**ЗАТВЕРДЖЕНО**
Вченою радою факультету
інформаційно-комп'ютерних технологій
31 серпня 2023 р., протокол № 5
Голова Вченої ради
Тетяна НІКІТЧУК

# РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ОК 26 «ТЕОРІЯ РИЗИКІВ ТА ЇЇ ЗАСТОСУВАННЯ В КІБЕРБЕЗПЕЦІ»

для здобувачів вищої освіти освітнього ступеня «бакалавр»
спеціальності 125 «Кібербезпека та захист інформації»
освітньо-професійна програма «Кібербезпека та захист інформаційя»
факультет інформаційно-комп'ютерних технологій
кафедра комп'ютерної інженерії та кібербезпеки

Схвалено на засіданні
кафедри комп'ютерної інженерії та
кібербезпеки
28 серпня 2023 р., протокол № 7
Завідувач кафедри
Андрій ЄФІМЕНКО
Гарант освітньо-
професійної програми
Андрій ЄФІМЕНКО


Розробник: кандидат технічних наук, завідувач кафедри комп'ютерної інженерії та кібербезпеки Єфіменко Андрій Анатолійович, доктор педагогічних наук, професор кафедри комп'ютерної інженерії та кібербезпеки Семенець Сергій Петрович


Житомир
2025-2026 н.р.

# 1. Опис навчальної дисципліни

| Найменування показників | Галузь знань, напрям підготовки, освітній ступінь | Характеристика навчальної дисципліни |
|---|---|---|
| | | денна форма навчання |
| Кількість кредитів - 3 | *Галузь знань*<br>12 «Інформаційні технології» | нормативна |
| Модулів – 1 | *Спеціальність*<br>125 «Кібербезпека та захист інформації» | Рік підготовки: |
| Змістових модулів – 4 | | 3-й |
| | | Семестр |
| Загальна кількість годин - 90 | | 6-й |
| | | |
| Тижневих годин для денної форми навчання:<br>аудиторних - 3<br>самостійної роботи – 2,6 | *Освітній ступінь*<br>«бакалавр» | Лекції |
| | | 16 год. |
| | | Практичні |
| | | __ |
| | | Лабораторні |
| | | 32 год. |
| | | Самостійна робота |
| | | 42 год. |
| | | Вид контролю: екзамен |

Співвідношення кількості годин аудиторних занять до самостійної та індивідуальної роботи становить:

для денної форми навчання – 53% аудиторних занять,

47% самостійної та індивідуальної роботи.

## 2. Мета та завдання навчальної дисципліни

**Метою** курсу «Теорія ризиків та її застосування в кібербезпеці» є оволодіння здобувачами вищої освіти компетентностями, що забезпечують ефективне управління ризиками в сучасних кіберсистемах, уможливлюють кваліфіковану оцінку ризиків в умовах широкого використання сучасних методів кібербезпеки.

Для досягнення мети вирішуються такі **завдання**:

- опанування майбутніми фахівцями фундаментальними поняттями і законами теорії ризиків;
- засвоєння здобувачами вищої освіти знань з основ теорії прийняття рішень, формування вмінь їх застосовувати в сучасних кіберсистемах;
- оволодіння майбутніми фахівцями принципами побудови алгоритмів оцінки ризиків у кібербезпеці, основними стандартами оцінки ризиків під час розв’язування задач захисту інформації;
- формування вмінь здобувачів вищої освіти використовувати математичний апарат для оцінки ризиків у майбутній професійній діяльності;
- формування здатностей майбутніх фахівців проектувати та впроваджувати системи оцінки ризиків у кібербезпеці.

Зміст навчальної дисципліни направлений на формування таких **компетентностей**, визначених стандартом вищої освіти зі спеціальності 125 «Кібербезпека та захисті інформації»:

**КЗ 5.** Здатність до пошуку, оброблення та аналізу інформації.

**КФ 2.** Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

**КФ 4.** Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

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

**КФ 12.** Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Отримані знання з навчальної дисципліни стануть складовими таких **програмних результатів** навчання за спеціальністю 125 «Кібербезпека та захисті інформації»:

**РН 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.

**РН 33.** Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.

**РН 46.** Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.

## 3. Програма навчальної дисципліни

### Модуль 1
### Змістовий модуль 1

### Основи теорії ризиків

**Тема 1. Поняття ризику**. Ризики в кібербезпеці (формулювання проблеми). Ризик та його етимологія. Становлення та розвиток теорії ризиків. Практична зумовленість теорії ризиків. Об'єктивний ризик. Суб'єктивна концепція ризику. Сума ризиків. Внутрішнє протиріччя ризику. Поняття ризику в безпеці життєдіяльності. Математична модель повного ризику. Обчислення ризиків як комплексного числа.

**Тема 2. Типологія ризиків.** Класифікація ризиків. Ризики техногенні (природні), індивідуальні та колективні, безумовно прийнятні, прийнятні та неприйнятні. Ризики короткострокові, середньострокові та довгострокові, разові, періодичні та постійні, локальні та глобальні. Ризики знехтувані, прийнятні, гранично допустимі та надмірні. Ризики в кібербезпеці. Класифікація за складниками ризику: об'єктивний і суб'єктивний. Класифікація за мірою прояву ризику: низький, нижче середнього, середній, вище середнього, високий, найвищий. Нульовий ризик. Сучасна концепція безпеки життєдіяльності.

### Змістовий модуль 2

### Застосування основ теорії ймовірностей в умовах ризиків

**Тема 3. Обчислення ризиків.** Задачі на знаходження класичного, статистичного, геометричного ризику.

**Тема 4. Основні теореми для обчислення ризиків.** Теореми додавання ризиків. Теореми множення ризиків. Ризик принаймні однієї події. Ризик виходу системи з ладу.

**Тема 5. Обчислення ризиків за основними формулами теорії ймовірностей.** Обчислення ризиків за формулою повної ймовірності та формулою Байеса. Ризики, що обчислюються за формулою Бернуллі. Ризики, що обчислюються за граничними теоремами в схемі Бернуллі. Використання числових характеристик випадкових величин (математичного сподівання,

дисперсії, середнього квадратичного відхилення) в умовах ризиків.

## Змістовий модуль 3

## Теорія і технологія прийняття рішень

**Тема 6. Прийняття рішення.** Концептуальні засади теорії прийняття рішень. Поняття «прийняття рішення», його широкий і вузький сенси. Інтуїтивне рішення. Технологія інтуїтивного рішення. Раціональне рішення. Технологія раціонального рішення та його оцінювання. Прийняття рішення в системі інформаційної безпеки.

**Тема 7. Моделі прийняття рішення.** Умови повної визначеності рішення. Основні моделі прийняття рішення. Класична модель. Поведінкова модель. Ірраціональна модель. Методи прийняття рішення. Метод суду. Метод комісій. Метод Делфі. Метод генерації ідей.

## Змістовий модуль 4

## Оцінка ризиків кібербезпеки

**Тема 8. Методи кількісної оцінки ризиків кібербезпеки.** Ризики в системі управління інформаційною безпекою. Аналіз та ідентифікація ризиків. Основні етапи забезпечення інформаційної безпеки. Оцінка ризиків інформаційної безпеки. Групи методів кількісної оцінки ризиків кібербезпеки

**Тема 9. Методики управління ризиками інформаційної безпеки.** Методика оцінки NIST 800-30. Методика CRAMM. Методика OCTAVE. Методи експертних оцінок ризиків: метод Дельфі, метод бальної оцінки ризику. Якості експерта. Вимоги до експертної інформації. Коефіцієнт конкордації Кендала. Вимоги до інформаційної безпеки. Перелік загроз і вразливостей. Визначення кількісного значення комплексного інформаційного ризику.

# 4. Структура (тематичний план) навчальної дисципліни

| Змістові модулі і теми | Кількість годин | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | денна форма | | | | заочна форма | | | |
| | усього | лекції | лабораторні | самостійна робота | усього | лекції | практичні | самостійна робота |
| **Модуль 1** | | | | | | | | |
| **Змістовий модуль 1. Основи теорії ризиків** | | | | | | | | |
| Тема 1. Поняття ризику | 7 | 1 | 2 | 4 | | | | |
| Тема 2. Типологія ризиків | 11 | 1 | 2 | 8 | | | | |
| ***Разом за змістовий модуль 1*** | **18** | **2** | **4** | **12** | | | | |
| **Змістовий модуль 2. Застосування основ теорії ймовірностей в умовах ризиків** | | | | | | | | |
| Тема 3. Обчислення ризиків | 12 | 2 | 4 | 6 | | | | |
| Тема 4. Основні теореми для обчислення ризиків | 10 | 2 | 4 | 4 | | | | |
| Тема 5. Обчислення ризиків за основними формулами теорії ймовірностей | 10 | 2 | 4 | 4 | | | | |
| ***Разом за змістовий модуль 2*** | **32** | **6** | **12** | **14** | | | | |
| **Змістовий модуль 3. Теорія і технологія прийняття рішень** | | | | | | | | |
| Тема 6. Прийняття рішення | 10 | 2 | 4 | 4 | | | | |
| Тема 7. Моделі прийняття рішення | 10 | 2 | 4 | 4 | | | | |
| ***Разом за змістовий модуль 3*** | **20** | **4** | 8 | **8** | | | | |
| **Змістовий модуль 4. Оцінка ризиків кібербезпеки** | | | | | | | | |
| Тема 8. Методи кількісної оцінки ризиків кібербезпеки | 10 | 2 | 4 | 4 | | | | |
| Тема 9. Методики управління ризиками інформаційної безпеки | 10 | 2 | 4 | 4 | | | | |
| ***Разом за змістовий модуль 4*** | **20** | **4** | **8** | **8** | | | | |
| **ВСЬОГО** | **90** | **16** | **32** | **42** | | | | |

## 5. Теми лабораторних занять

| № з/п | Назва теми | Кількість годин |
|---|---|---|
| | | денна форма |
| 1 | Поняття ризику | 4 |
| 2 | Обчислення ризиків | 4 |
| 3 | Основні теореми для обчислення ризиків | 4 |
| 4 | Обчислення ризиків за основними формулами теорії ймовірностей | 4 |
| 5 | Прийняття рішення | 4 |
| 6 | Моделі прийняття рішення | 4 |
| 7 | Методи кількісної оцінки ризиків кібербезпеки | 4 |
| 8 | Методики управління ризиками інформаційної безпеки | 4 |
| **РАЗОМ** | | **32** |

## 6. Завдання для самостійної роботи

**Тема 1. Поняття ризику**

1. Проблема ризиків у кібербезпеці (формулювання проблеми). Кіберзахист і його забезпечення.

2. Ризик та його етимологія. Становлення та розвиток теорії ризиків. Практична зумовленість теорії ризиків.

3. Підприємницький ризик. Суб’єктивна концепція ризику. Внутрішнє протиріччя ризику. Поняття ризику в безпеці життєдіяльності.

4. Означення ризику. Сума ризиків. Порівняльне оцінювання суми ризиків. Математична модель повного ризику. Обчислення ризиків як комплексного числа.

**Тема 2. Типологія ризиків**

1. Класифікація ризиків. Ризики техногенні (природні), індивідуальні та колективні, безумовно прийнятні, прийнятні та неприйнятні. Ризики короткострокові, середньострокові та довгострокові, разові, періодичні та постійні, локальні та глобальні. Ризики знехтувані, прийнятні, гранично допустимі та надмірні.

2. Ризики в кібербезпеці. Класифікація за складниками ризику: об’єктивний і суб’єктивний. Класифікація за мірою прояву ризику: низький, нижче середнього, середній, вище середнього, високий, найвищий.

3. Нульовий ризик. Сучасна концепція безпеки життєдіяльності.

**Тема 3. Обчислення ризиків**

1. Задачі на знаходження класичного ризику.

2. Задачі на знаходження статистичного ризику.
3. Задачі на знаходження геометричного ризику.

**Тема 4. Основні теореми для обчислення ризиків**

1. Теореми додавання ризиків.
2. Теореми множення ризиків.
3. Ризик принаймні однієї події.
4. Ризик виходу системи з ладу.

**Тема 5. Обчислення ризиків за основними формулами теорії ймовірностей**

1. Обчислення ризику за формулою повної ймовірності та формулою Байеса.
2. Ризики, що обчислюються за формулою Бернуллі.
3. Ризики, що обчислюються за граничними теоремами в схемі Бернуллі.
4. Використання числових характеристик випадкових величин (математичного сподівання, дисперсії, середнього квадратичного відхилення) в умовах ризиків.

**Тема 6. Прийняття рішення**

1. Концептуальні засади теорії прийняття рішень. Поняття «прийняття рішення», його широкий і вузький сенси.
2. Інтуїтивне рішення. Технологія інтуїтивного рішення.
3. Раціональне рішення. Технологія раціонального рішення та його оцінювання.
4. Прийняття рішення в системі інформаційної безпеки.

**Тема 7. Моделі прийняття рішення**

1. Умови повної визначеності рішення.
2. Основні моделі прийняття рішення. Класична модель. Поведінкова модель. Ірраціональна модель.
3. Методи прийняття рішення. Метод суду. Метод комісій. Метод Делфі. Метод генерації ідей.

**Тема 8. Методи кількісної оцінки ризиків кібербезпеки**

1. Ризики в системі управління інформаційною безпекою. Аналіз та ідентифікація ризиків.
2. Основні етапи забезпечення інформаційної безпеки. Оцінка ризиків кібербезпеки.
3. Групи методів кількісної оцінки ризиків кібербезпеки.

**Тема 9. Методики управління ризиками інформаційної безпеки**

1. Методика оцінки NIST 800-30.
2. Методика CRAMM.
3. Методика OCTAVE.
4. Методи експертних оцінок ризиків: метод Дельфі, метод бальної оцінки ризику. Якості експерта.
5. Коефіцієнт конкордації Кендала. Вимоги до експертної інформації.
6. Основні етапи аналізу експертної інформації.
7. Вимоги до інформаційної безпеки. Перелік загроз і вразливостей.
8. Визначення кількісного значення комплексного інформаційного ризику.

## 7. Індивідуальні завдання -

Не передбачені.

## 8. Методи навчання

Словесні – лекція, пояснення, розповідь, бесіда, дискусія тощо.

Практичні – виконання вправ, практичні роботи, реферати, графічні роботи; проблемно-пошуковий; пояснювально-ілюстративний; репродуктивний; дослідницький; проектний; розвивально-задачний.

## 9. Методи контролю

Письмова контрольна робота, усна перевірка знань і вмінь, усне опитування теоретичного матеріалу, тестування, екзамен.

## 10. Розподіл балів

| Поточне оцінювання та самостійна робота | | | | | | | | | Сума |
|---|---|---|---|---|---|---|---|---|---|
| Змістовий модуль 1 | | Змістовий модуль 2 | | | Змістовий модуль 3 | | Змістовий модуль 4 | | |
| Т1 | Т2 | Т3 | Т4 | Т5 | Т6 | Т7 | Т8 | Т9 | 100 |
| 8 | 8 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | |

## Шкала оцінювання

| За шкалою | Екзамен | Залік | Бали |
|---|---|---|---|
| A | Відмінно | Зараховано | 90-100 |
| B | Добре | Зараховано | 82-89 |
| C | | | 74-81 |
| D | Задовільно | Зараховано | 64-73 |

| | | | |
|---|---|---|---|
| E | | | 60-63 |
| FX | Незадовільно | Не зараховано | 35-59 |
| F | | Не зараховано | 0-34 |

## 11. Рекомендована література

***Основна література***

1. Барковський В.В., Барковська Н.В., Лопатін О.К. Теорія ймовірностей та математична статистика. – Київ: ЦУЛ, 2002. – 448 с. – Серія: Математичні науки.

2. Богуш В.М., Довидьков О.А., Кривуца В.Г. Основи захищених інформаційних технологій. – К.: ДУІКТ, 2010 - 454 с.

3. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: Монографія. – К.: НАУ, 2013. – 432 с.

4. Бурячок В.Л., Толубко В.Б., Хорошко В. О., Толюпа С.В. Інформаційна і кібербезпека: соціотехнічний аспект: Підручник. – К.: ДУТ, 2015. – 288 с.

5. Бурячок В.Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: Підручник. – К.: ДУТ, 2015. – 449 с.

6. Василевич Л.Ф., Юртин І.І. Прийняття рішень за умов конфлікту та невизначеності середовища. Навчальний посібник – К.: Видавництво Київського університету ім. Б. Грінченка, 2013. – 128с.

7. Василевич Л.Ф., Маловик К.Н., Смирнов С.Б. Количественные методи принятия решений в условиях риска. – Севастополь.: СНУЯЭиП, 2006. – 232 с.

8. Головня Р. М. Збірник завдань з теорії ймовірностей, математичної статистики та випадкових процесів: [навчальний посібник] / Р. М. Головня, В. О. Коваль, О. В. Лущиков. – Житомир : ЖДТУ, 2011 – 140 с.

9. Домарєв В.В., Скворцов С.О. Організація захисту інформації на об’єктах державної та підприємницької діяльності. Навч. посібник. – К.: Вид-во Європейського Університету, 2006. – 102 с.

10. Машина Н.І. Ризик і методи його вимірювання: Навчальний посібник. – К.: ЦНЛ, 2003. – 188 с.

11. Огірко О. І., Галайко Н. В. Теорія ймовірностей та математична статистика / О. І. Огірко, Н. В. Галайко. – Львів: ЛьвДУВС, 2017. – 292 с.

12. Семенець С.П. Методичні рекомендації до лабораторних робіт із навчальної дисципліни «Теорія ризиків та її застосування в кібербезпеці»: [для здобувачів освітньо-кваліфікаційного рівня «бакалавр» спеціальності 125 «Кібербезпека»]. – Житомир : РВВ «Житомирська політехніка», 2020. – 51 с.

13. Теорія ймовірностей та математична статистика: навч. посіб./ О. І. Кушлик-Дивульська, Н. В. Поліщук, Б. П. Орел, П. І. Штабалюк. – К: НТУУ «КПІ», 2014. – 212 с.

14. Risk Theory: A Heavy Tail Approach. https://www.tandfonline.com/doi/full/10.1080/01621459.2019.1662244

***Допоміжна література***

1. Probability theory and mathematical statistics: a textbook / A.V.Tyurin, A.Yu. Akhmerov – Odessa: «Odessa I.I. N Mechnikovational University», 2020. - 138 p.

2. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. – М.: Изд-во "Яхтсмен", 1996.– 192 с.

3. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия-Телеком, 2000. – 452 с.

4. Теоретические основы компьютерной безопасности: Учебное пособие для вузов / П.Н. Девянин и др. – М.: Радио и связь, 2000. – 192 с.

5. Доценко С.М., Шпак. В.Ф. Комплексная безопасность объекта: от теории к практике. - С.- Петербург: ООО «Издательство Полигон». – 2000. –176 с.

6. Гришина Н.В. Организация комплексной защиты информации. – Гелиос АРВ, 2007. – 256 с.

7. Гранатуров В.М. Риск. Сущность, методы измерения, пути снижения. – Дело и Сервис, 2010. – 208 с.

8. Балдин К.В., Воробьев С. Н. Модели и методы управления рисками. – М.: МПСИ, МОДЭК, 2009. – 432 с.

9. Хохлов Н.В. Управление риском. – М.: ЮНИТИ-ДАНА, 2001. – 239 с.

10. Саати Т. Принятия решений. Метод анализа иерархий. – М.: Радио и связь, 1991. – 320 с.

## 12. Інформаційні ресурси в Інтернеті

Бібліотечно-інформаційний ресурс (книжковий фонд, періодика, фонди на електронних носіях тощо) бібліотек:

1. Бібліотека Державного університету «Житомирська політехніка»: https://lib.ztu.edu.ua/
2. Бібліотека українських підручників [Електронний ресурс] – Режим доступу до ресурсу: http://pidruchniki.ws/
3. Житомирська обласна універсальна наукова бібліотека ім. Олега Ольжича [Електронний ресурс] – Режим доступу до ресурсу: http://www.lib.zt.ua/
4. Національна бібліотека України імені В. І. Вернадського: режим доступу: http://nbuv.gov.ua

Інституційний репозитарій Державного університету «Житомирська

політехніка»

*Індекс структурного підрозділу відповідно до наказу ректора «Про затвердження організаційної структури Державного університету «Житомирська політехніка» (наприклад, 22.06).

** Індекс освітньої програми відповідно до наказу ректора «Про індексацію освітніх програм Державного університету «Житомирська політехніка» (наприклад, 122.00.1/Б).

*** Шифр освітньої компоненти в освітній програмі (наприклад, ОК1).