**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ**
**ІМЕНІ СЕМЕНА КУЗНЕЦЯ**

**"ЗАТВЕРДЖУЮ"**
Проректор з навчально-методичної роботи
Каріна НЕМАШКАЛО

# ТЕОРІЯ РИЗИКІВ В КІБЕРБЕЗПЕЦІ

**робоча програма навчальної дисципліни**

| | |
|---|---|
| Галузь знань | ***12 Інформаційні технології*** |
| Спеціальність | ***125 Кібербезпека*** |
| Освітній рівень | **другий (магістерський*)*** |
| Освітня програма | ***Кібербезпека*** |

| | |
|---|---|
| Статус дисципліни | ***обов'язкова*** |
| Мова викладання, навчання та оцінювання | ***українська*** |

Завідувач кафедри
*кібербезпеки*
*та інформаційних технологій* *Ольга СТАРКОВА*

Харків
**2022**

ЗАТВЕРДЖЕНО
на засіданні кафедри *кібербезпеки та інформаційних технологій*
Протокол № 1 від 27.08.2022 р.

Розробники:
*Солодовник Ганна Валеріївна,* к.т.н., доцент кафедри КІТ

**Лист оновлення та перезатвердження**
**робочої програми навчальної дисципліни**

| Навчальний рік | Дата засідання кафедри – розробника РПНД | Номер протоколу | Підпис завідувача кафедри |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## Анотація навчальної дисципліни

Навчальна дисципліна «Теорія ризиків в кібербезпеці» призначена для здобувачів вищої освіти, що навчаються за освітньо-кваліфікаційним рівнем «магістр». Вивчення дисципліни передбачає формування у майбутніх спеціалістів умінь та компетенцій для забезпечення ефективної оцінки ризиків в сфері інформаційних технологій. Здобувачі мають ознайомитися із сучасними науковими досягненнями в питаннях якісного аналізу, кількісного оцінювання ризику; опанувати способи аналізу ризикових ситуацій, методи вибору оптимальної стратегії в умовах невизначеності та ризику.

Мета навчальної дисципліни: вивчення сучасних методів якісного та кількісного аналізу інформаційного ризику, набуття навичок розробки математичних моделей ризикових ситуацій та прийняття обґрунтованих рішень в умовах невизначеності та ризику.

Завдання: вивчення основних засад ризикології як науки та її базових понять, методів кількісного оцінювання ризиків, експертних методів та моделей оцінювання ризиків, визначення погодженості експертних оцінок, моделей прийняття рішень в умовах невизначеності і ризику, засобів зменшення інформаційних ризиків, сучасних стандартів оцінки інформаційної безпеки, методів аналізу можливих загроз з боку шкідливого програмного забезпечення.

Предмет вивчення навчальної дисципліни: моделі та методи кількісного оцінювання ризиків та прийняття рішень в умовах ризику та невизначеності.

Результатами вивчення дисципліни є системні знання та практичні навички в області якісного та кількісного аналізу ризиків, управління інформаційними ризиками.

### Характеристика навчальної дисципліни

| | |
|---|---|
| Курс | **1** |
| Семестр | **1** |
| Кількість кредитів ECTS | **4** |
| Форма підсумкового контролю | **залік** |

### Структурно-логічна схема вивчення дисципліни

| Пререквізити | Постреквізити |
|---|---|
| Вища математика | Основи наукових досліджень та науково-педагогічна діяльність в галузі кібербезпеки |
| Технології обробки інформації | Розширена мережева та хмарна безпека |
| | Тестування на проникнення та етичний хакінг |
| | Стандартизація та сертифікація кібернетичної діяльності |

### Компетентності та результати навчання за дисципліною

| Компетентності | Результати навчання |
|---|---|
| - КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт.<br>- КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, | - РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. |

| | | |
|---|---|---|
| | інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.<br>- КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. | |
| | - КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт.<br>- КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.<br>- КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної | - РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення. |

| | |
|---|---|
| безпеки та/або кібербезпеки організації. | |
| - КЗ-1. Здатність застосовувати знання у практичних ситуаціях.<br>- КЗ-2. Здатність проводити дослідження на відповідному рівні.<br>- КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу.<br>- КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт. | - РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки. |
| - КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт.<br>- КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.<br>- КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. | - РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. |
| - КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт. | - РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. |

| | |
|---|---|
| - КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт. | - РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. |
| - КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт.<br>- КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. | - РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації. |

**Програма навчальної дисципліни**

**Змістовий модуль 1. Загальні засади теорії ризиків**
ТЕМА 1. Поняття ризику, його основні елементи й ознаки.
ТЕМА 2. Класифікація ризиків порушення інформаційної безпеки.
ТЕМА 3. Методи оцінювання ризиків.
ТЕМА 4. Аналіз та оцінювання інформаційної безпеки.
**Змістовий модуль 2. Методи оцінювання інформаційних ризиків**
ТЕМА 5. Методики та технології управління інформаційними ризиками.
ТЕМА 6. Аналіз ризиків з боку шкідливого програмного забезпечення.
ТЕМА 7. Інформаційні ризики в умовах постквантової криптографії.

Перелік лабораторних занять, а також питань та завдань до самостійної роботи наведено у таблиці «Рейтинг-план навчальної дисципліни».

**Методи навчання та викладання**

Викладання дисципліни передбачає залучання пояснювально-ілюстративного, репродуктивного, дослідницького методів, а також методів проблемного навчання. Так під час проведення лекційних занять викладач надає здобувачам певний обсяг теоретичного матеріалу з аналізу ризиків (Тема 1, 4, 6,7), з наданням пояснень у графічному вигляді (схеми, таблиці, презентації) та за допомогою прикладів розв'язання задач (Тема 2, 3, 4, 6). На практичних заняттях здобувачі мають змогу отримати практичні навички розв'язання задач на підставі проблеми, сформульованої за тематикою заняття (Тема 2, 3, 4, 5, 6). Вдосконалення практичних навичок відбувається під час виконання індивідуальних завдань та самостійної роботи (Тема 2, 3, 4, 5, 6, 7).

Наведені методи навчання спрямовані на формування у здобувачів здатності розв'язання складних комплексних задач в галузі оцінювання ризиків.

## Порядок оцінювання результатів навчання

Програма навчальної дисципліни передбачає лекційні, практичні та самостійну види робіт. Знання та компетентності отримані здобувачами під час лекційних занять оцінюються за написання контрольних робіт та складання тестів, навички отримані під час практичних занять оцінюються за розв'язанням задач передбачених тематикою роботи. Самостійна робота окремо не оцінюється, оскільки вона полягає у підготовці до інших видів занять. Оцінювання сформованих компетентностей здобувачів здійснюється за рейтинговою накопичувальною 100-бальною системою. Контрольні заходи включають:

- поточний контроль, що здійснюється протягом семестру під час проведення лекційних та практичних занять і оцінюється сумою набраних балів (максимальна сума – 60 балів; мінімальна сума, що надає студенту складати екзамен – 35 балів);

- модульний контроль передбачає виконання підсумкових контрольних завдань, які можуть включати творчу дослідницьку складову та потребують знань та навичок отриманих під час вивчення певної сукупності матеріалу за тематикою модуля.

За поточного контролю знання здобувачів оцінюються за такими критеріями:

– вільне володіння навчальним матеріалом в повному обсязі, з розумінням прикладів та можливістю наведення власних прикладів для пояснення сутності матеріалу;

– демонстрація навичок застосування методів якісного аналізу та кількісного оцінювання ризиків;

– демонстрація навичок застосування інноваційних методів роботи під час розв'язання задач;

– демонстрація вміння пошуку та аналізу джерел інформації, обґрунтування отриманих результатів та формування висновків за роботою;

– демонстрація навичок командної роботи під час розв'язання комплексних завдань з аналізу та оцінювання ризиків.

Формування завдань та контроль за їх виконанням мають за мету сприяння набуття здобувачами навичок активного творчого мислення, прищеплення когнітивних навичок та норм доброчесної співпраці. Головною вимогою до виконання завдань є самостійність їх виконання або визначення відсотку вкладу за умови командної роботи.

Розподіл балів поточного оцінювання за видами робіт є наступним.

**Лекційні заняття:** рівень оволодіння теоретичними знаннями визначається під час захисту виконання практичних робіт, за написання контрольних робіт або виконання індивідуального завдання (максимальна кількість балів становить – 23).

**Практичні заняття:** рівень набутих навичок застосування знань для розв'язання задач визначається правильністю виконання завдань практичних робіт (максимальна кількість балів становить – 77).

**Самостійна робота:** рівень оволодіння навичками використання новітніх знань, методології та методів проведення наукових досліджень визначається за ступенем підготовки здобувача до виконання практичних робіт та написання контрольних робіт (в технологічній карті додаткових балів на цей вид робіт не передбачено).

**Підсумковий контроль**: проводиться у вигляді заліку з урахуванням балів отриманих здобувачем під час складання практичних та контрольних робіт.

Форми оцінювання та розподіл балів наведено у таблиці "Рейтинг-план навчальної дисципліни".

## Рейтинг-план навчальної дисципліни

| Тема | Форми та види навчання | | Форми оцінювання | Max бал |
|---|---|---|---|---|
| Тема 1 | ***Аудиторна робота*** | | | |
| | Лекція | Лекція 1. Поняття ризику, його основні елементи й ознаки | Робота на лекції | |
| | Практичне заняття | Практична робота №1. Ризик як ймовірнісна категорія | Виконання та захист практичної роботи | 11 |
| | ***Самостійна робота*** | | | |
| | Питання та завдання до самостійного опрацювання | Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань | | |
| Тема 2 | ***Аудиторна робота*** | | | |
| | Лекція | Лекція 2. Класифікація ризиків порушення інформаційної безпеки | Робота на лекції | |
| | Практичне заняття | Практична робота №2. Кількісне оцінювання ризиків. Теоретико-ігрова модель | Виконання та захист практичної роботи | 11 |
| | ***Самостійна робота*** | | | |
| | Питання та завдання до самостійного опрацювання | Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань | | |
| Тема 3 | ***Аудиторна робота*** | | | |
| | Лекція | Лекція 3. Методи оцінювання ризиків | Робота на лекції | |
| | Практичне заняття | Практична робота №3. Суб’єктивні методи оцінювання ризиків | Виконання та захист практичної роботи | 11 |
| | ***Самостійна робота*** | | | |
| | Питання та завдання до самостійного опрацювання | Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань | | |
| Тем | ***Аудиторна робота*** | | | |
| | Лекція | Лекція 4. Аналіз та оцінювання інформаційної безпеки | Робота на лекції | |

| | | | | |
|---|---|---|---|---|
| **а 4** | Практичне заняття | Практична робота №4. Оцінювання ризиків за допомогою дерева рішень | Виконання та захист практичної роботи | 11 |
| | | Модульний контроль | Письмова контрольна робота за темами 1-4 | 10 |
| | ***Самостійна робота*** | | | |
| | Питання та завдання до самостійного опрацювання | Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань | | |
| **Тема 5** | ***Аудиторна робота*** | | | |
| | Лекція | Лекція 5. Методики та технології управління інформаційними ризиками | Робота на лекції | |
| | Практичне заняття | Практична робота №5. Теорія корисності у вимірюванні ризику | Виконання та захист практичної роботи | 11 |
| | ***Самостійна робота*** | | | |
| | Питання та завдання до самостійного опрацювання | Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань | | |
| **Тема 6** | ***Аудиторна робота*** | | | |
| | Лекція | Лекція 6. Аналіз ризиків з боку шкідливого програмного забезпечення | Робота на лекції | |
| | Практичне заняття | Практична робота №6. Ймовірнісний підхід до визначення працездатності ІС | Виконання та захист практичної роботи | 11 |
| | ***Самостійна робота*** | | | |
| | Питання та завдання до самостійного опрацювання | Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань | | |
| **Тема 7** | ***Аудиторна робота*** | | | |
| | Лекція | Лекція 7. Інформаційні ризики в умовах постквантової криптографії | Робота на лекції | |
| | Практичне заняття | Практична робота №7. Аналіз загроз з боку фішингу | Виконання та захист практичної роботи | 11 |

| | | | | |
|---|---|---|---|---|
| | | Модульний контроль | Письмова контрольна робота за темами 5-7 | 13 |
| | Самостійна робота | | | |
| | Питання та завдання до самостійного опрацювання | Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань | | |
| | Підсумок | | | 100 |

## Рекомендована література

**Основна**


1. Вітлінський В. В., Великоіватенко Г. І. Ризикологія в економіці та підприємництві: Моногр. — К.: КНЕУ, 2020. — 390 с.
2. Ветлінський В. та інш. Економічний ризик, ігрові моделі,: навч. Посібник К.: КНЕУ.-2019.
3. Андрійчук В., Бауер А. Менеджмент: прийняття рішень і ризик. Навчальний посібник. К.: КНЕУ, 2018. — 270 с..
4. Вітлінський В. В., Верченко П. і., Наконечний Я. С., Сігал А. В. Економічнийризик: ігровімоделі: Навч. посіб. — К.: КНЕУ, 2020. — 446 с.
5. Солодовник Г.В. Управління економічним та інформаційним ризиком: навчальний посібник. – Х.: ТОВ «ДІСА ПЛЮС», 2018. -152 с. (ISBN 978-617-7645-125-2)


**Додаткова**


6. Правові засади інформаційної безпеки України: монографія / Біленчук П.Д. [та ін.] ; за ред. П.Д. Біленчука. Харків, 2018. 289 с.
7. 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.**


8. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною "Теорія ризиків в кібербезпеці" https://pns.hneu.edu.ua/course/view.php?id=8944