**Силабус освітнього компонента**
Програма навчальної дисципліни

# Основи наукових досліджень

Шифр та назва спеціальності
125 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій (320)

Освітня програма
Освітньо-професійна програма Кібербезпека

Кафедра
Кібербезпеки (328)

Рівень освіти
Магістр

Тип дисципліни
Спеціальна (фахова) підготовка, Обов'язкова

Семестр
1

Мова викладання
Українська

## Викладачі, розробники

**ЄВСЄЄВ Сергій Петрович**

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

Кількість наукових публікацій: понад 350, з них патентів на корисну модель 42, 17 монографій, з яких 9 колективних монографій, 31 навчальний посібник, з яких 4 з грифом Міністерства освіти і науки України, 163 статті у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus. Провідний лектор з дисциплін: «Менеджмент інформаційної безпеки», «Введення в мережі», «Безпека банківських систем» , «Гібридні війни та національна безпека», «Аудит та моніторинг корпоративних мереж», «Blockchain: основи та приклади застосування», «Основи смарт-контрактів», «Основи кібербезпеки» у студентів бакалавріата та магістратури, Розділ «Методи і технології моніторингу та аудиту інформаційної безпеки», «Методи побудови постквантових криптосистем», «Новітні технології забезпечення кібербезпеки на основі технології блокчейн» для аспірантів
Детальніше про викладача на сайті кафедри

## Загальна інформація

### Анотація

Навчальна дисципліна «Основи наукових досліджень» належить до нормативних, спрямована на поглиблення у студентів знань щодо специфіки наукових досліджень, вивчення термінології та методології сучасної науки, застосування отриманих знань на практиці в освітньому та дослідницькому процесах. Дисципліна орієнтує на вибір методів та інструментарію наукових досліджень, дотримання принципів академічної доброчесності.

### Мета та цілі дисципліни

Ознайомлення з теоретичними засадами науково-дослідної діяльності, надання методичних рекомендацій щодо виконання конкретних видів наукових, навчально-дослідних та студентських робіт..

## Формат занять

Лекції, практичні заняття, самостійна робота, консультації. Підсумковий контроль – іспит.

## 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.
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.
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.
КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань нформаційної безпеки та/або кібербезпеки.

## 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 150 год. (5 кредитів ECTS): лекції – 32 год., практичні заняття – 32 год., самостійна робота – 86 год.

## Передумови вивчення дисципліни (пререквізити)

Англійська мова в академічних застосунках. Цифрова криміналістика.

## 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

## Теми лекційних занять

Тема 1. Основні визначення та поняття.
Що таке наукові дослідження: мета, методи та значення. Типи наукових досліджень: теоретичні та експериментальні підходи. Етапи проведення наукового дослідження.
Тема 2. Класифікація та основні етапи науково-дослідних робіт.
Класифікація науково-дослідних робіт. Основні етапи. Додаткові аспекти досліджень.
Тема 3. Наукове дослідження та методика його виконання.
Рівні наукового дослідження. Основні методи емпіричного дослідження. Обробка результатів експерименту. Метод індукції. Основні методи теоретичного пізнання. Структура і функції наукової теорії.
Тема 4. Вибір теми та планування наукових досліджень.
Основні поняття. Обгрунтування актуальності теми. Новизна ідеї. Планування наукових досліджень. Вивчення та аналіз літературних джерел за темою досліджень. Структура наукової статті. Структура змісту магістерської роботи.
Тема 5. Вивчення та аналіз літературних джерел за темою досліджень.
Як правильно робити огляд літератури: аналіз джерел. Використання наукових баз даних та бібліографічних менеджерів. Стилі цитування (APA, MLA, Chicago) та уникнення плагіату.
Тема 6. Методологія наукових досліджень.
Якісні та кількісні методи дослідження: переваги та недоліки. Спостереження, експеримент, анкетування та інші методи збору даних. Вибір методів та інструментів для дослідження.
Тема 7. Аналіз та інтерпретація даних.
Статистичні методи аналізу даних: основи та практичне застосування. Візуалізація даних: створення графіків, таблиць та діаграм. Як інтерпретувати результати та робити висновки.
Тема 8. Етика наукових досліджень.
Етичні норми в науці: чесність, прозорість і відповідальність. Проблеми плагіату та фабрикації даних. Роль етичних комісій у дослідженнях.
Тема 9. Інновації та роль міждисциплінарних досліджень.
Як міждисциплінарний підхід стимулює нові відкриття. Приклади успішних міждисциплінарних досліджень. Виклики та можливості співпраці між різними науками.
Тема 10. Тенденції в сучасних наукових дослідженнях.
Використання великих даних (Big Data) у наукових дослідженнях. Роль штучного інтелекту в науковому аналізі. Глобалізація науки: міжнародні проекти та спільні дослідження.

## Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

## Теми лабораторних робіт

Тема 1. Еволюція науки. теоретичні принципи та методологія науки.
Тема 2. Аналіз наукової публікації.
Тема 3. Організація виконання розробки автоматизованої інформаційної системи.
Тема 4. Методологія наукових досліджень.
Тема 5. Підготовка наукової публікації.
Тема 6. Підготовка дисертаційної роботи.

## 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. Мазур О.В. Основи наукових досліджень : навч. посіб. Для студ. вищих навч. заклад. філол. спец. /О. В. Мазур, О.В. Подвойська, С. В. Радецька. – Вінниця : Нова Книга, 2013. – 120с. https://www.google.com.ua/books/edition/_/jl3XCQAAQBAJ?hl=ru&gbpv=1&pg=PP1&dq=inauthor:%22%D0%9C%D0%B0%D0%B7%D1%83%D1%80+%D0%9E.+%D0%92.+%D1%82%D0%B0+%D1%96%D0%BD.%22
2. Данильян О. Г. Методологія наукових досліджень : підручник / О. Г. Данильян, О. П. Дзьобань. – Харків : Право, 2019. – 368 с.
https://library.nlu.edu.ua/POLN_TEXT/SENMK/OMND.pdf
3. Методологія та організація наукових досліджень : навч. посіб. / І. С. Добронравова, О. В. Руденко, Л. І. Сидоренко та ін. ; за ред. І. С. Добронравової (ч. 1), О. В. Руденко (ч. 2). – К. : ВПЦ "Київський університет", 2018. – 607 с.
http://www.philsci.univ.kiev.ua/biblio/Methodol.pdf
4. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
5. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
6. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. – Kharkiv: PC TECHNOLOGY CENTER, 2022. – 196 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju

### Додаткова література :

7. "Research Design: Qualitative, Quantitative, and Mixed Methods Approaches", John W. Creswell (2017)
https://www.ucg.ac.me/skladiste/blog_609332/objava_105202/fajlovi/Creswell.pdf.
8. "How to Write a Lot: A Practical Guide to Productive Academic Writing", Paul J. Silvia (2018)
https://books.google.com.ua/books/about/How_to_Write_a_Lot.html?id=xiCbEAAAQBAJ&redir_esc=y
9. "Social Research Methods", Alan Bryman (2021)
https://www.academia.edu/45262372/Social_Research_Methods
10. Про затвердження Вимог до оформлення дисертації : Наказ Міністерства освіти і науки України від 12.01.2017р. № 40 https://zakon.rada.gov.ua/laws/show/z0155-17#Text

## Система оцінювання

### Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:
- практичні заняття: 30% семестрової оцінки;
- самостійна робота: 10% семестрової оцінки;
- контрольна робота: 20% семестрової оцінки;
- іспит: 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
Ольга КОРОЛЬ