ПРОЄКТ
Розглянуто на засіданні кафедри 16.01.2026 Протокол № 9

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

ЗАТВЕРДЖУЮ
Ректор НТУ «ХПІ»

_____ Євген СОКОЛ

«___» _____ 2026 р.

ОСВІТНЬО-НАУКОВА 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 «___»_____ 2026 р.

Харків 2026 р.

ЛИСТ ПОГОДЖЕННЯ

освітньо-наукової 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 ОНП із спеціальності
«Кібербезпека та захист інформації»
Гарант ОНП

_____Станіслав МІЛЕВСЬКИЙ

Протокол №___
«____» _____2026 р.

РЕКОМЕНДОВАНО
Методичною радою НТУ «ХПІ»
Заступник голови методичної ради

_____ Руслан МИГУЩЕНКО

Протокол №___
«____» _____2026 р.

ПОГОДЖЕНО
Завідувач кафедри
кібербезпека

_____ Сергій ЄВСЕЄВ

Протокол №___
«____» _____2026 р.

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

_____ Михайло ГОДЛЕВСЬКИЙ

«____»_____2026 р.

ПОГОДЖЕНО
здобувач вищої освіти
(член робочої групи ОНП)
№ групи КН-Н1125

_____ Максим РОГОЗІН

«____»_____2026 р.

ЗАТВЕРДЖЕНО ТА НАДАНО ЧИННОСТІ
Наказом ректора Національного технічного університету «Харківський політехнічний інститут» від «___» _____2026 року № _____.

РЕЦЕНЗЕНТИ:

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

1. Іван ОПІРСЬКИЙ, доктор технічних наук, професор, завідувач кафедри захисту інформації Інституту комп'ютерних технологій, автоматики та метрології Національного університету «Львівська політехніка»
2. Владислав КОВТУН, кандидат технічних наук, доцент, директор ТОВ "Сайфер"
3. Сергій ГОЛОВАШИЧ, кандидат технічних наук, доцент директор ТОВ "Мікрокрипт Текнолоджіс"
4. Олена ВОЛОЩУК, кандидат технічних наук, керівник освітніх програм ТОВ "Distributed Lab".
5. Ольга ШАПОВАЛ, виконавчий директор Громадської спілки «Харківський кластер інформаційних технологій»

Рецензії

ПЕРЕДМОВА

Відповідає Стандарту вищої освіти другого (магістерського) рівня галузі знань «Інформаційні технології», спеціальністю F5 «Кібербезпека та захист інформації», який затверджено наказом Міністерства освіти і науки України від 18.03.2021 р. № 332.

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

Гарант освітньо-наукової програми
Станіслав МІЛЕВСЬКИЙ, доктор технічних наук, доцент, професор кафедри кібербезпеки.

Члени робочої групи ОНП :
1. Сергій ЄВСЕЄВ, доктор технічних наук, професор, завідувач кафедри кібербезпеки.
2. Сергій ПОГАСІЙ, доктор технічних наук, доцент, професор кафедри кібербезпеки.
3. Ольга КОРОЛЬ, кандидат технічних наук, доцент, доцент кафедри кібербезпеки.
4. Максим РОГОЗІН, студент групи КН-Н1125.

1. ПРОФІЛЬ ОСВІТНЬО-НАУКОВОЇ 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 (освітньої, професійної) мовою оригіналу	Ступінь вищої освіти – Магістр Галузь знань - F Інформаційні технології Спеціальність – F5 Кібербезпека та захист інформації Освітня кваліфікація – магістр з кібербезпеки та захисту інформації.
Професійна кваліфікація	Відсутня
Форма навчання	Інституційна (очна (денна)).
Офіційна назва освітньо-наукової програми	Кібербезпека
Назви спеціалізацій (предметних спеціальностей)	Відсутня
Тип диплому одиничний, спільний (подвійний) за наявності та обсяг освітньої програми	Диплом магістра, одиничний, 120 кредитів ЄКТС, термін навчання 1 рік 9 місяців
Наявність акредитації	Акредитація за даною ОНП не проводилась
Цикл/рівень	Другий (магістерський) рівень вищої освіти; НРК України – 7 рівень, EQF LLL – 7 рівень, FQ-EHEA– другий цикл.
Передумови	Наявність ступеня вищої освіти «бакалавр»
Мова викладання	Українська мова, Англійська мова
Термін дії освітньо-наукової програми	Відповідно до терміну дії сертифікату. Переглядається щорічно
Посилання на постійне розміщення опису освітньо-наукової програми	https://blogs.kpi.kharkov.ua/v2/quality/dokumenty/diyuchy-osvitni-programy/osvitnij-riven-magistr/
2 – Мета освітньо-наукової 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 соціокіберфізичних системах (об'єктах критичної інфраструктури).	
3 – Характеристика освітньо-наукової програми	

Предметна область (галузь знань, спеціальність, спеціалізація або предметна спеціальність (за наявності))	**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 освітньої програми	Освітньо-наукова. Підготовка фахівців у сфері кібербезпеки та захисту інформації.
Основний фокус освітньої програми та спеціалізації або предметна спеціальність (за наявності)	Поглиблене вивчення механізмів та методів кіберзахисту соціокіберфізичних систем (об'єктів критичної інфраструктури) з комплексуванням з методами штучного інтелекту в умовах постквантового періоду. Отримання сертифікатів курсів академії Cisco, сприяє підвищенню конкурентноспроможності на ринке праці, удосконаленню механізмів многоконтурних систем захисту соціокіберфізичних систем (об'єктів критичної інфраструктури). Ключові слова: кібербезпека, цифрова криміналістика, етичний хакінг.
Особливості програми	Особливостями програми є підготовка професіоналів, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки, формування у здобувачів навичок побудови многоконтурних систем захисту в соціокіберфізичних систем (об'єктах критичної інфраструктури) для забезпечення безпеки контуру бізнес-процесів в умовах постквантового періоду (появи повномасштабного квантового комп'ютеру). 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 академічні права випускників	
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.
Академічні права випускників	Здобувачі освіти, які пройшли підготовку за даною навчальною програмою та отримали диплом магістра, мають право на здобуття освіти на третьому (освітньо-науковому) рівні вищої освіти у ЗВО України та за кордоном в галузі знань “Інформаційні технології” або суміжних. 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 науковими та технічними 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 (визначені стандартом вищої освіти спеціальності)	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).
Спеціальні (фахові) компетентності (визначені стандартом вищої освіти спеціальності)	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. КФ11. Здатність здійснювати наукові та/або прикладні дослідження у галузі інформаційної безпеки та/або кібербезпеки із застосуванням сучасних експериментальних і теоретичних методів моделювання процесів, формувати науково-технічну звітність.
7 – Результати навчання	
Результати навчання за спеціальністю (визначені стандартом вищої освіти спеціальності)	РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі. РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-

	математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення. РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення. РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки. РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури. РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому. РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до

	персоналу, партнерів та інших осіб. РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень. РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання. РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки. РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності. РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик. РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки. РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки. РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації. РН24. Планувати та виконувати наукові та прикладні дослідження у сфері інформаційної безпеки та/або кібербезпеки із застосуванням сучасних технологій, експериментальних і теоретичних методів і моделей теорії прийняття рішень, системного аналізу, оптимізації процесів, математичної статистики. РН25. Оцінювати ефективність та практичну цінність результатів наукових і практичних досліджень та інновацій.
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, внесенимизгідно з Постановою КМ № 365 від 24.03.2021, додаток 15-16). Склад робочої групи освітньої програми, професорсько викладацький склад, що задіяний до викладання навчальних дисциплін за спеціальністю відповідають Ліцензійним умовам провадження освітньої діяльності на другому (магістерському) рівні вищої освіти. 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). Навчально-науково-виробнича база у вигляді: –навчальні корпуси, комп'ютерні класи, об'єднані локальною обчислювальною мережею з виходом до Інтернету, мультимедійне обладнання;–спеціалізоване програмне забезпечення, 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 КМ № 365 від 24.03.2021, додаток 18). Інформаційне та навчально-методичне забезпечення навчального процесу реалізується наявністю необхідної навчальної та методичної літератури: підручники, навчальні посібники, методичні рекомендації до практичних занять, самостійної роботи, силабуси освітніх компонентів (https://cybersecurity.khpi.edu.ua/sylabusy-onp-mahistry-obovyazkovi/). Інформаційні ресурси розміщені у фондах наукової бібліотеки НТУ "ХПІ", сайтах випускових кафедр.
9 – Академічна мобільність	
Національна кредитна	На основі двосторонніх договорів між Національним

мобільність	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. На основі двосторонніх договорів між Національним технічним університетом «Харківський політехнічний інститут» та вищими навчальними закладами зарубіжних країн-партнерів.
Навчання іноземних здобувачів освіти	Підготовка іноземних громадян здійснюється згідно з вимогами чинного законодавства за умови визнання попереднього освітнього рівня.

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

2.1 Перелік компонент освітньо-наукової програми

Код н/д	Компоненти освітньо-професійної програми	Кількість кредитів	Форма підсумкового контролю
1. Обов'язкові освітні компоненти			
1.1 Загальна підготовка			
ЗП 1	*Академічна англійська*	*3,0*	*Екзамен*
ЗП 2	*Інноваційне підприємництво та управління стартап-проєктами*	*3,0*	*Екзамен*
1.2. Спеціальна (фахова) підготовка			
СП1	*Мережева та хмарна безпека*	*5,0*	*Екзамен*
СП2	*GEOINT-безпека*	*4,0*	*Екзамен*
СП3	*Цифрова криміналістика*	*4,0*	*Залік*
СП4	*Безпека об'єктів крітичної інфраструктури*	*3,0*	*Екзамен*
СП5	*Безпека нейронних мереж*	*4,0*	*Залік*
СП6	*Математичні моделі управління IT-проєктами в галузі захисту інформації*	*4,0*	*Залік*
1.3. Наукова підготовка			
НП1	*Основи наукових досліджень*	*5,0*	*Екзамен*
НП2	*Філософські проблеми сучасного наукового пізнання*	*4,0*	*Екзамен*
НП3	*Сучасні проблеми постквантової криптографії*	*4,0*	*Залік*
НП4	*Безпека на основі штучного інтелекту*	*5,0*	*Залік*
НП5	*Авторське право у цифровому суспільстві*	*4,0*	*Залік*
НП6	*Безпека систем штучного інтелекту*	*4,0*	*Залік*
НП7	*Захист розподілених сервісів і операційних платформ*	*4,0*	*Залік*
2. Практична підготовка			
ПП 1	*Науково-дослідницька практика*	*19,0*	*Залік*
3. Атестація			
А1	*Виконання кваліфікаційної роботи*	*7,0*	
А2	*Захист кваліфікаційної роботи*	*4,0*	
Загальний обсяг обов'язкових компонентів		***90***	
4. Вибіркові освітні компоненти			
4.1 Освітні компоненти вільного вибору професійної підготовки загальноінститутського каталогу			
ОКВП 1	*ОК ВВ ПП 1*	*4,0*	Залік

ОКВП 2	*ОК ВВ ПП 2*	*4,0*	Залік
ОКВП 3	*ОК ВВ ПП 3*	*4,0*	Залік
4.2. Освітні компонети вільного вибору загальної підготовки			
ОКВЗ 1	*ОК ВВ 1*	*3,0*	*Залік*
ОКВЗ 2	*ОК ВВ 2*	*3,0*	*Залік*
4.3. Освітні компоненти вільного вибору науково-професійного спрямування (НПС)			
ОКВН 1	*ОК ВВ НПС 1*	*4,0*	*Залік*
ОКВН 2	*ОК ВВ НПС 2*	*4,0*	*Залік*
ОКВН 3	*ОК ВВ НПС 3*	*4,0*	*Залік*
Загальний обсяг вибіркових компонент:		***30***	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬО-НАУКОВОЇ ПРОГРАМИ:		***120***	

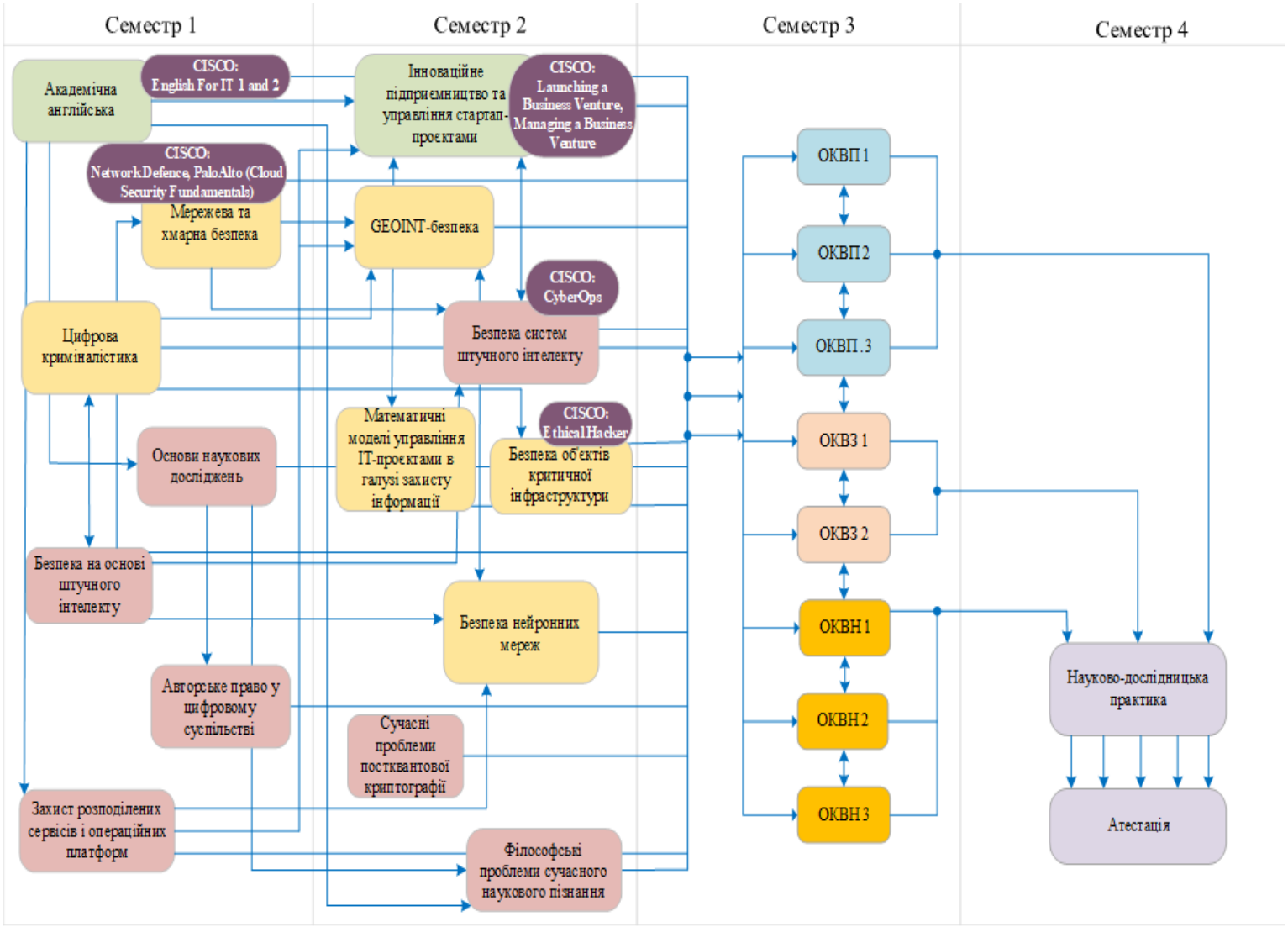
3. РОЗПОДІЛ ЗМІСТУ ОСВІТНЬО-НАУКОВОЇ ПРОГРАМИ ЗА ГРУПАМИ КОМПОНЕНТІВ ТА ЦИКЛАМИ ПІДГОТОВКИ

№п/п	Цикл підготовки	Обсяг навчального навантаження здобувача вищої освіти (кредитів ECTS / %)		
		Обов'язкові компоненти освітньо-наукової програми	Вибіркові компоненти освітньо- наукової програми	Всього за весь термін навчання
1	Загальна підготовка	6 / 5	-	**6 / 5**
2	Спеціальна (фахова) підготовка	24 / 20	-	**24 / 20**
3	Наукова підготовка	30 / 25	-	**30 / 25**
4	Практична підготовка	19/15,8	-	**19/15,8**
5	Компоненти вільного вибору	-	30 / 25	**30 / 25**
6	Атестація	11/9,2	-	**11/9,2**
Всього за весь термін навчання		**90 / 75**	**30 / 25**	**120 / 100**

4. 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.

6. СТРУКТУРНО-ЛОГІЧНА СХЕМА



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

Класифікація компетентностей (результатів навчання) за НРК	**Знання** **Зн1** Спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері професійної діяльності або галузі знань і є основою для оригінального мислення та проведення досліджень, критичне осмислення проблем у галузі та на межі галузей знань	**Уміння/Навички Ум1** Спеціалізовані уміння/навички розв'язання проблем, необхідні для проведення досліджень та/або провадження інноваційної діяльності з метою розвитку нових знань та процедур **Ум2** Здатність інтегрувати знання та розв'язувати складні задачі у широких або мультидисциплінарних контекстах **Ум3** Здатність розв'язувати проблеми у нових або незнайомих середовищах за наявності неповної або обмеженої інформації з урахуванням аспектів соціальної та етичної відповідальності	**Комунікація К1** Зрозуміле і недвозначне донесення власних знань, висновків та аргументації до фахівців і нефахівців, зокрема до осіб, які навчаються	**Відповідальність і автономія АВ1** Управління робочими або навчальними процесами, які є складними, непередбачуваними та потребують нових стратегічних підходів **АВ2** Відповідальність за внесок до професійних знань і практики та/або оцінювання результатів діяльності команд та колективів **АВ3** Здатність продовжувати навчання з високим ступенем автономії
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
ДОДАТКОВО ДЛЯ ОСВІТНЬО-НАУКОВИХ ПРОГРАМ*				
КФ11*	Зн1,	Ум1, Ум2, Ум3		АВ2, АВ3

ПРОЄКТ
Розглянуто на засіданні кафедри 16.01.2026 Протокол № 9

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	КФ 11*
РН 1	ЗП1 ЗП2 СП1 СП2 СП4 СП5 СП6 НП1 НП2 НП3 НП4 НП5 НП6 НП7 ПП1		СП3 СП5 СП6 НП1 НП2 НП3 НП5 НП7 ПП1			ЗП2 СП1 СП4 СП6 НП1 НП3 НП4 НП5 НП6 НП7 ПП1									
РН 2		СП5 НП1 НП2 НП3 НП5 НП7 ПП1	СП3 СП5 СП6 НП1 НП2 НП3 НП5 НП7 ПП1			ЗП2 СП1 СП4 СП6 НП1 НП3 НП4 НП5 НП6 НП7 ПП1	ЗП2 СП3 СП5 НП1 НП3 НП4 НП5 НП6 НП7 ПП1	ЗП2 СП1 СП2 СП3 СП4 СП5 СП6 НП1 НП3 НП4 НП6 НП7 ПП1							ЗП2 НП1 НП3 НП4 НП6 ПП1
РН 3	ЗП1					ЗП2										ЗП2

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	КФ 11*
	ЗП2 СП1 СП2 СП4 СП5 СП6 НП1 НП2 НП3 НП4 НП5 НП6 НП7 ПП1					СП1 СП4 СП6 НП1 НП3 НП4 НП5 НП6 НП7 ПП1										НП1 НП3 НП4 НП6 ПП1
РН 4	ЗП1 ЗП2 СП1 СП2 СП4 СП5 СП6 НП1 НП2 НП3 НП4 НП5 НП6 НП7 ПП1	СП5 НП1 НП2 НП3 НП5 НП7 ПП1	СП3 СП5 СП6 НП1 НП2 НП3 НП5 НП7 ПП1	ЗП2 СП2 СП5 СП6 НП1 НП2 НП3 НП5 НП6 НП7 ПП1		ЗП2 СП1 СП4 СП6 НП1 НП3 НП4 НП5 НП6 НП7 ПП1	ЗП2 СП3 СП5 НП1 НП3 НП4 НП5 НП6 НП7 ПП1									
РН 5			СП3 СП5 СП6		СП2 СП3 СП5		ЗП2 СП3 СП5									ЗП2 НП1 НП3

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	КФ 11*
			НП1 НП2 НП3 НП5 НП7 ПП1		НП1 НП2 НП3 НП5 НП7 ПП1		НП1 НП3 НП4 НП5 НП6 НП7 ПП1									НП4 НП6 ПП1
РН 6	ЗП1 ЗП2 СП1 СП2 СП4 СП5 СП6 НП1 НП2 НП3 НП4 НП5 НП6 НП7 ПП1			ЗП2 СП2 СП5 СП6 НП1 НП2 НП3 НП5 НП6 НП7 ПП1		ЗП2 СП1 СП4 СП6 НП1 НП3 НП4 НП5 НП6 НП7 ПП1		ЗП2 СП1 СП2 СП3 СП4 СП5 СП6 НП1 НП3 НП4 НП6 НП7 ПП1		ЗП2 СП1 СП2 СП3 СП4 СП5 НП1 НП4 НП5 НП6 НП7 ПП1	ЗП2 СП5 НП1 НП3 НП4 НП5 НП6 ПП1	ЗП2 СП1 СП2 СП3 СП4 НП1 НП3 НП4 НП6 НП7 ПП1		ЗП2 СП1 СП6 НП1 НП4 НП5 НП6 НП7 ПП1		
РН 7	ЗП1 ЗП2 СП1 СП2 СП4 СП5 СП6 НП1 НП2 НП3		СП3 СП5 СП6 НП1 НП2 НП3 НП5 НП7 ПП1				ЗП2 СП3 СП5 НП1 НП3 НП4 НП5 НП6 НП7 ПП1									

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	КФ 11*
	НП4 НП5 НП6 НП7 ПП1															
РН 8	ЗП1 ЗП2 СП1 СП2 СП4 СП5 СП6 НП1 НП2 НП3 НП4 НП5 НП6 НП7 ПП1	СП5 НП1 НП2 НП3 НП5 НП7 ПП1		ЗП2 СП2 СП5 СП6 НП1 НП2 НП3 НП5 НП6 НП7 ПП1	СП2 СП3 СП5 НП1 НП2 НП3 НП5 НП7 ПП1			ЗП2 СП1 СП2 СП3 СП4 СП5 СП6 НП1 НП3 НП4 НП6 НП7 ПП1						ЗП2 СП1 СП6 НП1 НП4 НП5 НП6 НП7 ПП1	НП1 НП4 НП5 ПП1	
РН 9	ЗП1 ЗП2 СП1 СП2 СП4 СП5 СП6 НП1 НП2 НП3 НП4 НП5	СП5 НП1 НП2 НП3 НП5 НП7 ПП1	СП3 СП5 СП6 НП1 НП2 НП3 НП5 НП7 ПП1	ЗП2 СП2 СП5 СП6 НП1 НП2 НП3 НП5 НП6 НП7 ПП1					ЗП2 СП1 СП3 СП4 СП5 СП6 НП1 НП3 НП4 НП5 НП6 НП7					ЗП2 СП1 СП6 НП1 НП4 НП5 НП6 НП7 ПП1	НП1 НП4 НП5 ПП1	

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	КФ 11*
	НП6 НП7 ПП1								ПП1							
РН 10	ЗП1 ЗП2 СП1 СП2 СП4 СП5 СП6 НП1 НП2 НП3 НП4 НП5 НП6 НП7 ПП1		СП3 СП5 СП6 НП1 НП2 НП3 НП5 НП7 ПП1	ЗП2 СП2 СП5 СП6 НП1 НП2 НП3 НП5 НП6 НП7 ПП1						ЗП2 СП1 СП2 СП3 СП4 СП5 НП1 НП4 НП5 НП6 НП7 ПП1				ЗП2 СП1 СП6 НП1 НП4 НП5 НП6 НП7 ПП1		
РН 11	ЗП1 ЗП2 СП1 СП2 СП4 СП5 СП6 НП1 НП2 НП3 НП4 НП5 НП6 НП7		СП3 СП5 СП6 НП1 НП2 НП3 НП5 НП7 ПП1	ЗП2 СП2 СП5 СП6 НП1 НП2 НП3 НП5 НП6 НП7 ПП1							ЗП2 СП5 НП1 НП3 НП4 НП5 НП6 ПП1				НП1 НП4 НП5 ПП1	

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	КФ 11*
	ППІ1															
РН 12	ЗП1 ЗП2 СП1 СП2 СП4 СП5 СП6 НП1 НП2 НП3 НП4 НП5 НП6 НП7 ППІ1		СП3 СП5 СП6 НП1 НП2 НП3 НП5 НП7 ППІ1	ЗП2 СП2 СП5 СП6 НП1 НП2 НП3 НП5 НП6 НП7 ППІ1					ЗП2 СП1 СП3 СП4 СП5 СП6 НП1 НП3 НП4 НП5 НП6 НП7 ППІ1			ЗП2 СП1 СП2 СП3 СП4 НП1 НП3 НП4 НП6 НП7 ППІ1			НП1 НП4 НП5 ППІ1	
РН 13	ЗП1 ЗП2 СП1 СП2 СП4 СП5 СП6 НП1 НП2 НП3 НП4 НП5 НП6 НП7 ППІ1		СП3 СП5 СП6 НП1 НП2 НП3 НП5 НП7 ППІ1	ЗП2 СП2 СП5 СП6 НП1 НП2 НП3 НП5 НП6 НП7 ППІ1									ЗП2 СП1 НП1 НП3 НП4 НП6 НП7 ППІ1		НП1 НП4 НП5 ППІ1	
РН 14	ЗП1		СП3	ЗП2					ЗП2					ЗП2	НП1	

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	КФ 11*
	ЗП2 СП1 СП2 СП4 СП5 СП6 НП1 НП2 НП3 НП4 НП5 НП6 НП7 ПП1		СП5 СП6 НП1 НП2 НП3 НП5 НП7 ПП1	СП2 СП5 СП6 НП1 НП2 НП3 НП5 НП6 НП7 ПП1					СП1 СП3 СП4 СП5 СП6 НП1 НП3 НП4 НП5 НП6 НП7 ПП1					СП1 СП6 НП1 НП4 НП5 НП6 НП7 ПП1	НП4 НП5 ПП1	
РН 15				ЗП2 СП2 СП5 СП6 НП1 НП2 НП3 НП5 НП6 НП7 ПП1	СП2 СП3 СП5 НП1 НП2 НП3 НП5 НП7 ПП1										НП1 НП4 НП5 ПП1	
РН 16	ЗП1 ЗП2 СП1 СП2 СП4 СП5 СП6	СП5 НП1 НП2 НП3 НП5 НП7 ПП1	СП3 СП5 СП6 НП1 НП2 НП3 НП5	ЗП2 СП2 СП5 СП6 НП1 НП2 НП3				ЗП2 СП1 СП2 СП3 СП4 СП5 СП6	ЗП2 СП1 СП3 СП4 СП5 СП6 НП1	ЗП2 СП1 СП2 СП3 СП4 СП5 НП1	ЗП2 СП5 НП1 НП3 НП4 НП5 НП6	ЗП2 СП1 СП2 СП3 СП4 НП1 НП3		ЗП2 СП1 СП6 НП1 НП4 НП5 НП6	НП1 НП4 НП5 ПП1	ЗП2 НП1 НП3 НП4 НП6 ПП1

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	КФ 11*
	НП1 НП2 НП3 НП4 НП5 НП6 НП7 ПП1		НП7 ПП1	НП5 НП6 НП7 ПП1				НП1 НП3 НП4 НП6 НП7 ПП1	НП3 НП4 НП5 НП6 НП7 ПП1	НП4 НП5 НП6 НП7 ПП1	ПП1	НП4 НП6 НП7 ПП1		НП7 ПП1		
РН 17								ЗП2 СП1 СП2 СП3 СП4 СП5 СП6 НП1 НП3 НП4 НП6 НП7 ПП1							НП1 НП4 НП5 ПП1	
РН 18	ЗП1 ЗП2 СП1 СП2 СП4 СП5 СП6 НП1 НП2 НП3 НП4			ЗП2 СП2 СП5 СП6 НП1 НП2 НП3 НП5 НП6 НП7 ПП1	СП2 СП3 СП5 НП1 НП2 НП3 НП5 НП7 ПП1										НП1 НП4 НП5 ПП1	

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	КФ 11*
	НП5 НП6 НП7 ПП1															
РН 19	ЗП1 ЗП2 СП1 СП2 СП4 СП5 СП6 НП1 НП2 НП3 НП4 НП5 НП6 НП7 ПП1			ЗП2 СП2 СП5 СП6 НП1 НП2 НП3 НП5 НП6 НП7 ПП1	СП2 СП3 СП5 НП1 НП2 НП3 НП5 НП7 ПП1	ЗП2 СП1 СП4 СП6 НП1 НП3 НП4 НП5 НП6 НП7 ПП1	ЗП2 СП3 СП5 НП1 НП3 НП4 НП5 НП6 НП7 ПП1	ЗП2 СП1 СП2 СП3 СП4 СП5 СП6 НП1 НП3 НП4 НП6 НП7 ПП1	ЗП2 СП1 СП3 СП4 СП5 СП6 НП1 НП3 НП4 НП5 НП6 НП7 ПП1		ЗП2 СП5 НП1 НП3 НП4 НП5 НП6 ПП1	ЗП2 СП1 СП2 СП3 СП4 НП1 НП3 НП4 НП6 НП7 ПП1	ЗП2 СП1 НП1 НП3 НП4 НП6 НП7 ПП1	ЗП2 СП1 СП6 НП1 НП4 НП5 НП6 НП7 ПП1		
РН 20	ЗП1 ЗП2 СП1 СП2 СП4 СП5 СП6 НП1 НП2 НП3 НП4 НП5 НП6	СП5 НП1 НП2 НП3 НП5 НП7 ПП1	СП3 СП5 СП6 НП1 НП2 НП3 НП5 НП7 ПП1	ЗП2 СП2 СП5 СП6 НП1 НП2 НП3 НП5 НП6 НП7 ПП1	СП2 СП3 СП5 НП1 НП2 НП3 НП5 НП7 ПП1	ЗП2 СП1 СП4 СП6 НП1 НП3 НП4 НП5 НП6 НП7 ПП1		ЗП2 СП1 СП2 СП3 СП4 СП5 СП6 НП1 НП3 НП4 НП6 НП7 ПП1								ЗП2 НП1 НП3 НП4 НП6 ПП1

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	КФ 11*
	НП7 ПП1															
РН 21	ЗП1 ЗП2 СП1 СП2 СП4 СП5 СП6 НП1 НП2 НП3 НП4 НП5 НП6 НП7 ПП1	СП5 НП1 НП2 НП3 НП5 НП7 ПП1	СП3 СП5 СП6 НП1 НП2 НП3 НП5 НП7 ПП1	ЗП2 СП2 СП5 СП6 НП1 НП2 НП3 НП5 НП6 НП7 ПП1		ЗП2 СП1 СП4 СП6 НП1 НП3 НП4 НП5 НП6 НП7 ПП1		ЗП2 СП1 СП2 СП3 СП4 СП5 СП6 НП1 НП3 НП4 НП6 НП7 ПП1		ЗП2 СП1 СП2 СП3 СП4 СП5 НП1 НП4 НП5 НП6 НП7 ПП1		ЗП2 СП1 СП2 СП3 СП4 НП1 НП3 НП4 НП6 НП7 ПП1	ЗП2 СП1 НП1 НП3 НП4 НП6 ПП1			ЗП2 НП1 НП3 НП4 НП6 ПП1
РН 22		СП5 НП1 НП2 НП3 НП5 НП7 ПП1	СП3 СП5 СП6 НП1 НП2 НП3 НП5 НП7 ПП1	ЗП2 СП2 СП5 СП6 НП1 НП2 НП3 НП5 НП6 НП7 ПП1		ЗП2 СП1 СП4 СП6 НП1 НП3 НП4 НП5 НП6 НП7 ПП1		ЗП2 СП1 СП2 СП3 СП4 СП5 СП6 НП1 НП3 НП4 НП6 НП7 ПП1								ЗП2 НП1 НП3 НП4 НП6 ПП1
РН 23	ЗП1 ЗП2		СП3 СП5	ЗП2 СП2		ЗП2 СП1	ЗП2 СП3	ЗП2 СП1			ЗП2 СП5	ЗП2 СП1	ЗП2 СП1	ЗП2 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	КФ 11*
	СП1 СП2 СП4 СП5 СП6 НП1 НП2 НП3 НП4 НП5 НП6 НП7 ПП1		СП6 НП1 НП2 НП3 НП5 НП7 ПП1	СП5 СП6 НП1 НП2 НП3 НП5 НП6 НП7 ПП1		СП4 СП6 НП1 НП3 НП4 НП5 НП6 НП7 ПП1	СП5 НП1 НП3 НП4 НП5 НП6 НП7 ПП1	СП2 СП3 СП4 СП5 СП6 НП1 НП3 НП4 НП6 НП7 ПП1			НП1 НП3 НП4 НП5 НП6 ПП1	СП2 СП3 СП4 НП1 НП3 НП4 НП6 НП7 ПП1	НП1 НП3 НП4 НП6 НП7 ПП1	СП6 НП1 НП4 НП5 НП6 НП7 ПП1		
Додатково для освітньо-наукових програм*																
РН 24		СП5 НП1 НП2 НП3 НП5 НП7 ПП1	СП3 СП5 СП6 НП1 НП2 НП3 НП5 НП7 ПП1	ЗП2 СП2 СП5 СП6 НП1 НП2 НП3 НП5 НП7 ПП1	СП2 СП3 СП5 НП1 НП2 НП3 НП5 НП7 ПП1			ЗП2 СП1 СП2 СП3 СП4 СП5 СП6 НП1 НП3 НП4 НП6 НП7 ПП1							НП1 НП4 НП5 ПП1	ЗП2 НП1 НП3 НП4 НП6 ПП1
РН 25	ЗП1 ЗП2 СП1 СП2 СП4	СП5 НП1 НП2 НП3 НП5	СП3 СП5 СП6 НП1 НП2	ЗП2 СП2 СП5 СП6 НП1				ЗП2 СП1 СП2 СП3 СП4								ЗП2 НП1 НП3 НП4 НП6

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	КФ 11*
	СП5 СП6 НП1 НП2 НП3 НП4 НП5 НП6 НП7 ПП1	НП7 ПП1	НП3 НП5 НП7 ПП1	НП2 НП3 НП5 НП6 НП7 ПП1				СП5 СП6 НП1 НП3 НП4 НП6 НП7 ПП1								ПП1

8. РЕЗУЛЬТАТИ ОБГОВОРЕННЯ ОСВІТНЬОЇ ПРОГРАМИ

Стейкхолдери (вказати ПІБ та посаду, місце роботи)	Рекомендація	Враховано / частково враховано / не враховано	Примітка
Гарант ОНП, д.т.н., проф. Мілевський С.В. завідувач кафедри, д.т.н., професор Євсеєв С.П. Члени робочої групи ОНП	Зміна шифру спеціальності та галузі знань (згідно з постановою Кабінету Міністрів України від 30 серпня 2024 р. No 1021).	Враховано.	Зміни внесено.
Гарант ОНП, д.т.н., проф. Мілевський С.В. завідувач кафедри, д.т.н., професор Євсеєв С.П. Члени робочої групи ОНП	З метою приведення у відповідність до сучасної термінології та стандартів вищої освіти оновити назви окремих дисциплін освітньої програми.	Враховано.	У межах періодичного перегляду освітньої програми з урахуванням рекомендацій стейкхолдерів, сучасних тенденцій розвитку галузі та актуалізації термінології було оновлено назви окремих навчальних дисциплін. Зміни мають редакційний характер і не впливають на зміст дисциплін, результати навчання, обсяг кредитів ЄКТС та структуру освітньої програми.
Волощук О. Б., к. т. н., керівник освітніх програм ТОВ “Distributed Lab”	Позитивний відгук. Без зауважень.	-	-

Опірський І. Р., доктор технічних наук, професор, завідувач кафедри захисту інформації Інституту комп'ютерних технологій, автоматики та метрології Національного університету «Львівська політехніка»	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.	-	-

Завідувач кафедри кібербезпека _____ Сергій ЄВСЕЄВ

Гарант освітньої програми _____ Станіслав МІЛЕВСЬКИЙ

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			
Рекомендація 2			
Рекомендація 3			

Акредитація планується на 2026 навчальний рік.

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

Гарант освітньої програми _____Станіслав МІЛЕВСЬКИЙ