Силабус освітнього компонента
Програма навчальної дисципліни

Безпека серверних систем

Шифр та назва спеціальності
F5 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Спеціалізація

Кафедра
Кібербезпеки (328)

Освітня програма
Кібербезпека

Тип дисципліни
Професійна підготовка, Вибіркова

Рівень освіти
Другий (магістерський)

Форма навчання
Денна, заочна

Семестр
2

Мова викладання
Українська, англійська

Викладачі, розробники

ЄВСЕЄВ Сергій Петрович

serhii.yevseiev@khpi.edu.ua
Доктор технічних наук, професор, завідувач кафедри кібербезпеки НТУ «ХПІ».

Лауреат національної премії імені Бориса Патона.
Кількість наукових публікацій: понад 351, з них патентів на корисну модель 44, 11 монографій, з яких 10 колективних монографій, 31 навчальний посібник, з яких 4 з грифом Міністерства освіти і науки України, 149 статтей у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus. Гарант освітньо-професійної програми "Кібербезпека" першого (бакалаврського) рівня вищої освіти. Провідний лектор з дисциплін: Математичні основи криптології, Комп`ютерні мережі, Основи криптографічного захисту, Методи криптоаналізу, Основи кібербезпеки, Сучасні проблеми постквантової криптографії, Основи наукових досліджень, Цифрова криміналістика, Етичний хакінг у студентів бакалавріата та магістратури, Методологія наукової та педагогічної діяльності в науках кіберзахисту для аспірантів.

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна «Ігрові моделі кіберконфліктів» розроблена таким чином, щоб надати учасникам необхідні знання, про матричні ігри, нескінчені антагоністичні та неантагоністичні ігри, багатокрокові ігри, антагоністичні та неантагоністичні диференційні ігри, кооперативні ігри, принципи оптимальності в різних ігрових ситуаціях.

Мета та цілі дисципліни

Мета навчальної дисципліни - вивчення базових знань з основ застосування методів і моделей теорії ігор, розвиток логічного мислення, здатність будувати модель гри та обґрунтувати вибір моделі, що відповідає досліджуваній задачі, здатність досліджувати отриману модель та критично аналізувати отримані результати.

Формат занять

Лекції, лабораторні заняття, самостійна робота, консультації. Підсумковий контроль – диференційований залік.

Компетентності

КЗ1. Здатність застосовувати знання у практичних ситуаціях.
КЗ2. Здатність проводити дослідження на відповідному рівні.
КЗ3. Здатність до абстрактного мислення, аналізу та синтезу.
КЗ4. Здатність оцінювати та забезпечувати якість виконуваних робіт.
КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.
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.
КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.
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.
КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ7. Здатність 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.
КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.

Результати навчання

РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.
РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
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.
РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
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.
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.
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.
РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.
РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.
РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.
РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.
РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.
РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.

РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.
РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.
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.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 16 год., лабораторні роботи – 32 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Технології захисту інформації.

Особливості дисципліни, методи та технології навчання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, індивідуальні групові проєкти, майстер-класи.

Програма навчальної дисципліни

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Основні поняття теорії ігор. Задачі теорії ігор. Конфлікти в теорії ігор. Основні поняття та класифікація видів ігор.	2
Тема 2. Статичні ігри з повною інформацією. Способи завдання безкоаліційних ігор. Ігри в нормальній формі. Доміновані стратегії. Послідовне виключення домінованих стратегій. Рівновага Неша і домінування.	2
Тема 3. Змішані стратегії та існування рівноваги. Поняття змішаних стратегій та рівноваги у них. Матричне означення очікуваних виграшів. Опуклі комбінації та множини змішаних стратегій. Умова найкращої відповіді та існування змішаних рівноваг.	2
Тема 4. Динамічні ігри з повною інформацією. Позиційні форми гри. Обернена індукція та скінченні ігри з досконалою інформацією. Досконала підігрова рівновага по Нешу. Ігри з недосконалою інформацією. Змішані стратегії в динамічній грі.	2
Тема 5. Антагоністичні ігри в нормальній формі. Означення ігор, максимальні та мінімальні стратегії. Ситуації рівноваги. Основна теорема для прямокутних ігор.	2

Тема 6. Кооперативні ігри. Класичні кооперативні ігри. Ігри без побічних платежів. Нечіткі коаліції. Застосування кооперативних ігор.	2
Тема 7. Ігри з природою. Поняття ігри з природою. Поняття ігри з природою. Прийняття рішень в умовах повної невизначеності. Прийняття рішень в умовах ризику. Критерії вибору оптимальних стратегій. Планування експерименту в іграх з природою. Вибір рішення за допомогою дерева рішень.	2
Тема 8. Теоретико-ігрові моделі економічних та управлінських процесів. Теоретико-ігрове моделювання задач управління персоналом, суспільними інституціями, суспільно-економічними процесами.	2
Загальна кількість годин	**16**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Матрична гра «зловмисник – адміністратор». Вивчення моделі антагоністичної гри між атакувальником і захисником. Побудова платіжної матриці, визначення оптимальних стратегій, аналіз рівноваги та мінімаксних рішень.	4	0,1
Тема 2. Вибір програмного додатку для оптимального набору засобів захисту. Практичне моделювання вибору комплексних засобів кіберзахисту на основі теорії ігор або методів оптимізації. Порівняння стратегій захисту й оцінка їх виграшності.	4	0,1
Тема 3. Відбиття атак у кіберпросторі. Захист комп'ютерної системи від НСД. Симуляція атаки і захисту у моделі «напад – контрзаходи». Аналіз рішень у статичних та динамічних іграх, вибір оптимальної стратегії захисту.	4	0,1
Тема 4. Розміщення конфіденційної інформації на серверах. Дослідження стратегій розподілу та дублювання даних для зменшення ризику компрометації. Моделювання ігор із природою та з ризиком для визначення надійної конфігурації.	4	0,1
Тема 5. Боротьба з вірусами. Захист комп'ютерної системи як позиційна гра. Розгляд боротьби зі шкідливим ПЗ як позиційної динамічної гри. Аналіз послідовних ходів, сценаріїв поширення вірусу та стратегій ліквідації.	4	0,1
Тема 6. Моделювання поведінки азартного зловмисника. Побудова моделей зловмисника, що приймає ризиковані рішення. Використання змішаних стратегій, ігор з неповною інформацією та стохастичних моделей поведінки.	4	0,1
Тема 7. Стохастичні ігри. Вивчення ігор із випадковими станами та переходами, моделювання стратегій у невизначених умовах. Аналіз стратегій довгострокового виграшу, значення дисконтних факторів.	4	0,1

Тема 8. Аналіз безпеки комп'ютерної мережі. Застосування теоретико-ігрових моделей для оцінки вразливостей мережі, вибору оптимальної стратегії моніторингу та розміщення ресурсів захисту. Побудова графових моделей атаки та захисту.	4	0,1
Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i = 0{,}8$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Статичні, змішані та антагоністичні моделі в теорії ігор. Контрольна робота охоплює базові поняття теорії ігор, статичні ігри з повною інформацією, принципи домінування стратегій та рівновагу Неша. Також перевіряється розуміння змішаних стратегій, умов існування рівноваги та основ антагоністичних (нульової суми) ігор. Метою є оцінити здатність студента аналізувати ігрові ситуації та обчислювати рівноваги у різних типах статичних моделей.	0,1
Тема 2. Динамічні, кооперативні та невизначені ігрові моделі та їх застосування. Контрольна робота присвячена динамічним іграм, методам оберненої індукції, рівновазі у підіграх, а також аналізу ігор з неповною інформацією. Додатково перевіряється знання кооперативних моделей, ролі коаліцій, рішень у ситуаціях невизначеності (ігри з природою), а також уміння застосовувати теоретико-ігрові підходи до економічних, соціальних та управлінських процесів.	0,1
Загалом	$\sum_{i=1}^{m} b_i = 0{,}2$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріалу

Теми для самостійного вивчення	Кількість годин
Тема 1 Ігрові моделі кібербезпеки: базові концепції. Вивчення специфіки кіберконфліктів: асиметрія інформації між атакуючим і захисником, непередбачуваність дій та динамічний характер загроз. Порівняння кіберконфліктів із класичними моделями конфліктів.	8
Тема 2. Моделі «атакуючий–захисник» (Attacker–Defender Games). Формалізація протистояння: вибір атакуючим вектора атаки, вибір захисником розподілу ресурсів для захисту. Аналіз мінімаксних стратегій, оптимальних захисних політик.	8
Тема 3. Байєсівські ігри у кіберконфліктах. Моделювання ситуацій з неповною інформацією: невідомі можливості атакуючого, рівень компетентності противника, приховані наміри. Оцінка ймовірностей типів гравців та пошук рівноваги в умовах невизначеності.	7
Тема 4. Динамічні ігри для моделювання багатокрокових кібератак. Використання дерев рішень і марківських моделей для опису ланцюгів атак (A→B→C). Моделювання ескалації, прихованості, відкладених дій та реакцій	7

захисника.	
Тема 5. Ігрові моделі повторюваних атак і стратегії покарання. Вивчення довгострокової взаємодії між хакерами та інфраструктурою. Застосування рівноваг Фолка, стратегій «тит-фор-тат» та динаміки довіри/покарань.	7
Тема 6. Моделювання розподілу ресурсів у кібероборони (Resource Allocation Games). Аналіз задач, де ресурси обмежені: бюджет на кібербезпеку, час реагування, кількість спеціалістів. Пошук оптимальних стратегій розподілу для мінімізації ризику.	7
Тема 7. Сторонні учасники та коаліції в кіберконфліктах. Розгляд моделей, де кілька організацій об'єднуються для взаємного захисту або обміну інформацією. Кооперативні ігри, ядро, Шеплі-вектор у контексті кібероборонних альянсів.	7
Тема 8. Інформаційні операції та дезінформація як ігровий процес. Моделювання маніпуляцій інформаційним простором: створення фейків, блокування, протидія дезінформації. Ігри на мережах, моделі поширення впливу та стратегічного приховування.	7
Тема 9. Теорія ігор у контексті кіберфізичних систем. Аналіз атак на критичну інфраструктуру (енергосистеми, транспорт, промисловість). Моделі взаємодії цифрових і фізичних компонентів, оптимізація захисних протоколів.	7
Тема 10. Ігри на графах у кіберконфліктах. Використання графових структур для опису мереж: вибір вузлів для атаки або захисту, моделювання поширення шкідливого коду. Застосування центральності, мережевих рівноваг.	7
Загальна кількість годин	**72**

Неформальна освіта

Здобувач має можливість перезарахувати окремі теми або курс шляхом: проходження професійних курсів чи тренінгів, онлайн-освіти, професійних стажувань, у сфері, що відповідає навчальним цілям дисципліни.
Для зарахування необхідно надати: сертифікат (електронний або друкований) про проходження курсу/стажування, опис програми тренінгу із зазначенням змісту тем, обсягу та тривалості.

Рекомендовані курси, тренінги, стажування

За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.

Література, навчальні матеріали та інформаційні ресурси

Основна література

1 Вітлінський В.В. та ін. Економічний ризик: ігрові моделі: Навч. посібник /В.В.Вітлінський, П.І.Верченко, А.В.Сігал, Я.С.Наконечний; за ред.. д-ра екон.наук, проф.. в.В.Вітлінського. – К. : КНЕУ, 2002. – 446 с. [Електронний ресурс]. – Режим доступу : https://h.twirpx.link/file/671825/
2. Теорія ігор: Курс лекцій. Навчальний посібник / укл. Барановська Л.В. – Київ : КПІ ім. І.Сікорського. – 2022. – 244 с. [Електронний ресурс]. – Режим доступу : https://ela.kpi.ua/items/e60f0070-647d-431e-ad79-356b61953b55
3. Peter W. Singer, Allan Friedman, Cybersecurity: What Everyone Needs to Know [Електронний ресурс].

– Режим доступу : https://books.google.com.ua/books/about/Cybersecurity.html?id=9VDSAQAAQBAJ&redir_esc=y
4. Dr. Chase Cunningham, Cyber Warfare – Truth, Tactics, and Strategies [Електронний ресурс]. – Режим доступу : https://books.google.com.ua/books?id=Cd7SDwAAQBAJ&printsec=frontcover&hl=ru&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false
5. Jeffrey Pawlick, Quanyan Zhu, 2021 Game Theory for Cyber Deception: From Theory to Applications [Електронний ресурс]. – Режим доступу https://link.springer.com/book/10.1007/978-3-030-66065-9?utm_source=chatgpt.com

Додаткова література

6. Charles A. Kamhoua, Quanyan Zhu, Christopher D. Kiekintveld, Fei Fang, 2021 Game Theory and Machine Learning for Cyber Security [Електронний ресурс]. – Режим доступу https://www.ellibs.com/book/9781119723912/game-theory-and-machine-learning-for-cyber-security?utm_source=chatgpt.com
7. Шевченко , С., Жданова, Ю., Складанний, П., & Бойко, С. (2023). ТЕОРЕТИКО-ІГРОВИЙ ПІДХІД ДО МОДЕЛЮВАННЯ КОНФЛІКТІВ У СИСТЕМАХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 168–178. https://doi.org/10.28925/2663-4023.2023.22.168178
8. Теоретико-ігрові та оптимізаційні моделі і методи підвищення безпеки кіберінфраструктур / В. М. Горбачук, Г. В. Голоцуков, М. С. Дунаєвський, А. А. Сирку, С.-Б. Сулейманов // Проблеми керування та інформатики. - 2022. - № 2. - С. 92-106. - http://doi.org/10.34229/2786-6505-2022-2-6

Система оцінювання

Підсумкова оцінка з освітнього компонента визначається відповідальним лектором за темами, видами занять, тощо у відповідності до силабусу і є інтегральною оцінкою результатів усіх вид навчальної діяльності здобувача вищої освіти. Підсумкова оцінка повинна відображати всі оцінки за складовими навчального процесу з урахуванням їх вагових показників k:

Поточний контроль (практичні, семінарські, лабораторні заняття), k_1	Контрольні роботи (за наявності), k_2	Індивідуальне завдання (за наявності), k_3	Підсумковий контроль (для ОК з іспитом), k_4
0,8	0,2		

Сума коефіцієнтів повинна складати одиницю: $k_1 + k_2 + k_3 + k_4 = 1$. Підбір вагових коефіцієнтів підсумкової оцінки здійснює розробник курсу.
Розрахунок підсумкової оцінки проводиться за формулою:

$$О = П \cdot k_1 + K \cdot k_2 + І \cdot k_3 + Пк \cdot k_4$$

де: П – середньозважена середня оцінка за поточний контроль
І – оцінка за виконання індивідуального завдання
K – середньозважена оцінка за контрольні роботи
Пк – оцінка за підсумковий контроль

$$П = \frac{П_1 \cdot a_1 + П_2 \cdot a_2 + ... + П_n \cdot a_n}{\sum_{i=1}^{n} a_i}$$

де: a_i - ваговий коефіцієнт за кожне практичне (семінарське) або лабораторне заняття.

$$K = \frac{K_1 \cdot b_1 + K_2 \cdot b_2 + ... + K_m \cdot b_m}{\sum_{i=1}^{m} b_i}$$

де: b_i - ваговий коефіцієнт за кожну контрольну роботу.

Поточні оцінки за кожну складову (П, *К*, І,...) виставляються за 100-бальною шкалою згідно з положенням «Про критерії та систему оцінювання знань та вмінь і про рейтинг здобувачів вищої освіти» НТУ «ХПІ».

Підсумкова оцінка виставляється відповідно до розрахованої О з округленням до найближчого цілого числа в більшу сторону.

Шкала оцінювання

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B
75–81	Добре	C
64–74	Задовільно	D
60–63	Задовільно	E
35–59	Незадовільно (потрібне додаткове вивчення)	FX
1–34	Незадовільно (потрібне повторне вивчення)	F

Норми академічної етики і політика курсу

Здобувач вищої освіти повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту.
Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

Погодження

Силабус погоджено	30.08.2025		**Завідувач кафедри** Сергій ЄВСЕЄВ
	30.08.2025		**Гарант ОП** Ольга КОРОЛЬ