУЮ**

В.о. декана ФКІТ
Ігор ЯКИМЕНКО

_____
«___» _____ 2023 р.

**ЗАТВЕРДЖУЮ**

В.о. проректора з науково-педагогічної роботи
Віктор ОСТРОВЕРХОВ

_____
«___» _____ 2023 р.

# РОБОЧА ПРОГРАМА

з дисципліни «Оцінка та управління ризиками»
ступінь вищої освіти – бакалавр
галузь знань - 12 Інформаційні технології
спеціальність – 125 Кібербезпека
освітньо-професійна програма – Кібербезпека

Кафедра кібербезпеки

| Форма навчання | Курс | Семестр | Лекції (год.) | Лабор. роботи (год.) | ІРС (год.) | Тренінг, КПІЗ (год.) | Самост. робота студ. (год.) | Разом (год.) | Екзам. (сем.) |
|---|---|---|---|---|---|---|---|---|---|
| Денна | 3 | 5 | 28 | 28 | 3 | 8 | 83 | 150 | 5 |

Тернопіль – 2023

Робоча програма розроблена на основі освітньо-професійної програми підготовки бакалавра галузі знань 12 «Інформаційні технології» за спеціальністю 125 «Кібербезпека», затвердженої Вченою радою ЗУНУ (протокол № 9 від 26.05.2021 р.).

Робочу програму склав завідувач кафедри кібербезпеки, д.т.н., професор Василь Яцків

Робоча програма затверджена на засіданні кафедри кібербезпеки, протокол № 1 від 28.08.2023 р.

Завідувач кафедри кібербезпеки Василь ЯЦКІВ

Розглянуто та схвалено групою забезпечення спеціальності 125 «Кібербезпека та захист інформації», протокол №1 від 30.08.2023 р.

Голова групи
забезпечення спеціальності Василь ЯЦКІВ

Гарант ОП Ігор ЯКИМЕНКО

## СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

### 1. Опис дисципліни «Оцінка та управління ризиками»

| Дисципліна «Оцінка та управління ризиками» | Галузь знань, спеціальність, СВО | Характеристика навчальної дисципліни |
|---|---|---|
| Кількість кредитів ECTS – 5 | Галузь знань<br>12 Інформаційні технології | **Статус дисципліни:**<br>обов'язкова<br><br>**Мова навчання**:<br>українська |
| Кількість залікових модулів – 4 | Спеціальність 125 «Кібербезпека» | Рік підготовки:<br>Денна –3<br>Семестр:<br>Денна – 5 |
| Кількість змістових модулів – 3 | Ступінь вищої освіти – бакалавр | Лекції: 28 год.<br>Лабораторні заняття:28 год. |
| Загальна кількість годин – 150 | | Самостійна робота: 83 год.<br>Тренінг, КПІЗ: 8 год.<br>Індивідуальна робота: 3 год. |
| Тижневих годин –11,<br>з них аудиторних – 4 | | Вид підсумкового контролю – екзамен |

### 2. Мета й завдання вивчення дисципліни "Оцінка та управління ризиками"

#### 2.1. Мета дисципліни

**Мета курсу «Оцінка та управління ризиками»** полягає у формуванні у майбутніх спеціалістів умінь та компетенцій для забезпечення ефективної оцінки та управління кіберризиками, навчити їх застосуванню методів та засобів оцінки та управління ризиками в умовах широкого використання сучасних інформаційних технологій.

Вивчення курсу "Оцінка та управління ризиками» передбачає наявність систематичних та ґрунтовних знань із суміжних курсів («Теорія ймовірностей та математична статистика», „Основи кібербезпеки", «Дискретна математика», «Математичний аналіз»), а також цілеспрямованої роботи на лекційних та лабораторних заняттях, самостійної роботи студентів.

#### 2.2. Завдання вивчення дисципліни

В результаті вивчення курсу „Оцінка та управління ризиками " студенти повинні:

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

– знати принципи побудови алгоритмів оцінки ризиків та управління ними у кібербезпеці, основних стандартів оцінки ризиків та їх використання в задачах захисту інформації;

– використовувати основний математичний апарат та закони оцінки та управління ризиками у професійній діяльності;

– вміти використовувати програмні засоби, які реалізують основні функції оцінки та управління ризиками;

– програмно реалізовувати основні алгоритми оцінки та управління ризиками для вирішення типових задач захисту інформації;

– проектувати різного рівня системи оцінки та управління ризиками;

– вміння використовувати методи та засоби оцінки та управління ризиками у кібербезпеці.

Завдання лекційних занять

Мета проведення лекцій полягає у тому, щоб ознайомити студентів із головними питаннями курсу «Оцінки та управління ризиками». Завдання проведення лекцій полягає у: викладенні студентам у відповідності з програмою та робочим планом основних питань курсу «Оцінка та управління ризиками» та формуванні у студентів цілісної системи теоретичних знань з курсу «Оцінка та управління ризиками».

Завдання проведення лабораторних занять

Мета проведення лабораторних занять полягає у тому, щоб виробити у студентів практичні навички використання теоретичного матеріалу. Завдання проведення лабораторних занять полягає у глибшому засвоєнні та закріпленні теоретичних знань, одержаних на лекціях.

**2.3. Найменування та опис компетентностей, формування котрих забезпечує вивчення дисципліни:**

– здатність до пошуку, оброблення та аналізу інформації.

– здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки;

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

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

–

**2.4. Передумови для вивчення дисципліни**

Вивчення курсу «Оцінка та управління ризиками» передбачає наявність систематичних та ґрунтовних знань із суміжних курсів, таких як «Вища математика», «Теорія ймовірності та математична статистика», «Дискретна математика», «Основи кібербезпеки», «Основи програмування».

**2.5. Результати навчання**

- використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності;

- 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;

- розробляти моделі загроз та порушника;

- аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки;

- 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.

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

- проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах;

- вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.

- застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик орієнтованому контролі доступу до інформаційних активів.

- здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно

телекомунікаційних системах.

## 3. Програма навчальної дисципліни «Оцінка та управління ризиками»

### *Змістовий модуль 1. Поняття ризику, методи його оцінки. Класифікація ризиків.*

**Тема 1.** Концепції оцінки ризику. Проблеми оцінки ризиків Управління ризиками. Поняття ризику. Предмет, методи і задачі дисципліни.

**Тема 2.** Ідентифікація активів. Апаратні засоби. Програмні активи. Інформаційні активи. Бізнес активи. Реєстр активів.

**Тема 3.** Ідентифікація загрози. Модель загрози STRIDE. Типи загроз. Джерела інформації. Ідентифікація контролю. Контроль уникнення. Контроль страхування. Контроль уразливості. Контроль реагування.

**Тема 4.** Ідентифікація вразливості. Категорії вразливості. Національна та загальна база даних вразливостей. Система оцінки вразливостей.

**Тема 5.** Підходи до оцінки ризиків. Кількісна та якісна оцінка ризику. Простий робочий лист аналізу ризиків. Факторний аналіз інформаційного ризику.

**Тема 6.** Оцінка імовірності ризику. Частота подій загрози. Оцінка вразливості. Частота втрат. Оцінка впливу ризику. Оцінка первинного збитку. Оцінка вторинних збитків. Вплив ризиків на бізнес.

**Тема 7.** Визначення ризику. Визначення потенційних загроз Перелік загроз. Зменшення небажаної упередженості в міркуваннях загроз. Перелік загроз за допомогою SWOT-аналізу. Використання аналізу прогалин для виявлення загроз. Перелік технічних загроз.

### *Змістовий модуль 2. Кількісна оцінка ризиків у кібербезпеці*

**Тема 8.** Методологія оцінки ризику. Оцінка наслідків. Оцінка ймовірності інциденту. Вимірювання рівня ризику.

**Тема 9.** Обробка ризиків. Зниження ризику. Утримання ризику. Уникнення ризику. Передача ризику. Методи оцінки ризиків. Структура оцінки інформаційних ризиків. Процес оцінки інформаційних ризиків

**Тема 10.** Концепції управління ризиками. Цілісне управління ризиками. Політика управління ризиками інформаційних систем. Команда управління ризиками. Процес управління ризиками. Огляд вразливостей і загроз. Виявлення загроз і вразливостей.

**Тема 11.** Відповідь на ризики. Загальний ризик проти залишкового ризику. Вибір та впровадження контрзаходів. Типи елементів керування. Контрольні оцінки.

**Тема 12.** Моніторинг ризиків. Моніторинг ефективності. Моніторинг змін. Моніторинг відповідності. Звітність про ризики. Постійне покращення.

**Тема 13.** Управління ризиками ланцюга постачання. Постачальники вгору та вниз за течією. Ризики, пов’язані з обладнанням, програмним забезпеченням та послугами. Інші ризики третіх сторін. Мінімальні вимоги безпеки. Угоди про рівень обслуговування.

**Тема 14.** Безперервність бізнесу. Стандарти та передовий досвід. Перетворення BCM (Business Continuity Management) в програму безпеки підприємства. Аналіз впливу на бізнес.

**4. Структура залікового кредиту дисципліни «Оцінка та управління ризиками»**

| | Кількість годин | | | | | |
|---|---|---|---|---|---|---|
| | Лекції | Лабора-торні заняття | СРС | ІРС | Тренінг, КПІЗ | Контрольні заходи |
| *Змістовий модуль 1. Поняття ризику, методи його оцінки. Класифікація ризиків.* | | | | | | |
| Тема 1. Концепції оцінки ризику | 2 | - | 5 | | 4 | Поточне опитування |
| Тема 2. Ідентифікація активів | 2 | 2 | 6 | | | Поточне опитування |
| Тема 3. Ідентифікація загрози | 2 | 2 | 6 | 2 | | Поточне опитування |
| Тема 4. Ідентифікація вразливості | 2 | 2 | 6 | | | Поточне опитування |
| Тема 5. Підходи до оцінки ризиків | 2 | 2 | 6 | | | Поточне опитування |
| Тема 6. Оцінка імовірності ризику | 2 | 4 | 6 | | | Поточне опитування |
| Тема 7. Визначення ризику | 2 | 4 | 6 | | | Поточне опитування |
| *Змістовий модуль 2. Кількісна оцінка ризиків у кібербезпеці* | | | | | | |
| Тема 8. Методологія оцінки ризику | 2 | | 6 | | 4 | Поточне опитування |
| Тема 9. Обробка ризиків | 2 | 4 | 6 | | | Поточне опитування |
| Тема 10. Концепції управління ризиками | 2 | | 6 | | | Поточне опитування |
| Тема 11. Відповідь на ризики | 2 | 2 | 6 | | | Поточне опитування |
| Тема 12. Моніторинг ризиків | 2 | 2 | 6 | 1 | | Поточне опитування |
| Тема 13. Управління ризиками ланцюга постачання. | 2 | 4 | 6 | | | Поточне опитування |
| Тема 14. Безперервність бізнесу | 2 | - | 6 | 1 | | Поточне опитування |
| **Разом** | 28 | 28 | 83 | 3 | 8 | |

**5. Тематика лабораторних занять.**

**Лабораторне заняття №1**

**Тема:** Міжнародні стандарти та рекомендації для оцінки та управляння ризиками.
Мета: Дослідити нормативно-правові акти у сфері оцінки та управляння ризиками.
Література: 1-15.

**Лабораторне заняття № 2**

**Тема:** Структура систем управління ризиками у кібербезпеці
**Мета:** Вивчити та дослідити структуру систем управління ризиками у кібербезпеці
Література: 1-15.

**Лабораторне заняття №3**

**Тема:** Ідентифікація ризиків підприємств критичної інфраструктури
**Мета:** Вивчити та дослідити методи ідентифікації ризиків підприємства
Література: 1-15.

**Лабораторне заняття №4**

**Тема:** Оцінка ризиків інформаційної безпеки згідно стандарту ISO/IEC 27001:2013.
**Мета:** Вивчити та дослідити методику оцінки ризиків інформаційної безпеки згідно стандарту ISO/IEC 27001.

Література: 1-15.

**Лабораторне заняття №5**

**Тема:** Оцінка ризиків інформаційної безпеки з використанням програмного комплексу "Гриф" компанії Digital Security

**Мета:** Вивчити та здійснити оцінку ризиків інформаційної безпеки з використанням програмного комплексу "Гриф" компанії Digital Security

Література: 1-15.

**Лабораторне заняття № 6**

**Тема:** Оцінка ризиків Інтернет- речей.

**Мета:** Визначення ризику Інтернет- речей.

Література: 1-15.

**Лабораторне заняття № 7**

**Тема:** Аналіз журналів подій для визначення ризиків

**Мета:** Навчитися використовувати журнали подій для визначення ризиків.

Література: 1-15.

**Лабораторне заняття № 8**

**Тема:** Інструменти управління ризиками

**Мета:** Навчитися використовувати інструменту з відкритим кодом для управління ризиками

Література: 1-15.

**Лабораторне заняття № 9**

**Тема:** Використання інструменту управління ризиками LiteGRC

**Мета:** Навчитися використовувати інструмент LiteGRC для управління ризиками

Література: 1-15.

**Лабораторне заняття № 10**

**Тема:** Фреймворки для оцінка ризиків Інтернет-речей.

**Мета:** Вивчити та дослідити фреймворки для оцінка ризиків Інтернет-речей.

Література: 1-15.

**6. Комплексне практичне індивідуальне завдання (КПІЗ).**

Індивідуальне завдання з курсу “Оцінка та управління ризиками” виконується самостійно студентом на основі сформованого завдання. КПІЗ охоплює основні теми курсу. Метою виконання КПІЗ є оволодіння навиками оцінювання ступеня ризику при вирішенні конкретних задач кібербезпеки. Студенти повинні дослідити та застосувати відповідні методи та алгоритми за одним із варіантів:

1. Парето-оптимальні рішення.
2. Визначення коефіцієнтів пріоритетності часткових критеріїв рішень у кібербезпеці.
3. Нормалізація значень часткових критеріїв оцінки ризиків у кібербезпеці.
4. Загальний адитивний критерій оцінки ризиків у кібербезпеці.
5. Метод послідовних поступок.
6. Диверсифікація як спосіб зниження ризику у кібербезпеці.
7. Недиверсифікований ризик у кібербезпеці.
8. Способи зниження ризику у кібербезпеці.
9. Хеджування як способ зниження ризику у кібербезпеці.
10. Вартість, час, ризик та інформація.

11. Нечітка інформація в задачах оцінки ризиків у кібербезпеці.
12. Нечітка множина, величина, число, лінгвістична змінна.
13. Логічні операції над нечіткими множинами.
14. Арифметичні операції над нечіткими величинами.
15. Порівняння нечітких величин. Методи дефазіфікації.
16. Порівняння дискретних нечітких множин.
17. Нечітке відношення переваги.
18. Застосування нечітких величин в задачах кібербезпеки.
19. Системи підтримки прийняття рішень у кібербезпеці.
20. Психолінгвістичні аспекти оцінки ризиків у кібербезпеці.
21. Проактивність. Визначення кінцевої цілі. Пріоритетність.
22. Особливості багатоособових рішень при оцінці ризиків у кібербезпеці. Метод Кодерса.
23. Метод Борде.
24. Показники якості прогнозування у кібербезпеці.
25. Наївні методи прогнозування у кібербезпеці.
26. Прогнозування методом усереднення.
27. Прогнозування методом ковзаючого усереднення.
28. Прогнозування методом експоненціального згладжування.
29. Циклічність та сезонність у прогнозуванні в задачах кібербезпеки.
30. Експертне прогнозування в задачах прийняття рішень. Метод Дельфі.

Виконання КПІЗ є одним із обов'язкових складових модулів залікового кредиту.

**7. Самостійна робота та дуальна освіта**

| № п/п | Тематика |
|---|---|
| 1 | Методологічні основи оцінки ризиків у кібербезпеці. |
| 2 | Загальна формальна математична модель оцінки ризиків у кібербезпеці. |
| 3 | Інформація та фактор часу при оцінці ризиків у кібербезпеці. |
| 4 | Прийняття рішень і ризик. Причини ризику. |
| 5 | Способи управління ризиком у кібербезпеці. |
| 6 | Принципи теорії оцінки ризиків у кібербезпеці. |
| 7 | Класифікація математичних моделей оцінки ризиків у кібербезпеці |
| 8 | Класифікація ризиків у кібербезпеці |
| 9 | Поняття системи в задачі оцінки ризиків у кібербезпеці. |
| 10 | Класифікація систем. |
| 11 | Властивості системи як об'єкта оцінки ризиків у кібербезпеці. |
| 12 | Синергетика в задачах оцінки ризиків у кібербезпеці. |
| 13 | Петлі зворотного зв'язку як сутність системи оцінки ризиків у кібербезпеці. |
| 14 | Побочні ефекти оцінки ризиків у кібербезпеці |
| 15 | Емерджентні властивості системи. |
| 16 | Ментальні моделі суб'єкта оцінки ризиків у кібербезпеці. |
| 17 | Сила парадигми в процесі оцінки ризиків у кібербезпеці. |
| 18 | Системний підхід та системний аналіз при оцінці ризиків у кібербезпеці |
| 19 | Системній підхід до оцінки ризиків у кібербезпеці. |
| 20 | Системний аналіз як універсальна наукова методологія оцінки ризиків у кібербезпеці. |
| 21 | Математична модель задачі оцінки ризиків у кібербезпеці за умов багатокритеріальності. |
| 22 | Вибір показників та критеріїв ефективності оцінки ризиків у кібербезпеці. |

**8. Організація та проведення тренінгу з дисципліни «Оцінка та управління ризиками»**

| № п/п | Вид роботи | Порядок проведення тренінгу |
|---|---|---|
| 1 | Встановлення та налаштування програмного забезпечення | Підключення до веб-інтерфейсу OpenVAS |
| 2 | Сканування вразливостей за допомогою OpenVAS | Створіть нову мету зі списком портів за замовчуванням<br>2. Створіть нове завдання, використовуючи цю ціль із стандартною конфігурацією сканування<br>3. Запустіть сканування<br>4. Перемикайте перегляд на оновлення кожні 30 секунд, щоб ви могли відкинутися назад і спостерігати за ходом сканування |
| 3 | Виконання завдання | 1. Прочитайте інструкції та виконайте всі завдання.<br>2. Використовуйте nmap, щоб просканувати ціль і знайти версію програмного забезпечення ОС і запущених служб (укажіть принаймні 3 запущені служби).<br>3. Використовуйте OpenVAS, щоб знайти дві вразливості цілі та коротко описати їх |

**9. Засоби оцінювання та методи демонстрування результатів навчання**

У процесі вивчення дисципліни “Оцінка та управління ризиками ” використовуються наступні методи оцінювання навчальної роботи студента:

– поточне опитування;
– підсумкове тестування за кожним змістовним модулем;
– оцінювання виконання лабораторних робіт;
– ректорська контрольна робота;
– комплексне практичне індивідуальне заняття (КПІЗ).
– екзамен.

**10. Критерії, форми поточного та підсумкового контролю**

Підсумковий бал (за 100 – бальною шкалою) з дисципліни «Оцінка та управління ризиками» визначається як середньозважена величина, в залежності від питомої ваги кожної складової залікового кредиту:

Для екзамену

| Заліковий модуль 1 | Заліковий модуль 2 | Заліковий модуль 3 | Заліковий модуль 4 |
|---|---|---|---|
| 20% | 20% | 20% | 40% |
| 1. Усне опитування на заняттях – max 21 балів.<br>2. Письмова робота – max 54 балів.<br>3. Практичне завдання – max 25 балів | 1. Усне опитування на заняттях – max 21 балів.<br>2. Письмова робота – max 54 балів.<br>3. Практичне завдання – max 25 балів | 1. Підготовка КПІЗ – max 30 балів.<br>2. Захист КПІЗ – max 40 балів.<br>3. Оцінка за тренінг – max 30 балів | 1. Розв’язання 20 тестів по 3 бали = max 60 балів.<br>2. Практичне завдання = max 40 балів |

**Шкала оцінювання:**

| За шкалою ЗУНУ | За національною шкалою | За шкалою ECTS |
|---|---|---|
| 90-100 | відмінно | **A** (відмінно) |
| 85-89 | добре | **B** (дуже добре) |
| 75-84 | | **C** (добре) |
| 65-74 | задовільно | **D** (задовільно) |
| 60-64 | | **E** (достатньо) |
| 35-59 | незадовільно | **FX** (незадовільно з можливістю повторного складання) |
| 1-34 | | **F** (незадовільно з обов'язковим повторним курсом) |

**11. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна**

| № | Найменування | Номер теми |
|---|---|---|
| 1 | Електронний варіант лекцій | 1-14 |
| 2 | Методичні вказівки до виконання практичних робіт (електронний варіант) | 1–14 |
| 3 | ПК Intel Core i3-540; монітор 19 Samsung; принтер лазерний Canon MF4570. | 1-14 |
| 4 | VirtualBox, Kali Linux, OpenVas, Metasploitable 2. | 1-14 |

## РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ


1. Лісовська Ю. Кібербезпека. Ризики та заходи. – К.: Кондор, 2019. – 272 с.
2. Свед М. Мислення за принципом Чорної скриньки. Як звести ризик до мінімуму. – К. КМ-БУКС, 2018. – 464 с.
3. Stallings, W. Effective Cybersecurity: Understanding and Using Standards and Best Practices. Addison-Wesley. 2019. – 893 p.
4. NIST. *Framework for Improving Critical Infrastructure Cybersecurity.* April 16, 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST. CSWP.04162018.pdf
5. Fagan M, Marron, J, Brady KG, Jr, Cuthill BB, Megas KN, Herold R (2021) IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-213A. https://doi.org/10.6028/NIST.SP.800-213A
6. Stine K, Quinn S, Witte G, Gardner R (2020) Integrating Cybersecurity and Enterprise Risk Management (ERM). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8286. https://doi.org/10.6028/NIST.IR.8286
7. Soni, Arun. *The Cybersecurity Self-Help Guide*. CRC Press, 2021.
8. Ulven, J.B.; Wangen, G. A Systematic Review of Cybersecurity Risks in Higher Education. *Future Internet,* 2021,*13*,39. https://doi.org/ 10.3390/fi13020039
9. ISO 31010 2019. Risk management -Risk assessment techniques. Management du risque -Techniques. – 268 p.
10. Wangen, G. *Quantifying and Analyzing Information Security Risk from Incident Data*; Graphical Models for Security; Albanese, M., Horne, R., Probst, C.W., Eds.; Springer International Publishing: Cham, Switzerland, 2019, pp. 129–154.
11. Radanliev P., et al. "Cyber Risk in IoT Systems." (2019).
12. Lee, In. "Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management." *Future Internet* 12.9, 2020: 157.
13. Wilhelmsen, Cheryl A., and Lee T. Ostrom. *Risk assessment: tools, techniques, and their applications*. John Wiley & Sons, 2019.
14. Fagan, Michael, et al. "IoT Device Cybersecurity Guidance for the Federal Government." *NIST Special Publication* 800 (2021): 213.
15. Burnap, Pete. "Risk Management & Governance Knowledge Area Issue." (2021). Version 1.1.1. https://www.cybok.org/media/downloads/Risk_Management_Governance_v1.1.1.pdf