



Силабус освітнього компонента

Програма навчальної дисципліни



Комплексний тренінг

Шифр та назва спеціальності

125 – Кібербезпека та захист інформації

Інститут

ННІ комп'ютерних наук та інформаційних технологій (320)

Освітня програма

Кібербезпека

Кафедра

Кібербезпеки (328)

Рівень освіти

Бакалавр

Тип дисципліни

Спеціальна (фахова), Обов'язкова

Семестр

8

Мова викладання

Українська

Викладачі, розробники



МІЛЕВСЬКИЙ Станіслав Валерійович

stanislav.milevskyi@khpi.edu.ua

кандидат економічних наук, доцент кафедри кібербезпеки НТУ «ХПІ».

Автор понад 100 наукових та навчально-методичних праць. Науковий Гарант освітньо-наукової програми другого (магістерського) рівня вищої освіти. Провідний лектор з дисциплін: «Основи математичного моделювання систем безпеки», «Англійська мова в академічних застосунках», «Моделювання кіберфізичних дій» у студентів бакалавріата та магістратури.

[Детальніше про викладача на сайті кафедри](#)



ВОРОПАЙ Наталя Ігорівна

voropay.n@gmail.com

Кандидат технічних наук, доцент кафедри кібербезпеки НТУ «ХПІ».

Автор понад 30 наукових та навчально-методичних праць. Провідний лектор з дисциплін: «Технології програмування Ч.1», «Децентралізовані системи», «Захист об'єктів критичної інфраструктури», «Антивірусний захист інформації», «Блокчейн та смарт-технології в електронному документообігу».

[Детальніше про викладача на сайті кафедри](#)

Загальна інформація

Анотація

Навчальна дисципліна "Комплексний тренінг" є обов'язковою навчальною дисципліною.

Дисципліна спрямована на набуття студентами практичних навичок щодо виявлення та протидії сучасним загрозам в кіберпросторі.

Мета та цілі дисципліни

Формування у студентів практичних навичок щодо виявлення та протидії сучасним загрозам в кіберпросторі на основі відпрацювання практичних завдань.

Формат занять

Лекції, лабораторні роботи, самостійна робота, консультації. Підсумковий контроль – залік.

Компетентності

- КЗ 1. Здатність застосовувати знання у практичних ситуаціях.
- КЗ 2. Знання та розуміння предметної області та розуміння професії.
- КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.
- КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
- КЗ 5. Здатність до пошуку, оброблення та аналізу інформації
- КЗ 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
- КЗ 7. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
- КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.
- КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.
- КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.
- КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.
- КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.
- КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.
- КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).
- КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.
- КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.
- КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.
- КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.
- 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.

Результати навчання

РН-1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;

- РН-2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;
- РН-3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.
- 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-5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.
- РН-6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.
- РН-7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.
- РН-8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.
- РН-9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.
- РН-10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.
- РН-11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.
- РН-12. Розробляти моделі загроз та порушника.
- РН-13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.
- РН-14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.
- РН-15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
- РН-16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.
- РН-17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.
- РН-18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
- РН-19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.
- РН-20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.
- РН-21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
- РН-22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.
- РН-23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
- РН-24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).
- РН-25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних

(автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.

РН-26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.

РН-27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.

РН-28. 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.

РН-29. 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.

РН-30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.

РН-31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.

РН-32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.

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

РН-34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та\або кібербезпеки відповідно до цілей і завдань організації.

РН-35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки.

РН-36. Виявляти небезпечні сигнали технічних засобів.

РН-37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витoku технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації.

РН-38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.

РН-39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.

РН-40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.

РН-41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.

РН-42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і\або кібербезпеки.

РН-43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та\або кібербезпеки для розслідування інцидентів.

РН-44. 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.

РН-45. Застосовувати різні класи політик інформаційної безпеки та\або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.

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

- РН-47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.
- РН-48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.
- РН-49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.
- РН-50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).
- РН-51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах.
- РН-52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.
- РН-53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.
- РН-54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 24 год., лабораторні роботи – 36 год., самостійна робота – 60 год.

Передумови вивчення дисципліни (пререквізити)

Антивірусний захист інформації, Комплексні системи 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 проекти, майстер-класи.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Впровадження коду.

Виявлення ін'єкцій, таких як SQL, NoSQL, ОС та ін'єкція LDAP, які виникають, коли ненадійні дані надсилаються інтерпретатору як частина команди чи запиту.

Тема 2. Некоректна автентифікація і управління сесією.

Виявлення функцій іплікації, які пов'язані з автентифікацією та керуванням сеансом, що дозволяє зловмисникам компрометувати паролі, ключі або скельні маркери або використовувати інші недоліки впровадження, щоб тимчасово або назавжди припустити особистість інших користувачів.

Тема 3. Міжсайтовий скриптинг (XSS).

Виявлення веб-додатків та API, які не захищені належним чином. Зловмисники можуть вкрати або змінити такі слабко захищені дані, щоб вчинити шахрайство з кредитною карткою, крадіжку особи або інші злочини.

Тема 4. Небезпечні прямі посилання на об'єкти.

Аналіз старих або погано налаштованих процесорів XML оцінюють посилання зовнішніх об'єктів у документах XML. Зовнішні об'єкти можуть використовуватися для розкриття внутрішніх файлів за допомогою обробника URI файлів, обміну внутрішніми файлами, сканування внутрішніх портів, віддаленого виконання коду та відмови в атаці служби.

Тема 5. Небезпечна конфігурація.

Аналіз обмеження щодо дозволених користувачів, які дозволено робити, часто не виконуються належним чином. Зловмисники можуть використовувати ці недоліки для доступу до несанкціонованих функціональних можливостей та / або даних, таких як доступ до облікових записів інших користувачів, перегляд конфіденційних файлів, зміна даних інших користувачів, зміна прав доступу тощо.

Тема 6. Витік чутливих даних – оцінка конфігурації безпеки.

Зазвичай це результат небезпечних конфігурацій за замовчуванням, неповних або спеціальних конфігурацій, відкритого хмарного сховища, неправильно налаштованих заголовків HTTP та багатослівних повідомлень про помилки, що містять конфіденційну інформацію. Не тільки всі операційні системи, рамки, бібліотеки та додатки повинні бути надійно налаштовані, але вони повинні бути виправлені / модернізовані своєчасно.

Тема 7. Відсутність контролю доступу до функціонального рівня.

Визначення недоліків XSS, які виникають щоразу, коли програма включає недовірені дані на новій веб-сторінці без належної валідації або не відкриття, або оновлює наявну веб-сторінку за допомогою наданих користувачем даних за допомогою API браузера, який може створювати HTML або JavaScript. XSS дозволяє зловмисникам виконувати скрипти в браузері жертви, які можуть захоплювати сесии користувачів, знищувати веб-сайти або перенаправляти користувача на шкідливі сайти.

Тема 8. Підробка міжсайтових запитів (CSRF).

Оцінка небезпечної десеріалізації, яка часто призводить до віддаленого виконання коду. Навіть якщо дефери дезаріалізації не призводять до віддаленого виконання коду, їх можна використовувати для виконання атак, включаючи атаки відтворення, атаки ін'єкції та напади ескалції привілеїв.

Тема 9. Використання компонентів з відомими уразливостями.

Аналіз компонент, таких як бібліотеки, рамки та інші програмні модулі, які працюють із тими ж привілеями, що і додаток. Якщо використовується вразливий компонент, така атака може полегшити серйозні втрати даних або захоплення сервера. Програми та API, що використовують компоненти з відомою вразливістю, можуть підірвати захисні програми та включити різні атаки та впливи.

Тема 10. Невалідовані редіректи.

Виявлення недостатнього обліку та моніторингу у поєднанні з відсутньою або неефективною інтеграцією з реакцією на інцидент дозволяє зловмисникам надалі атакувати системи, підтримувати стійкість, перетворювати на більші кількості систем, а також підробляти, витягувати або знищувати дані. Більшість досліджень щодо порушення виявляють час виявлення порушення понад 200 днів, як правило, виявляються зовнішніми сторонами, а не внутрішніми процесами чи моніторингом.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Впровадження коду.

Тема 2. Некоректна автентифікація і управління сесією.

Тема 3. Міжсайтовий скриптинг (XSS).

Тема 4. Небезпечні прямі посилання на об'єкти.

Тема 5. Небезпечна конфігурація.

Тема 6. Витік чутливих даних – оцінка конфігурації безпеки.

Тема 7. Відсутність контролю доступу до функціонального рівня.

Тема 8. Підробка міжсайтових запитів (CSRF).

Тема 9. Використання компонентів з відомими уразливостями.

Тема 10. Невалідовані редіректи.

Самостійна робота

Самостійна робота студента є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час. Під час самостійної роботи студенти вивчають лекційний матеріал, готуються до лабораторних робіт, контрольних

робіт, заліків та іспитів. Студентам також рекомендуються додаткові матеріали (відео, статті) для самостійного вивчення та аналізу.

Неформальна освіта

В рамках неформальної освіти згідно відповідного Положення (<http://surl.li/pxssv>), освітня компонента або її окремі теми можуть бути враховано у разі самостійного проходження професійних курсів/тренінгів, отримання громадянської освіти, онлайн освіти, професійного стажування тощо.

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

Література та навчальні матеріали

Основна література:

1. Kali Linux Web Penetration Testing Cookbook, Second Edition (Packt Publishing) URL: <https://www.packtpub.com/product/kali-linux-web-penetration-testing-cookbook-second-edition/9781788991513>.
2. Зразок звіту з тестування на проникнення URL: <https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf>.
3. Зразок технічного звіту з проникнення URL: <https://tbgscurity.com>.
4. OWASP Top 10: issues in the 10 most critical security risk categories in your web applications URL: https://www.sonarqube.org/features/security/owasp/?gads_campaign=Europe-1-Generic&gads_ad_group=OWASP&gads_keyword=owasp%20top%2010&gclid=CjwKCAiAsNKQBhAPEiwAB-I5zQywwzTKai6fcrlMphlAn21CRehrI0q9DEjUZNPtHUoDt5V_bVpLm4RoCllkQAvD_BwE.
5. Технології захисту інформації. / С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с.
<http://kist.ntu.edu.ua/textPhD/tzi.pdf>
6. Євсєєв С.П. Кібербезпека: основи кодування та криптографії/ С.П. Євсєєв, О.В. Мілов, С.Е. Остапов, О.В. Северінов. – Харків: Вид. "Новий Світ-2000", 2023. – 657 с.
https://acrobat.adobe.com/id/urn%3Aaaid%3Asc%3AEU%3A3c427761-01ab-4365-88f6-37f76ca508c5/?x_api_client_id=chrome_extension_viewer&bookmarkAcrobat=true&x_api_client_location=bookmark&filetype=application%2Fpdf&viewer%21megaVerb=group-discover

Додаткова література :

7. Встановлення Metasploitable 2 URL: <https://metasploit.help.rapid7.com/docs/metasploitable-2>.
8. Збірка Metasploitable 3 URL: <https://github.com/rapid7/metasploitable3>.
9. Synergy of building cybersecurity systems: monograph / S. Yevseyev, V. Ponomarenko, O. Laptiev, O. Milov and others. - Kharkiv: PC TECHNOLOGY CENTER, 2021. - 188 p. URL: <https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju>
10. Models of socio-cyber-physical systems security: monograph / S. Yevseyev, Yu. Khokhlachova, S. Ostapov, O.Laptiev and others. - Kharkiv: PC TECHNOLOGY CENTER, 2023. - 168 p. URL: <https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju>
11. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseyev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. - Kharkiv: PC TECHNOLOGY CENTER, 2022. - 196 p. URL: <https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju>.

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:

- лабораторні роботи: 30% семестрової оцінки;
- самостійна робота: 10% семестрової оцінки;
- реферат: 20% семестрової оцінки;
- залік: 40% семестрової оцінки

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

Студент 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

28.08.2024



Завідувач кафедри

Сергій ЄВСЕЄВ

28.08.2024



Гарант ОП

Сергій ЄВСЕЄВ