Силабус освітнього компонента

Програма навчальної дисципліни

Презентація та обробка знань

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
Науково-професійного спрямування, Вибіркова

Рівень освіти
Другий (магістерський)

Форма навчання
Денна

Семестр
3

Мова викладання
Українська

Викладачі, розробники

ГАВРИЛОВА Алла Андріївна

alla.havrylova@khpi.edu.ua
PhD, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 50, з них патентів на корисну модель 2, 5 монографії, з яких 3 – у рецензованому виданні, що входить до бази даних Scopus, 1 – в іноземному науковому виданні, 2 – у фаховому виданні України; 14 статей, з них 7 наукових статей – у наукових фахових виданнях України, 4 наукові статті – у рецензованих виданнях, що входять до бази даних Scopus, 3 статті – в іноземних наукових виданнях. Лектор з дисциплін: «Презентація та обробка знань», «Основи управління в проєктах галузікібербезпеки та захисту інформації», «Безпека та анонімність роботи в Інтернет» у студентів магістратури.

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

У межах даної дисципліни здобувачі вищої освіти досліджують побудову інтелектуальних інформаційних систем із застосуванням різних методів представлення знань та моделей, їх формалізації, згідно до обраної предметної області та поставленої мети.

Мета та цілі дисципліни

Сформувати системне базове уявлення, первинні знання, вміння і навички студентів з основ інженерії знань і нейроінформатікі, як двома напрямками побудови інтелектуальних інформаційних систем, дати уявлення про моделі знань і методах обробки знань, надбання вміння і навичок з орієнтації в різних методах представлення знань, переходах від одного методу до іншого, формалізації знань експертів із застосуванням різних методів представлення знань, розроблення продукційної бази знань для вирішення задач з вибору варіантів в предметній області, що слабо формалізована та програмування на мові Пролог.

Формат занять

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

Компетентності

КЗ-1. Здатність застосовувати знання у практичних ситуаціях.
КЗ-2. Здатність проводити дослідження на відповідному рівні.
КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу.
КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт.
КЗ-5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
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.

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.
РН24. Планувати та виконувати наукові та прикладні дослідження у сфері інформаційної безпеки та/або кібербезпеки із застосуванням сучасних технологій, експериментальних і теоретичних

методів і моделей теорії прийняття рішень, системного аналізу, оптимізації процесів, математичної статистики.
РН25. Оцінювати ефективність та практичну цінність результатів наукових і практичних досліджень та інновацій.

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)

Інноваційне підприємництво та управління стартап-проєктами, Математичні моделі управління ІТ-проєктами, Філософські проблеми сучасного наукового пізнання.

Особливості дисципліни, методи та технології навчання

Лекції проводяться інтерактивно з використанням мультимедійних технологій. Застосовуються активні форми проведення занять: лекція, лекційне опитування, лабораторні заняття, консультація. На заняттях використовується компетентністний підхід до навчання, акцентується увага на застосуванні он-лайн курсу з розгляду сучасних питань у галузі кібербезпеки.

Програма навчальної дисципліни

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Знання і дані. 1. Властивості знань і відмінність знань від даних 2. Типи знань: декларативні і процедурні, екстенсіональності і інтенсіональні 3. Нечіткі знання 4. Визначення. Причини нечіткості знань 5. Нечітка логіка 6. Проблема розуміння сенсу як вилучення знань з даних і сигналів	2
Тема 2. Методи представлення знань. 1. Логіка предикатів першого порядку 2. Логічні та евристичні методи представлення знань 3. Поняття предиката, формули, квантори загальності та існування 4. Інтерпретація формул в логіці предикатів 1-го порядку	2
Тема 3. Методи обробки знань. 1. Метод резолюції для доведення теорем в логіці 1-го порядку 2. Логіка Хорна як основа мови логічного програмування Prolog 3. Особливості побудови модальних систем 4. Семантика можливих світів	1
Тема 4. Псевдофізичні логіки. 1. Теорія нечітких множин - основа псевдофізичних логік 2. Нечітка логіка 3. Поняття лінгвістичної змінної 4. Приклади псевдофізіческіх логік: просторова й часова логіки	1
Тема 5. Правила-продукції. 1. Структура правил-продукцій 2. Структура продукційного правила 3. Методи логічного висновку: прямий і зворотний	2

4. Стратегії вибору правил при логічному висновку 5. Методи представлення й обробки нечітких знань в продукційних системах 6. Переваги та недоліки правил-продукцій як методу представлення знань	
Тема 6. Семантичні мережі. 1. Основні поняття семантичних мереж: уявлення об'єктів та відносин між ними як орієнтованого графа 2. Типи відносин у семантичних мережах 3. Класифікація семантичних мереж 4. Принципи обробки інформації у семантичних мережах 5. Використання семантичних мереж	2
Тема 7. Фрейми і об'єкти. 1. Основні поняття фрейму: слоти, приєднані процедури-слуги і процедури-демони, успадкування властивостей 2. Зв'язок поняття фрейму і об'єкта в об‘єетно-орієнтованому програмуванні 3. Мережі фреймів 4. Приклади мов інженерії знань, заснованих на фреймах: FRL і KRL	2
Тема 8. Нейронні мережі. 1. Основні поняття про природні та штучні нейронні мережі і нейрони 2. Формальний нейрон Маккаллок-Питтса 3. Нейронна мережа як механізм, якого навчають розпізнаванню образів або адекватної реакції на вхідні сигнали (вхідну інформацію) 4. Класифікація нейронних мереж 5. Переваги та недоліки нейронних мереж як методу представлення й обробки знань	2
Тема 9. Методи придбання знань. 1. Основні поняття методів навчання 2. Класифікація методів навчання за способом навчання: емпіричні та аналітичні, по глибині навчання - символьні (поверхневі) і на основі знань (глибинні) 3. Зв'язок цієї класифікації з поняттями індуктивного виводу, виведення за аналогією, навчання на прикладах 4. Індукція Мілля. Недоліки цього методу 5. ДСМ-метод. Визначення індуктивного виводу	2
Загальна кількість годин	**16**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Встановлення середовища програмування. 1. Середа Visual Prolog 2. Факти та правила 3. Основні розділи Visual Prolog 4. Сфери використання Visual Prolog 5. Основи та синтаксис мови Visual Prolog	4	1
Тема 2. Створення баз знань у Visual Prolog 1. Записати за правилами Visual Prolog факти та сформулювати запити 2. За деревом родинних відношень записати факти за правилами Visual Prolog та сформулювати запити	4	1

Тема 3. Пошук з поверненням. Управління пошуком. 1. Використання налагоджувача для покрокового виконання програми 2. Цільове дерево пошуку рішення 3. Використання предикатів fail та відсічення 4. Використання предикату введення строкового значення Readln	6	2
Тема 4. Рішення логічних задач у Visual Prolog. 1. Короткі теоретичні відомості 2. Практичне застосування	6	2
Тема 5. Арифметичні обчислення та рекурсія у Visual Prolog. 1. Математичні операції і функції 2. Використання предикату для введення дійсних чисел - readreal 3. Рекурсія у Visual Prolog для організації повторюваних дій	6	2
Тема 6. Списки. 1. Формування списку 2. Об'єднання списків 3. Пошук елемента в списку 4. Вставка елемента в список та видалення зі списку	6	2
Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i = 10$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Запишіть за правилами Прологу факти та сформулювати запити. 1. Генеалогічне дерево 2. Родинні відносини 3. Переваги щодо фруктів 4. Переваги щодо видів спорту 5. Реалізувати проєкт підпункту 1 і доопрацювати вихідний код	12
Тема 2. Скласти правило спортсмен, правило музикант. 1. Визначити, хто захоплюється спортом 2. Побудувати цільове дерево пошуку із поверненням	12
Тема 3. Скласти правило з вирішення логічних завдань. 1. Визначити, з якою твариною гуляв кожен із дітей 2. Який колір волосся у кожного з друзів 3. В якому порядку сиділи друзі 4. Визначити другу за довжиною річку	12
Тема 4. Скласти правило вирішення арифметичних завдань. 1. Скласти програму для обчислення значення виразу 2. Скласти програму для перевірки введеного натурального числа на парність 3. Підрахувати суму ряду 4. Знайти значення добутку	12
Тема 5. Скласти правила за списками 1. Формування списків	12
Загалом	$\sum_{i=1}^{m} b_i$=60

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріалу

Теми для самостійного вивчення	Кількість годин
Тема 1. Знання і дані. 1. Властивості знань і відмінність знань від даних 2. Типи знань: декларативні і процедурні, екстенсіональності і інтенсіональні 3. Нечіткі знання 4. Визначення. Причини нечіткості знань 5. Нечітка логіка 6. Проблема розуміння сенсу як вилучення знань з даних і сигналів	8
Тема 2. Методи представлення знань. 1. Логіка предикатів першого порядку 2. Логічні та евристичні методи представлення знань 3. Поняття предиката, формули, квантори загальності та існування 4. Інтерпретація формул в логіці предикатів 1-го порядку	8
Тема 3. Методи обробки знань. 1. Метод резолюції для доведення теорем в логіці 1-го порядку 2. Логіка Хорна як основа мови логічного програмування Prolog 3. Особливості побудови модальних систем 4. Семантика можливих світів	8
Тема 4. Псевдофізичні логіки. 1. Теорія нечітких множин - основа псевдофізичних логік 2. Нечітка логіка 3. Поняття лінгвістичної змінної 4. Приклади псевдофізіческіх логік: просторова й часова логіки	8
Тема 5. Правила-продукції. 1. Структура правил-продукцій 2. Структура продукційного правила 3. Методи логічного висновку: прямий і зворотний 4. Стратегії вибору правил при логічному висновку 5. Методи представлення й обробки нечітких знань в продукційних системах 6. Переваги та недоліки правил-продукцій як методу представлення знань	8
Тема 6. Семантичні мережі. 1. Основні поняття семантичних мереж: уявлення об'єктів та відносин між ними як орієнтованого графа 2. Типи відносин у семантичних мережах 3. Класифікація семантичних мереж 4. Принципи обробки інформації у семантичних мережах 5. Використання семантичних мереж	8
Тема 7. Фрейми і об'єкти. 1. Основні поняття фрейму: слоти, приєднані процедури-слуги і процедури-демони, успадкування властивостей 2. Зв'язок поняття фрейму і об'єкта в об‘єетно-орієнтованому програмуванні 3. Мережі фреймів 4. Приклади мов інженерії знань, заснованих на фреймах: FRL і KRL	8
Тема 8. Нейронні мережі. 1. Основні поняття про природні та штучні нейронні мережі і нейрони 2. Формальний нейрон Маккаллок-Питтса	8

3. Нейронна мережа як механізм, якого навчають розпізнаванню образів або адекватної реакції на вхідні сигнали (вхідну інформацію) 4. Класифікація нейронних мереж 5. Переваги та недоліки нейронних мереж як методу представлення й обробки знань	
Тема 9. Методи придбання знань. 1. Основні поняття методів навчання 2. Класифікація методів навчання за способом навчання: емпіричні та аналітичні, по глибині навчання - символьні (поверхневі) і на основі знань (глибинні) 3. Зв'язок цієї класифікації з поняттями індуктивного виводу, виведення за аналогією, навчання на прикладах 4. Індукція Мілля. Недоліки цього методу 5. ДСМ-метод. Визначення індуктивного виводу	8
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. Аналіз даних та знань : навчальний посібник / Литвин В. В., Пасічник В. В., Нікольський Ю. В. – Львів : Магнолія-2006 , 2021. – 276 с. URL:https://magnolia.lviv.ua/wp-content/uploads/2024/04/Analiz-dannykh-ta-znan_zmist.pdf

2. Data Mining : пошук знань в даних / Гладун А. Я., Рогушина Ю. В. – К. : ТОВ «ВД «АДЕФ-Україна», 2016. – 452 с. URL: https://www.old.nas.gov.ua/siaz/Ways_of_development_of_Ukrainian_science/article/16098.063.pdf

3. Черняк О. І. Інтелектуальний аналіз даних : підручник / О. І. Черняк, П. В. Захарченко. – К. : Знання, 2014. – 599 с.URL: https://files.znu.edu.ua/files/Bibliobooks/Inshi54/0040761.pdf

Додаткова література

1. Любунь З. М. Основи теорії нейромереж / З. М. Любунь /: Текст лекцій. – Львів: Видавничий центр ЛНУ імені Івана Франка, 2007. –142 с.URL: https://f.eruditor.link/file/236389/

2. Інтелектуальний аналіз даних : навчальний посібник / А. О. Олійник, С. О. Субботін, О. О. Олійник. – Запоріжжя : ЗНТУ, 2012. – 278 с.URL: https://ru.scribd.com/document/460020140/%D0%9E%D0%BB%D1%96%D0%B9%D0%BD%D0%B8%D0%BA-%D0%90-%D0%9E-%D0%86%D0%BD%D1%82%D0%B5%D0%BB%D0%B5%D0%BA%D1%82%D1%83%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9-%D0%B0%D0%BD%D0%B0%D0%BB%D1%96%D0%B7-%D0%B4%D0%B0%D0%BD%D0%B8%D1%85

3. Data Mining and Image Processing Toolkits. – [Електронний ресурс]. – Режим доступу http://datamining.itsc.uah.edu/adam
4. www.drweb.com – Лабораторія DrWeb.
5. www.drweb.com – Лабораторія DrWeb.
6. Персональні навчальні системи кафедри кібербезпеки НТУ "ХПІ" за дисципліною "Презентація та обробка знань" https://iiiii-my.sharepoint.com/:f:/g/personal/

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
0,6	0,4		

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, K, 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** Станіслав МІЛЕВСЬКИЙ