ПРОЄКТ
Розглянуто на засіданні кафедри 17.01.2025 Протокол № 8

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

ЗАТВЕРДЖУЮ
Ректор НТУ «ХПІ»

_____ Євген СОКОЛ

«___» _____ 2025 р.

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРБЕЗПЕКА»

Другого (магістерського) рівня вищої освіти

за спеціальністю **F5 – Кібербезпека та захист інформації**

галузі знань **F – Інформаційні технології**

кваліфікація **магістр з кібербезпеки та захисту інформації**

ЗАТВЕРДЖЕНО
ВЧЕНОЮ РАДОЮ НТУ «ХПІ»
Голова вченої ради

_____/ Євген СОКОЛ

Протокол № _____
від «___»_____ 2025 р.

Харків 2025 р.

ПРОЄКТ
Розглянуто на засіданні кафедри 17.01.2025 Протокол № 8

ЛИСТ ПОГОДЖЕННЯ

Освітньо-професійної програми Кібербезпека

Рівень вищої освіти	другий (магістерський)
Галузь знань	F Інформаційні технології
Спеціальність	F5 «Кібербезпека та захист інформації»
Кваліфікація	магістр з кібербезпеки та захисту інформації

СХВАЛЕНО
Робочою групою ОПП із спеціальності
«Кібербезпека та захист інформації»
Гарант ОПП

_____ Ольга КОРОЛЬ

«____»_____2025 р.

РЕКОМЕНДОВАНО
Методичною радою НТУ «ХПІ»
Заступник голови методичної ради

_____ Руслан МИГУЩЕНКО

«____»_____2025 р.

ПОГОДЖЕНО
Завідувач кафедри
кібербезпека_____

_____ Сергій ЄВСЕЄВ

«____»_____2025 р.

ПОГОДЖЕНО
Директор навчально-наукового інституту
комп'ютерних наук та інформаційних
технолгій _

_____ Михайло ГОДЛЕВСЬКИЙ

«____»_____2025 р.

ПОГОДЖЕНО
здобувач вищої освіти
(член робочої групи ОПП)
№ групи _КН-М1124

_____ Дмитро БОБЧЕНОК

«____»_____2025 р.

РЕЦЕНЗЕНТИ:

Продуктивні зауваження та відгуки на проєкт освітньо-професійної програми одержано від:

1. МОЛОДЕЦЬКА Катерина Валеріївна, доктор технічних наук, професор, професор кафедри менеджменту організацій Києво-Могилянської бізнес-школи Національний університет «Києво-Могилянська академія»
2. КОВТУН Владислав Юрійович, кандидат технічних наук, доцент, директор ТОВ “Сайфер”
3. ГОЛОВАШИЧ Сергій Олександрович, кандидат технічних наук, доцент директор ТОВ “Мікрокрипт Текнолоджіс”
4. ВОЛОЩУК Олена Борисівна, кандидат технічних наук, керівник освітніх програм ТОВ “Distributed Lab”.

Рецензії

ПРОЄКТ
Розглянуто на засіданні кафедри 17.01.2025 Протокол № 8

ПЕРЕДМОВА

Відповідає Стандарту вищої освіти другого (магістерського) рівня галузі знань F «Інформаційні технології», спеціальності F5 «Кібербезпека та захист інформації», затвердженого та введеного в дію наказом Міністерства освіти і науки України від 18.03.2021 р. № 332.

Розроблено робочою групою ОПП «Кібербезпека»
Навчально-наукового інституту комп'ютерних наук та інформаційних технолгій
Національного технічного університету «Харківський політехнічний інститут»
у складі:

Гарант освітньо-професійної програми

КОРОЛЬ Ольга Григорівна, кандидат технічних наук, доцент, доцент кафедри кібербезпеки.

Члени робочої групи ОПП :

1. ЄВСЕЄВ Сергій Петрович, доктор технічних наук, професор, завідувач кафедри кібербезпеки.
2. ПОГАСІЙ Сергій Сергійович, доктор технічних наук, доцент, професор кафедри кібербезпеки.
3. МІЛЕВСЬКИЙ Станіслав Валерійович, доктор технічних наук, доцент, професор кафедри кібербезпеки.
4. БОБЧЕНОК Дмитро Олександрович, студент групи КН- М1124.

1. ПРОФІЛЬ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ ЗА СПЕЦІАЛЬНІСТЮ F5 КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

1 – Загальна інформація	
Вищий навчальний заклад та структурний підрозділ	Національний технічний університет «Харківський політехнічний інститут», Навчально-науковий інститут комп'ютерних наук та інформаційних технолгій кафедра кібербезпеки
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Магістр Освітня кваліфікація: магістр з кібербезпеки та захисту інформації Кваліфікація в дипломі: магістр з кібербезпеки та захисту інформації
Офіційна назва освітньо-професійної програми	Кібербезпека
Тип диплому та обсяг освітньо-професійної програми	Диплом магістра, одиничний, 90 кредитів ЄКТС, термін навчання 1 рік 4 місяці
Наявність акредитації	Національне агентство забезпечення якості вищої освіти. Україна. Сертифікат № 6112 термін дії до 01.07.2029р.
Цикл/рівень	другий (магістерський) рівень вищої освіти; НРК України – 7 рівень, FQ-EHEA– другий цикл, EQF LLL – 7 рівень
Передумови	Наявність ступеня вищої освіти «бакалавр»
Мова викладання	Українська, англійська
Термін дії освітньо-професійної програми	Відповідно до терміну дії сертифікату про акредитацію. Переглядається щорічно
Посилання на постійне розміщення опису освітньо-професійної програми	https://blogs.kpi.kharkov.ua/v2/quality/dokumenty/diyuchy-osvitni-programy/osvitnij-riven-magistr/
2 – Мета освітньо-професійної програми	
Підготовка фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки, використовувати і впроваджувати технології та застосовувати засоби захисту в системах безпеки контуру бізнес-процесів.	
3 – Характеристика освітньо-професійної програми	
Предметна область (галузь знань, спеціальність)	Галузь знань: F "Інформаційні технології" Спеціальність: F5 "Кібербезпека та захист інформації" **Об'єкти вивчення:** – сучасні процеси дослідження, аналізу, створення та забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів на об'єктах

	інформаційної діяльності та критичних інфраструктур сфери інформаційної безпеки та/або кібербезпеки; – інформаційні системи (інформаційно-комунікаційні, інформаційно-телекомунікаційні, автоматизовані) та технології; - інфраструктура об'єктів інформаційної діяльності та критичних інфраструктур; – системи та комплекси створення, обробки, передачі, зберігання, знищення, захисту та відображення даних (інформаційних потоків); – інформаційні ресурси різних класів (в т.ч. державні інформаційні ресурси); – програмне та програмно-апаратне забезпечення (засоби) кіберзахисту; – системи управління інформаційною безпекою та/або кібербезпекою; – технології, методи, моделі та засоби інформаційної безпеки та/або кібербезпеки. **Цілі навчання:** Підготовка фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки. **Теоретичний зміст предметної області** Теоретичні засади наукоємних технологій, фізичні і математичні фундаментальні знання, теорії ідентифікації та прийняття рішень, системного аналізу, складних систем, моделювання та оптимізації процесів, теорія математичної статистики, криптографічного та технічного захисту інформації, теорії ризиків та інших міждисциплінарних теорій і практик у галузі інформаційної безпеки та/або кібербезпеки. **Методи, методики та технології** Методи, моделі, методики та технології створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, а також методи та моделі розробки та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформаційної безпеки та/або кібербезпеки. Технології, методи та моделі дослідження, аналізу, управління та забезпечення бізнес/операційних процесів із застосуванням сукупності нормативно-правових та організаційно-технічних методів і засобів захисту інформаційних ресурсів у кіберпросторі. **Інструменти та обладнання**. Засоби, пристрої, мережне устаткування та середовище, прикладне та спеціалізоване програмне забезпечення, автоматизовані системи та комплекси проектування,

	моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту даних (інформаційних потоків), а також методи і моделі теорії ризиків та управління інформаційними ресурсами при дослідженні і супроводженні об'єктів інформаційної діяльності у галузі інформаційної безпеки та/або кібербезпеки.
Орієнтація освітньо-професійної програми	Професійна підготовка фахівців у сфері кібербезпеки та захист інформації
Основний фокус освітньо-професійної програми та спеціалізації	Поглиблене вивчення проведення, як зовнішнього, так й внутрішнього аудиту з метою забезпечення безпеки контуру бізнес-процесів. Отримання сертифікатів курсів академії Cisco, сприяє підвищенню конкурентноспроможності на ринке праці, удосконаленню механізмів аудиту та захисту за мировими методиками. Ключові слова: кібербезпека, цифрова криміналістика, етнічний хакінг.
Особливості програми	Особливостями програми є формування у здобувачів навичок побудови комплексних систем захисту інформації для забезпечення безпеки контуру бізнес-процесів на основі сучасних технологій та програмних застосунків, в умовах розвитку цифрової економіки. Орієнтація на партнерство із вітчизняними та закордонними закладами освіти та науки, приватним сектором, науковцями та практиками, участь в міжнародних програмах спільних дипломів. Можливість навчатися англійською мовою.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Фахівці з кібербезпеки та захисту інформації можуть працювати, згідно з чинною редакцією Національного класифікатора України: Класифікатор професій ДК 003:2010, а саме: 2139.2 Аналітик загроз безпеки; 2139.2 Аналітик систем захисту інформації та оцінки вразливостей; 2139.2 Аналітик з безпеки інформаційно-комунікаційних систем; 2139.2 Дізнавач (сфера кібербезпеки та захисту інформації); 2139.2 Експерт з цифрової криміналістики (сфера кібербезпеки та захисту інформації); 2139.2 Експерт-криміналіст судової експертизи (сфера кібербезпеки та захисту інформації); 2139.2 Слідчий з кіберзлочинів.
Подальше навчання	Продовження освіти за третім (освітньо-науковим) рівнем вищої освіти. Набуття додаткових кваліфікацій в системі освіти дорослих.

5 – Викладання та оцінювання	
Викладання та навчання	У процесі викладання передбачено застосування таких навчальних технологій, як: лекції, лабораторні роботи, практичні заняття, робота в малих групах, презентації, що розвивають комунікативні та лідерські навички, самостійна робота з літературними джерелами.
Оцінювання	Рейтингова система оцінювання. Поточний та підсумковий контроль знань (опитування, контрольні та індивідуальні завдання, тестування тощо), заліки та іспити (усні та письмові), публічний захист кваліфікаційної роботи чи проекту. Система оцінювання передбачає застосування міжнародної системи ЄКТС (з оцінками A, B, C, D, E, F), національної системи (з оцінками «відмінно», «добре», «задовільно» та «незадовільно»), а також 100-бальної системи закладу вищої освіти зі встановленою системою відповідності.
6 – Програмні компетентності	
Інтегральна компетентність	Здатність особи розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.
Загальні 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).
Фахові компетентності	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. КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. 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 інформаційної безпеки та/або кібербезпеки.
7 – Результати навчання	
Результати навчання за спеціальністю	РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення

(визначені стандартомвищої освіти спеціальності)	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.
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	Відповідає кадровим вимогам щодо забезпечення провадження освітньої діяльності у сфері вищої освіти згідно з діючим законодавством України (Постанова Кабінету Міністрів України “Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти” від 30 грудня 2015 р. № 1187, зі змінами, внесеними згідно з Постановою КМУ № 365 від 24.03.2021. Додаток 15-16). До викладання залучаються викладачі-практики, фахівці та співробітники ІТ-компаній, а також закордонні фахівці.
Матеріально-технічне забезпечення	Відповідає вимогам щодо матеріально-технічного забезпечення провадження освітньої діяльності у сфері вищої освіти згідно з діючим законодавством України (Постанова кабінету міністрів України «Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти» від 30 грудня 2015 р. № 1187, зі змінами, внесеними згідно з Постановою КМ № 365 від 24.03.2021, додаток 17). У наявності є аудиторний фонд та мультимедійне обладнання, кіберполігон.
Інформаційне та навчально-методичне забезпечення	Відповідає технологічним вимогам щодо навчально-методичного та інформаційного забезпечення освітньої діяльності у сфері вищої освіти згідно з діючим законодавством України (Постанова Кабінету Міністрів України “Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти” від 30 грудня 2015 р., № 1187, (зі змінами, внесеними згідно з Постановою КМУ № 365 від 24.03.2021. Додаток 18). Доступ до електронного репозитарію НТУ «ХПІ» (eNTUKhPIIR) через мережу Інтернет (у тому числі університетську мережу Wi-Fi).
9 – Академічна мобільність	
Національна кредитна мобільність	На основі двосторонніх договорів між Національним технічним університетом «Харківський політехнічний інститут» та провідними технічними університетами України. Регламентується «Положенням про академічну мобільність студентів, аспірантів, докторантів, науково-педагогічних та наукових працівників НТУ «ХПІ».
Міжнародна кредитна мобільність	На основі двосторонніх договорів. Польсько-українська програма обміну та спільних дипломів для підготовки

	магістрів за спеціальністю «Кібербезпека та захист інформації» з Університетом у Бєльсько-Бялій (м. Бельсько-Бяла, Польща).
Навчання іноземних здобувачів освіти	Підготовка іноземних громадян та осіб без громадянства здійснюється українською або англійською мовою відповідно до вимог Закону України «Про вищу освіту»..

2. ПЕРЕЛІК ОСВІТНІХ КОМПОНЕНТ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ «КІБЕРБЕЗПЕКА» ТА ЇХ ЛОГІЧНА ПОСЛІДОВНІСТЬ

2.1 Перелік компонент ОПП

Код н/д	Компоненти освітньо-професійної програми	Кількість кредитів	Форма підсумкового контролю
1. Обов'язкові освітні компоненти (здобувачі вищої освіти – громадяни України)			
1.1 Загальна підготовка			
ЗП 1	*Англійська мова в академічних застосунках*	*4,0*	*Екзамен*
ЗП 2	*Інноваційне підприємництво та управління стартап-проєктами*	*3,0*	*Екзамен*
ЗП 3	*Етичний хакінг*	*3,0*	*Екзамен*
ЗП 4	*Безпека Інтернет-речей та сервісів*	*4,0*	*Залік*
1.2. Спеціальна (фахова) підготовка			
СП1	*Основи наукових досліджень*	*5,0*	*Екзамен*
СП2	*Безпека безперервності бізнес-процесів*	*5,0*	*Залік*
СП3	*Мережева та хмарна безпека*	*4,0*	*Екзамен*
СП4	*Безпека систем Клієнт-Сервер*	*4,0*	*Залік*
СП5	*Цифрова криміналістика*	*4,0*	*Залік*
2. Практична підготовка			
ПП	*Переддипломна практика*	*12,0*	*Залік*
3. Атестація			
СП	*Атестація*	*10,0*	
Загальний обсяг обов'язкових компонентів		58	
4. Вибіркові освітні компоненти (здобувачі вищої освіти – громадяни України)			
4.1 Освітні компоненти вільного вибору професійної підготовки згідно переліку			
ОКВП1	*ОК ВВ ПП 1*	*4,0*	*Залік*
ОКВП2	*ОК ВВ ПП 2*	*4,0*	*Залік*
ОКВП3	*ОК ВВ ПП 3*	*4,0*	*Залік*
ОКВП4	*ОК ВВ ПП 4*	*4,0*	*Залік*
ОКВП5	*ОК ВВ ПП 5*	*4,0*	*Залік*
ОКВП6	*ОК ВВ ПП 6*	*4,0*	*Залік*
4.2 Освітні компоненти загальної підготовки згідно переліку			
ОКВЗ1	*ОК ВВ ЗП 1*	*4,0*	*Залік*
ОКВЗ2	*ОК ВВ ЗП 2*	*4,0*	*Залік*
Загальний обсяг вибіркових компонент:		32	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ:		**90**	

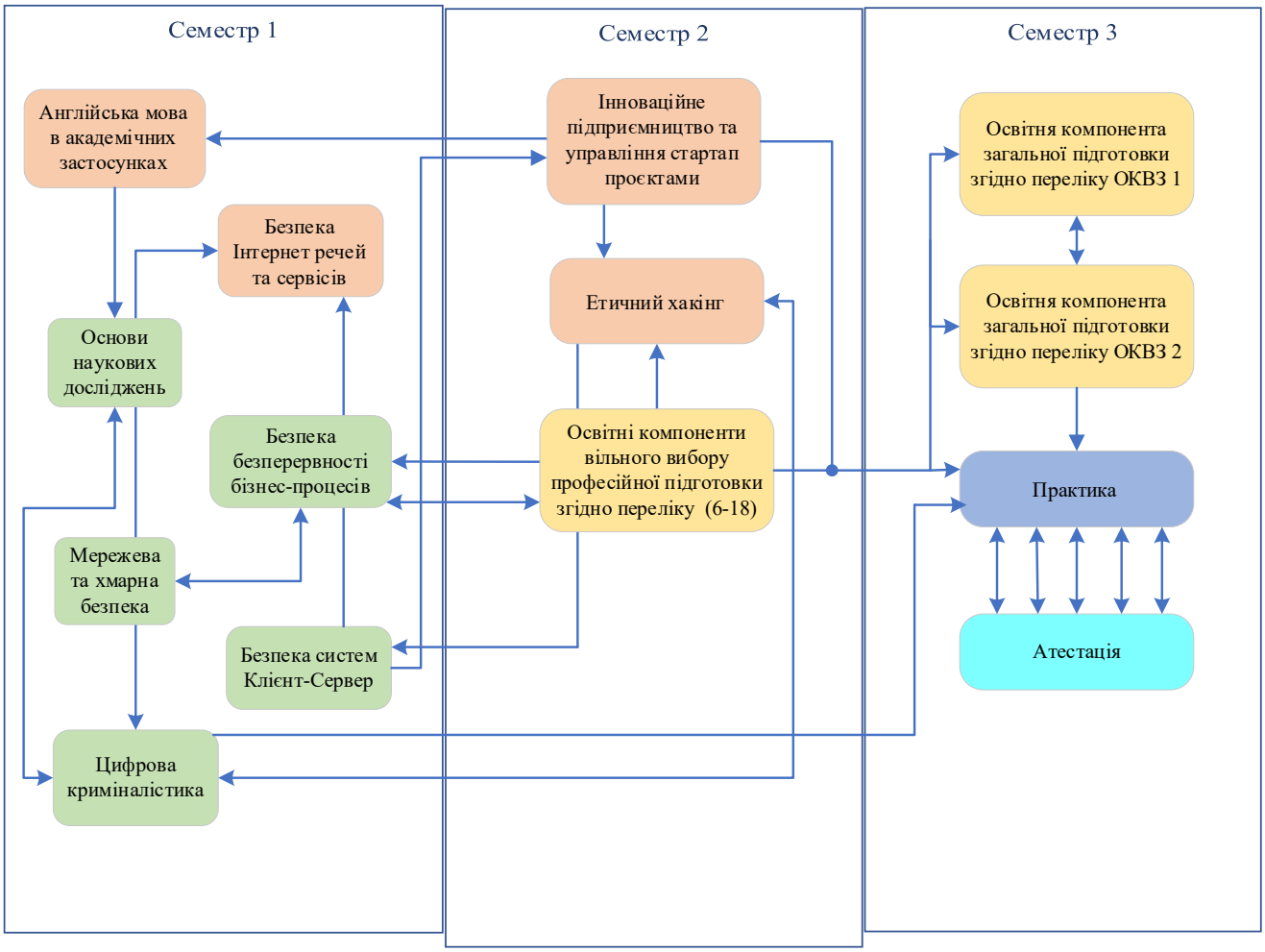
2.2 Розподіл змісту освітньо-професійної програми за групами компонентів та циклами підготовки

№ п/п	Цикл підготовки	Обсяг навчального навантаження здобувача вищої освіти (кредитів ECTS / %)		
		Обов'язкові компоненти освітньо-професійної програми	Вибіркові компоненти освітньо-професійної програми	Всього за весь термін навчання
1	Загальна підготовка	14 / 15,5	-	**14 / 15,5**
2	Спеціальна (фахова) підготовка	44 / 48,9	-	**44 / 48,9**
3	Дисципліни вільного вибору	-	32 / 35,6	**32 / 35,6**
Всього за весь термін навчання		**58 / 64,4**	**32 / 35,6**	**90 / 100**

3. ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі публічного захисту кваліфікаційної роботи.
Вимоги до кваліфікаційної роботи	Кваліфікаційна робота має розв'язувати складну задачу інформаційної безпеки та/або кібербезпеки і передбачати проведення досліджень та/або здійснення інновацій. Кваліфікаційна робота не повинна містити академічного плагіату, фабрикації, фальсифікації. Кваліфікаційна робота має бути розміщена на офіційному сайті (або у репозитарії) закладу вищої освіти або його підрозділу. Оприлюднення кваліфікаційних робіт з обмеженим доступом здійснюється відповідно до вимог законодавства.

4. СТРУКТУРНО-ЛОГІЧНА СХЕМА



5. ЗВЕДЕНА ТАБЛИЦЯ ФАХОВИХ КОМПЕТЕНТНОСТЕЙ ТА ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ

Фахові компетентності	Результати навчання
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.	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. РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. 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,

Фахові компетентності	Результати навчання
	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.
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.	РН2. Інтегрувати фундаментальні та спеціальні знання для розв’язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. 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. 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. 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. РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної

Фахові компетентності	Результати навчання
	безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.
КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.	РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. 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. 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

Фахові компетентності	Результати навчання
	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.
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.	РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки. 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. 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. 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. 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.
КФ5. Здатність до дослідження, системного аналізу та забезпечення	РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту,

Фахові компетентності	Результати навчання
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.	технології створення та використання спеціалізованого програмного забезпечення. 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. 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. РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.	РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. 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. 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. 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. РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної

Фахові компетентності	Результати навчання
	безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.
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.	РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. 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. 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. 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. РН21. Використовувати методи натурного, фізичного і комп’ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки. 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.
КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності та критичної інфраструктури, в інформаційних	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

Фахові компетентності	Результати навчання
системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.	інформаційної діяльності та критичної інфраструктури. 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. РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки. 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.
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.	РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. 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. 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. РН16. Приймати обґрунтовані рішення з

Фахові компетентності	Результати навчання
	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. 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. 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.
КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань 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. 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

Фахові компетентності	Результати навчання
	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.

6. МАТРИЦЯ ВІДПОВІДНОСТІ ВИЗНАЧЕНИХ СТАНДАРТОМ КОМПЕТЕНТНОСТЕЙ / РЕЗУЛЬТАТІВ НАВЧАННЯ ДЕСКРИПТОРАМ НРК

Класифікація компетентностей за НРК	Знання	Уміння	Комунікація	Автономія та відповідальність
ЗАГАЛЬНІ КОМПЕТЕНТНОСТІ				
КЗ1	Зн1,	Ум1, Ум3	К1	АВ1, АВ2
КЗ2	Зн1,	Ум1, Ум2, Ум3		АВ2, АВ3
КЗ3	Зн1	Ум2, Ум3		АВ1
КЗ4	Зн1	Ум3		АВ1, АВ2
КЗ5	Зн1	Ум2	К1	АВ1
СПЕЦІАЛЬНІ (ФАХОВІ) КОМПЕТЕНТНОСТІ				
КФ1	Зн1	Ум2		АВ2
КФ2	Зн1,	Ум2		АВ2
КФ3	Зн1	Ум1, Ум2, Ум3	К1	АВ1, АВ2
КФ4	Зн1,	Ум1, Ум2	К1	АВ1, АВ2
КФ5	Зн1,	Ум1, Ум2	К1	АВ1, АВ2
КФ6	Зн1	Ум1, Ум2	К1	АВ1
КФ7	Зн1	Ум1, Ум2	К1	АВ1
КФ8	Зн1	Ум1, Ум2	К1	АВ1
КФ9	Зн1	Ум1, Ум2	К1	АВ1
КФ10	Зн1	Ум1, Ум2, Ум3	К1	АВ1, АВ2

ПРОЄКТ
Розглянуто на засіданні кафедри 17.01.2025 Протокол № 8

7. МАТРИЦЯ ВІДПОВІДНОСТІ ВИЗНАЧЕНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ, КОМПЕТЕНТНОСТЕЙ ТА ОСВІТНІХ КОМПОНЕНТІВ

Результати навчання	**Компетентності**														
	Інтегральна компетентність														
	Загальні компетентності					**Спеціальні (фахові) компетентності**									
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10
РН 1	ЗП1, ЗП2, ЗП3, ЗП4, СП1, СП2, СП3, СП4, ПП		ЗП1, СП1, ПП			ЗП1, ЗП2, ЗП4, СП3, СП4, ПП									
РН 2		ЗП1, ЗП4, СП1, СП2, СП4, ПП	ЗП1, СП1, ПП			ЗП1, ЗП2, ЗП4, СП3, СП4, ПП	СП1, СП2, ПП	СП1, СП2, СП3, СП4, СП5, ПП							
РН 3	ЗП1, ЗП2, ЗП3, ЗП4, СП1, СП2, СП3, СП4, ПП					ЗП1, ЗП2, ЗП4, СП3, СП4, ПП									
РН 4	ЗП1, ЗП2, ЗП3, ЗП4, СП1,	ЗП1, ЗП4, СП1, СП2, СП4,	ЗП1, СП1, ПП	ЗП4, СП1, СП4, ПП		ЗП1, ЗП2, ЗП4, СП3, СП4,	СП1, СП2, ПП								

Результати навчання	**Компетентності**														
	Інтегральна компетентність														
	Загальні компетентності					**Спеціальні (фахові) компетентності**									
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10
	СП2, СП3, СП4, ПП	ПП				ПП									
РН 5			ЗП1, СП1, ПП		ЗП1, ЗП4, СП1, СП2, СП3, СП5, ПП		СП1, СП2, ПП								
РН 6	ЗП1, ЗП2, ЗП3, ЗП4, СП1, СП2, СП3, СП4, ПП			ЗП4, СП1, СП2, СП4, ПП		ЗП1, ЗП2, ЗП4, СП3, СП4, ПП		СП1, СП2, СП3, СП4, СП5, ПП		ЗП2, ЗП3, ЗП4, СП1, СП2, СП3, СП5, ПП	ЗП2, ПП	СП1, СП2, СП3, СП5, ПП		ЗП4, СП1, СП2, СП3, СП4, ПП	
РН 7	ЗП1, ЗП2, ЗП3, ЗП4, СП1, СП2, СП3, СП4, ПП		ЗП1, СП1, СП2, ПП				СП1, СП2, ПП								

Результати навчання	**Компетентності**														
	Інтегральна компетентність														
	Загальні компетентності					**Спеціальні (фахові) компетентності**									
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10
РН 8	ЗП1, ЗП2, ЗП3, ЗП4, СП1, СП2, СП3, СП4, ПП	ЗП1, ЗП4, СП1, СП2, СП4, ПП		ЗП4, СП1, СП2, СП4, ПП	ЗП1, ЗП4, СП1, СП2, СП3, СП5, ПП			ЗП3, СП1, СП2, СП3, СП4, СП5, ПП						ЗП4, СП1, СП2, СП3, СП4, ПП	ЗП1, ЗП4, СП1, ПП
РН 9	ЗП1, ЗП2, ЗП3, ЗП4, СП1, СП2, СП3, СП4, ПП	ЗП1, ЗП4, СП1, СП2, СП4, ПП	ЗП1, СП1, СП2, ПП	ЗП4, СП1, СП2, СП4, ПП					СП3, СП5, ПП					ЗП4, СП1, СП2, СП3, СП4, ПП	ЗП1, ЗП4, СП1, ПП
РН 10	ЗП1, ЗП2, ЗП3, ЗП4, СП1, СП2 СП3, СП4, ПП		ЗП1, СП1, СП2, ПП	ЗП4, СП1, СП2, СП4, ПП						ЗП2, ЗП3, ЗП4, СП1, СП2, СП3, СП5, ПП				ЗП4, СП1, СП2, СП3, СП4, ПП	
РН 11	ЗП1, ЗП2, ЗП3,		ЗП1, СП1, СП2,	ЗП4, СП1, СП2,							ЗП2, ПП				ЗП1, ЗП4, СП1,

Результати навчання	**Компетентності**														
	Інтегральна компетентність														
	Загальні компетентності					**Спеціальні (фахові) компетентності**									
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10
	ЗП4, СП1, СП2, СП3, СП4, ПП		ПП	СП4, ПП											ПП
РН 12	ЗП1, ЗП2, ЗП3, ЗП4, СП1, СП2, СП3, СП4, ПП		ЗП1, СП1, СП2, ПП	ЗП4, СП1, СП2, СП4, ПП					СП3, СП5, ПП			ЗП3, СП1, СП2, СП3, СП5, ПП			ЗП1, ЗП4, СП1, ПП
РН 13	ЗП1, ЗП2, ЗП3, ЗП4, СП1, СП2, СП3, СП4, ПП		ЗП1, СП1, СП2, ПП	ЗП4, СП1, СП2, СП4, ПП									СП3, ПП		ЗП1, ЗП4, СП1, ПП
РН 14	ЗП1, ЗП2, ЗП3, ЗП4, СП1, СП2,		ЗП1, СП1, СП2, ПП	ЗП4, СП1, СП2, СП4, ПП					СП3, СП5, ПП					ЗП4, СП1, СП2, СП3, СП4, ПП	ЗП1, ЗП4, СП1, ПП

Результати навчання	**Компетентності**														
	Інтегральна компетентність														
	Загальні компетентності					**Спеціальні (фахові) компетентності**									
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10
	СП3, СП4, ПП														
РН 15				ЗП4, СП1, СП2, СП4, ПП	ЗП1, ЗП4, СП1, СП2, СП3, СП5, ПП										ЗП1, ЗП4, СП1, ПП
РН 16	ЗП1, ЗП2, ЗП3, ЗП4, СП1, СП2, СП3, СП4, ПП	ЗП1, ЗП4, СП1, СП2, СП4, ПП	ЗП1, СП1, СП2, ПП	ЗП4, СП1, СП2, СП4, ПП				ЗП3, СП1, СП2, СП3, СП4, СП5, ПП	СП3, СП5, ПП	ЗП2, ЗП3, ЗП4, СП1, СП2, СП3, СП5, ПП	ЗП2, ПП	ЗП3, СП1, СП2, СП3, СП5, ПП		ЗП4, СП1, СП2, СП3, СП4, ПП	ЗП1, ЗП4, СП1, ПП
РН 17								ЗП3, СП1, СП2, СП3, СП4, СП5, ПП							ЗП1, ЗП4, СП1, ПП
РН 18	ЗП1, ЗП2, ЗП3, ЗП4,			ЗП4, СП1, СП2, СП4,	ЗП1, ЗП4, СП1, СП2,										ЗП1, ЗП4, СП1, ПП

Результати навчання	**Компетентності**														
	Інтегральна компетентність														
	Загальні компетентності					**Спеціальні (фахові) компетентності**									
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10
	СП1, СП2, СП3, СП4, ПП			ПП	СП3, СП5, ПП										
РН 19	ЗП1, ЗП2, ЗП3, ЗП4, СП1, СП2, СП3, СП4, ПП			ЗП4, СП1, СП2, СП4, ПП	ЗП1, ЗП4, СП1, СП2, СП3, СП5, ПП	ЗП1, ЗП2, ЗП4, СП3, СП4, ПП	СП1, СП2, ПП	ЗП3, СП1, СП2, СП3, СП4, СП5, ПП	СП3, СП5, ПП		ЗП2, ПП	ЗП3, СП1, СП2, СП3, СП5, ПП	СП3, ПП	ЗП4, СП1, СП2, СП3, ПП	
РН 20	ЗП1, ЗП2, ЗП3, ЗП4, СП1, СП2, СП3, СП4, ПП	ЗП1, ЗП4, СП1, СП2, СП4, ПП	ЗП1, СП1, СП2, ПП	ЗП4, СП1, СП2, СП4, ПП	ЗП1, ЗП4, СП1, СП2, СП3, СП5, ПП	ЗП1, ЗП2, ЗП4, СП3, СП4, ПП		ЗП3, СП1, СП2, СП4, СП5, ПП							
РН 21	ЗП1, ЗП2, ЗП3, ЗП4, СП1, СП2, СП3,	ЗП1, ЗП4, СП1, СП2, СП4, ПП	ЗП1, СП1, СП2, ПП	ЗП4, СП1, СП2, СП4, ПП		ЗП1, ЗП2, ЗП4, СП3, СП4, ПП		ЗП3, СП1, СП2, СП4, СП5, ПП		ЗП2, ЗП3, ЗП4, СП1, СП2, СП3, СП5,		ЗП3, СП1, СП2, СП3, СП5, ПП	СП3, ПП		

Результати навчання	**Компетентності**														
	Інтегральна компетентність														
	Загальні компетентності					**Спеціальні (фахові) компетентності**									
	КЗ 1	КЗ 2	КЗ 3	КЗ 4	КЗ 5	КФ 1	КФ 2	КФ 3	КФ 4	КФ 5	КФ 6	КФ 7	КФ 8	КФ 9	КФ 10
	СП4, ПП									ПП					
РН 22		ЗП1, ЗП4, СП1, СП2, СП4, ПП	ЗП1, СП1, СП2, ПП	ЗП4, СП1, СП2, СП4, ПП		ЗП1, ЗП2, ЗП4, СП3, СП4, ПП		ЗП3, СП1, СП2, СП4, СП5, ПП							
РН 23	ЗП1, ЗП2, ЗП3, ЗП4, СП1, СП2, СП3, СП4, ПП		ЗП1, СП1, СП2, ПП	ЗП4, СП1, СП2, СП4, ПП		ЗП1, ЗП2, ЗП4, СП3, СП4, ПП	СП1, СП2, ПП	СП1, СП2, СП3, СП4, СП5, ПП			ЗП2, ПП	ЗП3, СП1, СП2, СП3, СП5, ПП	СП3, ПП	ЗП4, СП1, СП2, СП3, СП4, ПП	

8. РЕЗУЛЬТАТИ ОБГОВОРЕННЯ ОСВІТНЬОЇ ПРОГРАМИ

Стейкхолдери (вказати ПІБ та посаду, місце роботи)	Рекомендація	враховано / частково враховано / не враховано	Примітка
Гарант ОПП, к.т.н., доц. Король О.Г. завідувач кафедри, д.т.н., професор Євсеєв С.П. Члени робочої групи ОПП	Освітньо-професійну програму привести у відповідність до вимог Стандарту вищої освіти за спеціальністю 125 Кібербезпека та захист інформації першого (бакалаврського) рівня вищої освіти, затвердженого та введеного в дію наказом Міністерства освіти і науки України від 24.10.2024р. № 1547.	Враховано. Зміни внесено.	
Гарант ОПП, к.т.н., доц. Король О.Г. завідувач кафедри, д.т.н., професор Євсеєв С.П. Члени робочої групи ОПП	Зміна шифру спеціальності та галузі знань (згідно з постановою Кабінету Міністрів України від 30 серпня 2024 р. No 1021).	Враховано. Зміни внесено.	
Волощук О. Б., к. т. н., керівник освітніх програм ТОВ “Distributed Lab”	Позитивний відгук. Без зауважень.	-	
Молодецька К. В., доктор технічних наук, професор, професор кафедри менеджменту організацій Києво-Могилянської бізнес-школи Національний університет «Києво-Могилянська академія»	Позитивний відгук. Без зауважень.	-	
Ковтун В. Ю., кандидат технічних наук, доцент, директор ТОВ “Сайфер”	Позитивний відгук. Без зауважень.	-	

Головашич С. О., кандидат технічних наук, доцент директор ТОВ “Мікрокрипт Текнолоджіс”	Позитивний відгук. Без зауважень.	-	

9. ПЛАН ВРАХУВАННЯ ЗАУВАЖЕНЬ ТА ВИПРАВЛЕННЯ НЕДОЛІКІВ ЗА ОСВІТНЬОЮ ПРОГРАМОЮ

Рекомендації, надані під час останньої акредитації	Період врахування (короткостроковий/довгостроковий/не доцільно враховувати)	Заходи, направлені на врахування рекомендацій	Терміни впровадження заходів
Рекомендації експертної групи та Галузевої експертної ради			
Рекомендація 1 Посилити інформування здобувачів з нормативними документами та основними положеннями академічної доброчесності.	Довгостроковий	Інформування проводится постійно під час проведення лекційних занять з дисципліни «Основи наукових досліджень»	Вересень 2025 н.р.
Рекомендація 2 Переглянути в наступній редакції ОПП перелік затверджених професійних стандартів в сфері кібербезпеки відповідно до Національного класифікатора професій України ДК 003:2010.	Довгостроковий	Оновлення у ОПП переліку затверджених професійних стандартів в сфері кібербезпеки відповідно до Національного класифікатора професій України ДК 003:2010.	Березень 2025 н.р.
Рекомендація 3 Розглянути можливість впровадження дуальної форми освіти на даній ОПП.	Довгостроковий	Розглянути можливість впровадження дуальної форми освіти на даній ОПП.	Серпнень 2026 н.р.
Рекомендація 4 Розмістити інформацію щодо ВК в ОПП у зручній для стейкхолдерів формі з чітким зазначенням компонент, доступних для вибору (посилання до ВК, таблиці тощо).	Довгостроковий	Доопрацювати інформаційну структуру веб-сайту	Березень 2026 н.р.

Рекомендація 5 Залучення студентів до обговорення та оновлення ОПП.	Довгостроковий	Залучення студентів до обговорення та оновлення ОПП	На початку 2025-2026 н.р.

Директор навчально-наукового інституту
комп'ютерних наук та інформаційних технологій_____Михайло ГОДЛЕВСЬКИЙ

Гарант освітньої програми _____Ольга КОРОЛЬ