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
«УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ»

першого (бакалаврського) рівня вищої освіти

за спеціальністю **К4 – Управління інформаційною безпекою**

галузі знань **К – Безпека та оборона**

кваліфікація **бакалавр з управління інформаційною безпекою**

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 Управління інформаційною безпекою

Рівень вищої освіти	Перший (бакалаврський)
Галузь знань	К – Безпека та оборона
Спеціальність	К4 «Управління інформаційною безпекою»
Кваліфікація	Бакалавр з управління інформаційною безпекою

СХВАЛЕНО
Робочою групою ОПП зі спеціальності
“Управління інформаційною безпекою”
Гарант ОПП

_____ Роман КОРОЛЬОВ

«____»_____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
Студент (член робочої групи ОПП)
№ групи КН-1423

_____ Артур КОНЮШЕНКО

«____»_____2025 р.

РЕЦЕНЗЕНТИ:

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

1. МАШТАЛІР Вадим Віталійович, доктор історичних наук, професор, заслужений винахідник України, начальник інституту інформаційно-комунікаційних технологій та кібероборони.
2. ПУНДА Юрій Васильович, доктор військових наук, старший науковий співробітник, начальник навчально-наукового центру підготовки офіцерів багатонаціональних штабів.
3. ШЕСТАКОВ Валерій Іванович, доктор технічних наук, доцент, лауреат Державної премії України в галузі науки і техніки, заступник директора (з навчальної та наукової роботи) Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій Національної академії Служби безпеки України.
4. ГОЛОВАШИЧ Сергій Олександрович, кандидат технічних наук, доцент директор ТОВ “Мікрокрипт Текнолоджіс”.

Рецензії

ПЕРЕДМОВА

Відповідає галузі знань Безпека та оборона, спеціальності Управління інформаційною безпекою відповідно до національної рамки кваліфікації.

Розроблено робочою групою освітньо-професійної програми “Управління інформаційною безпекою”
Навчально-наукового інституту комп’ютерних наук та інформаційних технолгій
Національного технічного університету “Харківський політехнічний інститут” у складі:

Гарант освітньо-професійної програми

КОРОЛЬОВ Роман Володимирович, кандидат технічних наук, доцент кафедри кібербезпеки.

Члени робочої групи ОПП:

1. ЄВСЕЄВ Сергій Петрович, доктор технічних наук, професор, завідувач кафедри кібербезпеки.
2. ТКАЧОВ Андрій Михайлович, кандидат технічних наук, старший науковий співробітник, доцент кафедри кібербезпеки.
3. КОНЮШЕНКО Артур Валерійович, студент групи КН-1423.

1. ПРОФІЛЬ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ ЗА СПЕЦІАЛЬНІСТЮ
К4 – УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

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	Бакалавр Освітня кваліфікація: бакалавр з управління інформаційною безпекою. Кваліфікація в дипломі: бакалавр з управління інформаційною безпекою
Офіційна назва освітньо-професійної програми	Управління інформаційною безпекою
Тип диплому та обсяг освітньо-професійної програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання 3 роки 10 місяців
Наявність акредитації	Освітня програма ліцензована (на підставі наказу МОН України від 07.06.2024 № 394-л)
Цикл/рівень	Перший (бакалаврський) рівень вищої освіти, НРК – 6 рівень, EQF– 6 рівень, QF-EHEA – перший цикл.
Передумови	Для здобуття освітнього ступеня «бакалавр» можуть вступати особи, які здобули повну загальну середню освіту або освітній ступінь «молодший бакалавр», фаховий «молодший бакалавр», ОКР «молодший спеціаліст».
Мова викладання	Українська, англійська
Термін дії освітньо-професійної програми	Оновлюється щорічно
Посилання на постійне розміщення опису освітньо-професійної програми	https://blogs.kpi.kharkov.ua/v2/quality/dokumenty/diyuchy-osvitni-programy/osvitnij-riven-bakalavr/
2 – Мета освітньої програми	
Надати освіту в сфері управління інформаційною безпекою для вирішення питань забезпечення виконання вимог міжнародних регуляторів та нормативних законодавчів актів країни щодо формування та використання системи управління інформаційною безпекою об'єктів критичної інфраструктури, широким доступом до працевлаштування (державні службовці органів державної влади та органів місцевого самоврядування, до сфери професійних обов'язків яких належить вирішення питань забезпечення безпеки життєдіяльності людини (індивіду), суспільства та держави, працівники недержавних та міжнародних організацій, науковоосвітніх установ, діяльність яких пов'язана із забезпеченням інформаційної	

безпеки) та створити передумови для подальшого вивчення державноуправлінських аспектів забезпечення безпеки на другому (магістерському) рівні вищої освіти.	
3 – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність)	Галузь знань: К “Безпека та оборона” Спеціальність: К4 “Управління інформаційною безпекою” **Об’єкт вивчення:** – об’єкти систем управління інформаційною безпекою інформатизації, включаючи об’єкти критичної інфраструктури, кіберфізичні, соціокіберфізичні, інформаційні, інформаційно-аналітичні, інформаційно-комунікаційні системи; – технології забезпечення інформаційної безпеки; – процеси управління інформаційною та/або кібербезпекою об’єктів, що підлягають захисту. **Цілі навчання:** підготовка фахівців здатних використовувати і впроваджувати технології управління інформаційною безпекою. Теоретичний зміст предметної області: Знання: – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення системи управління інформаційною безпекою; – принципів супроводу систем та комплексів інформаційної безпеки; – теорії, моделей та принципів управління доступом до інформаційних ресурсів; – теорії систем управління інформаційною безпекою; – методів та засобів виявлення, управління та ідентифікації ризиків; – методів та засобів оцінювання та забезпечення необхідного рівня інформаційної безпеки; – методів та засобів технічного та криптографічного захисту інформації; – сучасних інформаційно-комунікаційних технологій; – сучасного програмно-апаратного забезпечення **Методи, методики та технології:** Методи, методики, інформаційно-комунікаційні технології та інші технології управління інформаційною безпекою. **Інструменти та обладнання:** системи розробки, забезпечення, моніторингу та контролю процесів управління інформаційною безпекою; – сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; – спеціалізований клас (кіберполігон).
Орієнтація освітньо-професійної програми	Професійна підготовка фахівців у сфері управління інформаційною безпекою

Основний фокус освітньо-професійної програми та спеціалізації	Спеціальна освіта у галузі воєнних наук, національної безпеки, безпеки державного кордону зі спеціальності К4 “Управління інформаційною безпекою ”. Спеціальна освіта за спеціальністю управління інформаційною безпекою, яка забезпечує підготовку професіонала, здатного розв’язувати задачі формування, використання, поліпшення системи управління інформаційною безпекою об’єктів критичної інфраструктури, кіберфізичних та соціокіберфізичних систем. Ключові слова: управління інформаційною безпекою, об’єкти критичної інфраструктури
Особливості програми	Особливістю програми спеціальності “Управління інформаційною безпекою” є проходження виробничої практики в органах державної влади, кіберполіції тривалістю 4 тижні.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Фахівці з управління інформаційною безпекою можуть працювати, згідно з чинною редакцією Національного класифікатора України: Класифікатор професій ДК 003:2010: 2139.2 Фахівець з криптографічного захисту інформації; 2139.2 Фахівець з питань безпеки (інформаційно-комунікаційні технології); 2139.2 Фахівець з підтримки інфраструктури кіберзахисту; 2139.2 Фахівець з реагування на інциденти кібербезпеки; 2139.2 Фахівець сфери захисту інформації; 2419.3 Радник (органи державної влади, місцевого самоврядування); 3411 Фахівець з фінансово-економічної безпеки; 3439 Фахівець з режиму секретності; 3439 Фахівець із організації захисту інформації з обмеженим доступом; 3439 Фахівець із організації інформаційної безпеки.
Подальше навчання	Особа, яка закінчила навчання за цією освітньопрофесійною програмою та здобула ступінь бакалавра може продовжити навчання на другому (магістерському) рівні вищої освіти (при проходжені відбору у національної академії СБУ), а також має можливість набуття додаткових кваліфікацій в системі післядипломної освіти та підвищення кваліфікації.
5 – Викладання та оцінювання	
Викладання та навчання	Студенто-центриське навчання, самонавчання, проблемно-орієнтоване навчання, навчання через практикуми, які відбуваються на базах практики. На другому і третьому курсі студенти пишуть та захищають курсові роботи, зорієнтовані на засвоєння ними теоретичних знань та вирішення управлінських спеціалізованих завдань у сфері національної безпеки. Під час останнього року навчання студенти пишуть

	кваліфікаційну (бакалаврську) роботу, яка також презентується та обговорюється за участю викладачів, одногрупників та рецензується зовнішнім рецензентом
Оцінювання	Письмові та усні іспити, диференційовані заліки, семінари, наукові звіти, есе, аналітичні записки, презентації самостійних досліджень, поточний контроль, контрольні роботи, курсові роботи, комплексний кваліфікаційний іспит, захист кваліфікаційної (бакалаврської) роботи за участі науковців з інших університетів. Оцінювання здійснюється за національною шкалою (“відмінно”, “добре”, “задовільно”, “незадовільно”), 100-бальною шкалою та шкалою ECTS (A, B, C, D, E, FX, F).
6 – Програмні компетентності	
Інтегральна компетентність	Здатність здійснювати управлінську та проектну діяльність у визначені напрямів забезпечення захисту на об’єктах критичної інфраструктури, визначення політики та стратегії захисту інформації з обмеженим доступом, що передбачає застосування теорій та наукових методів у галузі управління інформаціною безпекою
Загальні компетентності	КЗ–1. Здатність реалізувати свої права і обов’язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого (безпечного) розвитку, верховенства права, прав і свобод людини і громадянина в Україні. КЗ–2. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя. КЗ–3. Здатність до абстрактного мислення, аналізу та синтезу. КЗ–4. Здатність спілкуватися державною мовою як усно, так і письмово. КЗ–5. Здатність спілкуватися іноземною мовою. КЗ–6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. КЗ–7. Здатність використовувати інформаційні та комунікаційні технології та формувати систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо системи управління інформаційною безпекою. КЗ-8. Здатність до соціальної взаємодії, співробітництва, розв’язання конфліктів у сфері професійної діяльності, лідерства і командної роботи.
Спеціальні (фахові, предметні)	ФК–1. Здатність використовувати безпекові режими під час виконання службових обов’язків. ФК-2. Здатність аналізувати та визначати політику та стратегії

компетентності	забезпечення захисту інформації. ФК-3. Проектувати системи управління та захисту інформації на підприємстві установі, організації. ФК-4. Здатність прогнозувати реалізації управлінських рішень щодо захисту інформації. ФК-5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою. ФК-6. Здатність використовувати іноземну мову для отримання додаткових знань і умінь з питань управління інформаційною безпекою, взаємодіяти з іноземними партнерами. ФК-7. Здатність організовувати та проводити аналіз оточення організації установ з метою виявлення та закриття можливих каналів витоку інформації. ФК-8. Здатність використовувати механізми забезпечення управління інформаційною безпекою у її визначальних сферах. ФК-9. Здатність організації реагування на загрози на об’єктах критичної інфраструктури, установах та підприємствах. ФК-10. Здатність забезпечувати неперервність бізнесу згідно з встановленою політикою інформаційної безпеки. ФК-11. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації.
7 – Програмні результати навчання	
Програмні результати навчання за спеціальністю	ПРН-1. Вміти реалізовувати свої права і обов’язки як члена суспільства, усвідомлювати цінності громадянського суспільства (вільного демократичного) та необхідність його сталого (безпечного) розвитку, верховенства права, прав і свобод людини і громадянина в Україні. ПРН-2. Вміти використовувати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя. ПРН-3. Вміти за допомогою абстрактного мислення, аналізу та синтезу оцінювати результати професійної діяльності та забезпечувати її якість, бути критичним і самокритичним, наполегливим щодо поставлених завдань і взятих зобов’язань. ПРН-4. Вільно спілкуватися державною мовою. ПРН-5. Вільно спілкуватися іноземною мовою у межах потреби своєї професійної діяльності. ПРН-6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки. ПРН-7. Вміти розробляти комплекс організаційних заходів

	щодо формування системи управління інформаційною безпекою. ПРН-8. Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційної безпеки. ПРН-9. Вміти використовувати безпекові режими під час виконання службових обов'язків. ПРН-10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки. ПРН-11. Вміти забезпечувати процеси захисту та функціонування системи управління інформаційною безпекою та захисту інформації на основі практик, навичок та знань, щодо інфраструктури кіберфізичних систем та інформаційних потоків. ПРН-12. Вміти використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів. ПРН-13. Вміти вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління інформаційної безпеки згідно встановленої політики безпеки в інформаційно-комунікаційних системах. ПРН-14. Вміти вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів та користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки. ПРН-15. Вміти визначати необхідні правові та організаційні заходи врегулювання конфліктів, пов'язаних із забезпеченням національної безпеки. ПРН-16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах. ПРН-17. Вміти розв'язувати задачі управління інфораційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою. ПРН-18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності. ПРН-19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-мунікаційних системах. ПРН-20. Вміти аналізувати та проводити оцінку ефективності та рівня захищеності інформаційних ресурсів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки. ПРН-21. Вміти застосовувати теорії та методи захисту для

	забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем. ПРН-22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп'ютерних інцидентів.
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). Склад робочої групи освітньої програми, професорсько викладацький склад, що задіяний до викладання навчальних дисциплін за спеціальністю відповідають Ліцензійним умовам провадження освітньої діяльності на першому (бакалаврському) рівні вищої освіти. До викладання залучаються викладачі-практики, фахівці та співробітники ІТ-компаній, а також фахівці Інституту СБУ, кіберполіції.
Матеріально-технічне забезпечення	Відповідає технологічним вимогам щодо матеріально-технічного 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 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; –бібліотека; гуртожитки; спортивні зали, майданчики; пункти харчування.
Інформаційне та навчально-методичне забезпечення	Інформаційне та навчально-методичне забезпечення освітньої програми відповідає постанові Кабінету МіністрівУкраїни від 30.12.2015 р. № 1187 «Про затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти» (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, робочі програми навчальних дисциплін. Інформаційні ресурси розміщені у фондах наукової бібліотеки НТУ "ХПІ", сайтах випускових кафедр.

	У навчальному процесі застосовується LMS (Learning Management System).
9 – Академічна мобільність	
Національна кредитна мобільність	На основі двосторонніх договорів про академічну мобільність з університетами України. Меморандуму про співпрацю щодо реалізації програм внутрішньої академічної мобільності здобувачів вищої освіти за освітньою програмою “Кібербезпека” спеціальності F5 “Кібербезпека та захист інформації” з національною академією СБУ.
Міжнародна кредитна мобільність	На основі двосторонніх договорів
Навчання іноземних здобувачів вищої 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 «УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ» ТА ЇХ ЛОГІЧНА ПОСЛІДОВНІСТЬ

2.1 Перелік компонент ОПП

Код н/д	Компоненти освітньо-професійної програми	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
1. Обов'язкові компоненти ОПП (здобувачі вищої освіти – громадяни Україні)			
1.1 Загальна підготовка (здобувачі вищої освіти – громадяни України)			
ЗП 1	*Історія та культура України*	*4*	*Екзамен*
ЗП 2	*Українська мова (професійного спрямування)*	*3*	*Залік*
ЗП 3	*Іноземна мова*	*16*	*Залік, Екзамен*
ЗП 4	*Вища математика*	*12*	*Залік, Екзамен*
ЗП 5	*Основи гуманітарно-філософських знань у професійній діяльності*	*4*	*Екзамен*
ЗП	*Фізичне виховання*	*8*	*Залік*
1.2 Спеціальна (фахова) підготовка			
СП 1	*Вступ до спеціальності. Ознайомча практика*	*3*	*Залік*
СП 2	*Основи програмування*	*4*	*Екзамен*
СП 3	*Інформаційна безпека держави*	*6*	*Екзамен*
СП 4	*Теорія інформації і кодування*	*3*	*Екзамен*
СП 5	*Фізичні основи технічних засобів розвідки*	*5*	*Екзамен*
СП 6	*Алгоритми та структури даних*	*5*	*Екзамен*
СП 7	*Правове регулювання кібербезпеки*	*4*	*Залік*
СП 8	*Менеджмент інформаційної безпеки*	*3*	*Екзамен*
СП 9	*Технології програмування*	*5*	*Екзамен*
СП 10	*Математичні основи криптології*	*4*	*Екзамен*
СП 11	*Основи соціальної інженерії*	*4*	*Залік*
СП 12	*Комп'ютерні мережі*	*5*	*Екзамен*
СП 13	*Інструментальні засоби програмування*	*6*	*Екзамен*
СП 14	*Основи криптографічного захисту*	*5*	*Залік*
СП 15	*Цифрова криміналістика*	*5*	*Залік*
СП 16	*Моделювання інформаційних систем*	*4*	*Залік*
СП 17	*Організація документообігу з обмеженим доступом*	*5*	*Залік*
СП 18	*Інтернетика. Теорія пошуку. Моделі та алгоритми*	*4*	*Екзамен*
СП 19	*Безпека в інформаційно-комунікаційних системах*	*4*	*Залік*
СП 20	*Розробка веб-додатків*	*6*	*Екзамен*
СП 21	*Веббезпека*	*5*	*Залік*
СП 22	*Блокчейн та смарт-технології в електронному документообігу*	*4*	*Екзамен*
СП 23	*Безпека інтернет-речей*	*4*	*Залік*
СП 24	*Антивірусний захист інформації*	*5*	*Залік*

1	2	3	4
СП 25	*Гібридні та інформаційні війни*	*4*	*Залік*
СП 26	*Інтернет-розвідка*	*4*	*Екзамен*
2. Практична підготовка			
ПП 1	*Виробнича практика*	*6*	*Залік*
ПП 2	*Переддипломна практика*	*6*	*Залік*
3. Атестація			
СП	*Атестація*	*3*	
Загальний обсяг обов'язкових компонент		*178*	
4. Вибіркові компоненти ОП (здобувачі вищої освіти – громадяни України)			
Профільований пакет дисциплін 01 "Штучний інтелект в системах захисту"			
ВП1.1	*Етичний хакінг*	*3*	*Екзамен*
ВП1.2	*Дата майнинг*	*3*	*Екзамен*
ВП1.3	*Математичні основи штучного інтелекту*	*3*	*Екзамен*
ВП1.4	*Python для штучного інтелекту та машинного навчання*	*4*	*Екзамен*
ВП1.5	*Генетичні алгоритми*	*3*	*Екзамен*
ВП1.6	*Python для інтернет-речей*	*3*	*Екзамен*
ВП1.7	*Системний інжинірінг*	*3*	*Екзамен*
Профільований пакет дисциплін 02 "Блокчейн-технологія та безпека банківських систем"			
ВП2.1	*Децентралізовані системи*	*3*	*Екзамен*
ВП2.2	*Ризик-менеджмент*	*3*	*Екзамен*
ВП2.3	*Blockchain: основи та приклади застосування*	*3*	*Екзамен*
ВП2.4	*Безпека банківських систем*	*4*	*Екзамен*
ВП2.5	*Захист об'єктів критичної інфраструктури*	*3*	*Екзамен*
ВП2.6	*Організація документообігу з обмеженим доступом*	*3*	*Екзамен*
ВП2.7	*Безпека в соціальних мережах*	*3*	*Екзамен*
Профільований пакет дисциплін 03 "Innovation Campus"			
ВП3.1	*Основи кібербезпеки*	*3*	*Екзамен*
ВП3.2	*Розробка корпоративних інформаційних систем (частина 1)*	*3*	*Екзамен*
ВП3.3	*Розробка корпоративних інформаційних систем (частина 2)*	*3*	*Екзамен*
ВП3.4	*Бази даних для корпоративних інформаційних систем*	*4*	*Екзамен*
ВП3.5	*Архітектура корпоративних інформаційних систем*	*3*	*Екзамен*
ВП3.6	*Безпека та аудит бездротових та рухомих мереж*	*3*	*Екзамен*
ВП3.7	*Захист об'єктів критичної інфраструктури*	*3*	*Екзамен*
Дисципліни вільного вибору студента профільної підготовки згідно переліку			
ОКВП1	*ОК ВВ ПП 1*	*4*	*Залік*
ОКВП2	*ОК ВВ ПП 2*	*4*	*Залік*
ОКВП3	*ОК ВВ ПП 3*	*4*	*Залік*

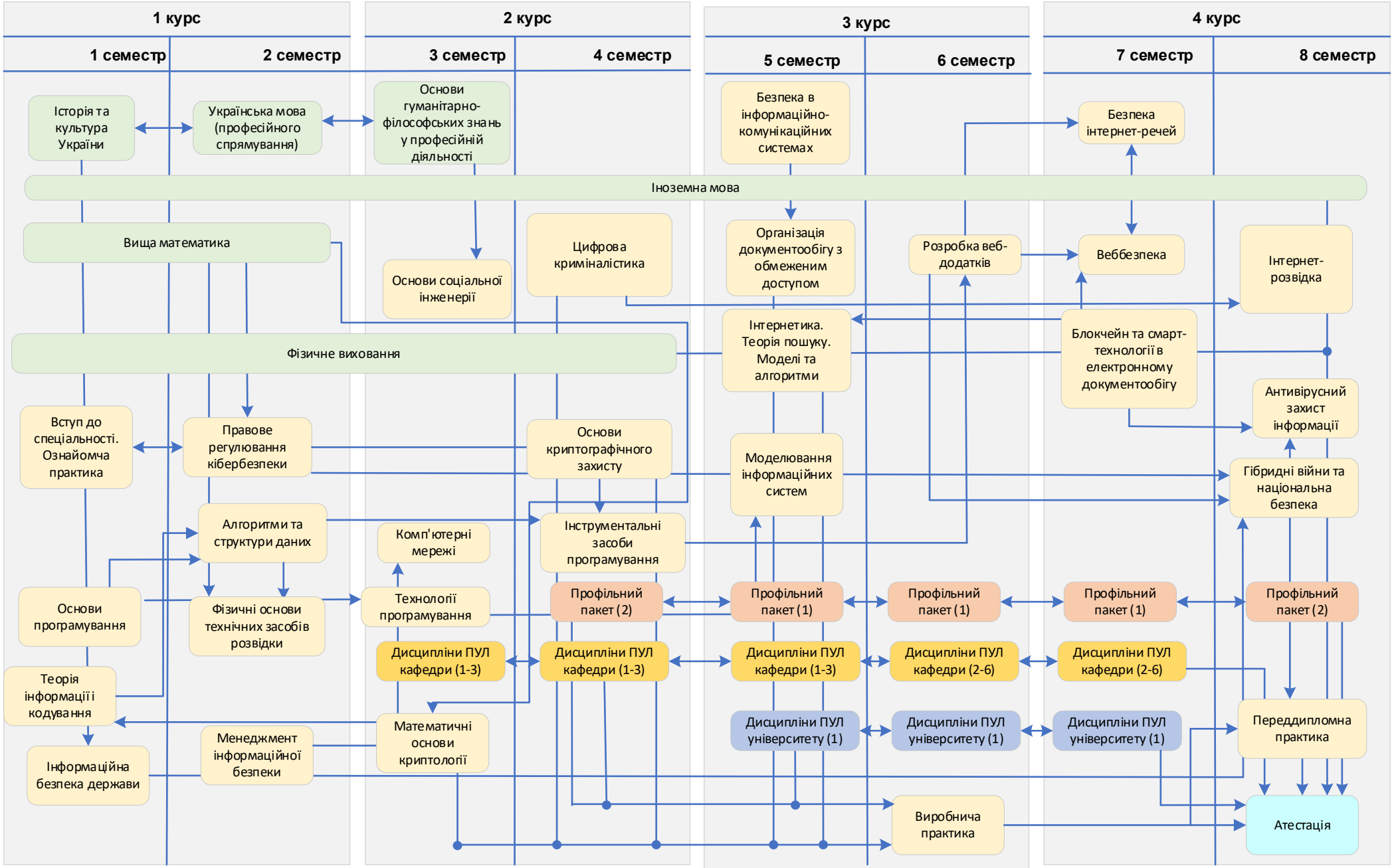
ОКВП4	*ОК ВВ ПП 4*	*4*	*Залік*
ОКВП5	*ОК ВВ ПП 5*	*4*	*Залік*
ОКВП6	*ОК ВВ ПП 6*	*4*	*Залік*
ОКВП7	*ОК ВВ ПП 7*	*4*	*Залік*
Дисципліни вільного вибору студента із загальноуніверситетського каталогу дисциплін			
ОКВ1	*ОК ВВ ЗП 1*	*4*	*Залік*
ОКВ2	*ОК ВВ ЗП 2*	*4*	*Залік*
ОКВ3	*ОК ВВ ЗП 3*	*4*	*Залік*
Загальний обсяг вибіркових компонент:		62	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ:		***240***	

2.2 Розподіл змісту освітньої 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	47 / 19,6	-	**47 / 19,6**
2	Спеціальна (фахова) підготовка	131/ 54,6	-	**131 / 54,6**
3	Дисципліни вільного вибору	-	62 / 25,8	**62 / 25,8**
Всього за весь термін навчання		**178 / 74,2**	**62 / 25,8**	**240 / 100**

ПРОЄКТ
Розглянуто на засіданні кафедри 17.01.2025 Протокол № 8

3. СТРУКТУРНО-ЛОГІЧНА СХЕМА



4. ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Форми атестації здобувачів вищої освіти	Атестація здійснюється у формі публічного захисту кваліфікаційного проекту/роботи. На атестацію допускаються студенти, які виконали всі вимоги програми підготовки
Вимоги до кваліфікаційного проекту/роботи	Кваліфікаційний проект/робота має передбачати розв'язання спеціалізованої задачі в сфері кіберзахисту галузі національної безпеки. Кваліфікаційний проект/робота має бути перевірений на плагіат.

5. ЗВЕДЕНА ТАБЛИЦЯ ФАХОВИХ КОМПЕТЕНТНОСТЕЙ ТА ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ

Фахові компетентності	Результати навчання
ФК–1. Здатність використовувати безпекові режими під час виконання службових обов'язків.	ПРН-6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки ПРН-7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою. ПРН-9. Вміти використовувати безпекові режими під час виконання службових обов'язків. ПРН-18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності. ПРН-19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-мунікаційних системах.
ФК-2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.	ПРН-6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки. ПРН-10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки. ПРН-19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-мунікаційних системах ПРН-21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем. ПРН-22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп'ютерних інцидентів.
ФК-3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.	ПРН-7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою.

	ПРН-8. Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційної безпеки. ПРН-10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки. ПРН-11. Вміти забезпечувати процеси захисту та функціонування системи управління інформаційною безпекою та захисту інформації на основі практик, навичок та знань, щодо інфраструктури кіберфізичних систем та інформаційних потоків. ПРН-12. Вміти використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів. ПРН-16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах. ПРН-17. Вміти розв'язувати задачі управління інфораційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою. ПРН-18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності. ПРН-21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем. ПРН-22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп'ютерних інцидентів.
ФК-4. Здатність прогнозувати реалізації управлінських рішень щодо захисту інформації.	ПРН-13. Вміти вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління інформаційної безпеки згідно встановленої політики безпеки в інформаційно-комунікаційних системах. ПРН-17. Вміти розв'язувати задачі управління інфораційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою. ПРН-18. Розуміти основні теоретичні поняття,

	застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності. ПРН-21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем. ПРН-22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп'ютерних інцидентів.
ФК-5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою.	ПРН-13. Вміти вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління інформаційної безпеки згідно встановленої політики безпеки в інформаційно-комунікаційних системах. ПРН-17. Вміти розв'язувати задачі управління інфораційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою. ПРН-18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності. ПРН-19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-мунікаційних системах.
ФК-6. Здатність використовувати іноземну мову для отримання додаткових знань і умінь з питань управління інформаційною безпекою, взаємодіяти з іноземними партнерами.	ПРН-5. Вільно спілкуватися іноземною мовою у межах потреби своєї професійної діяльності. ПРН-18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.
ФК-7. Здатність організовувати та проводити аналіз оточення організації установ з метою виявлення та закриття можливих каналів витоку інформації.	ПРН-13. Вміти вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління інформаційної безпеки згідно встановленої політики безпеки в інформаційно-комунікаційних системах. ПРН-19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-мунікаційних системах ПРН-21. Вміти застосовувати теорії та методи

	захисту для забезпечення безпеки елементів об’єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем. ПРН-22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп’ютерних інцидентів.
ФК-8. Здатність використовувати механізми забезпечення управління інформаційною безпекою у її визначальних сферах.	ПРН-16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах. ПРН-17. Вміти розв’язувати задачі управління інфораційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою. ПРН-19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-мунікаційних системах ПРН-21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об’єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем. ПРН-22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп’ютерних інцидентів.
ФК-9. Здатність організації реагування на загрози на об’єктах критичної інфраструктури, установах та підприємствах.	ПРН-13. Вміти вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління інформаційної безпеки згідно встановленої політики безпеки в інформаційно-комунікаційних системах. ПРН-14. Вміти вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів та користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки. ПРН-19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-мунікаційних системах ПРН-20. Вміти аналізувати та проводити оцінку ефективності та рівня захищеності інформаційних ресурсів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки. ПРН-21. Вміти застосовувати теорії та методи

	захисту для забезпечення безпеки елементів об’єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем. ПРН-22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп’ютерних інцидентів.
ФК-10. Здатність забезпечувати неперервність бізнесу згідно з встановленою політикою інформаційної безпеки.	ПРН-14. Вміти вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів та користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки. ПРН-17. Вміти розв’язувати задачі управління інфораційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою. ПРН-19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-мунікаційних системах ПРН-20. Вміти аналізувати та проводити оцінку ефективності та рівня захищеності інформаційних ресурсів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки. ПРН-21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об’єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем. ПРН-22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп’ютерних інцидентів.
ФК-11. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації.	ПРН-14. Вміти вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів та користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки. ПРН-17. Вміти розв’язувати задачі управління інфораційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою. ПРН-19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-мунікаційних системах ПРН-20. Вміти аналізувати та проводити оцінку ефективності та рівня захищеності

	інформаційних ресурсів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки. ПРН-21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об’єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем. ПРН-22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп’ютерних інцидентів.

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

Класифікація компетентностей за НРК	Знання	Уміння	Комунікація	Автономія та відповідальність
ЗАГАЛЬНІ КОМПЕТЕНТНОСТІ				
КЗ–1. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого (безпечного) розвитку, верховенства права, прав і свобод людини і громадянина в Україні.	+	+	+	+
КЗ–2. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.	+	+	+	+
КЗ–3. Здатність до абстрактного мислення, аналізу та синтезу.	+	+		+
КЗ–4. Здатність спілкуватися державною мовою як усно, так і письмово.	+	+	+	+
КЗ–5. Здатність спілкуватися іноземною мовою.	+	+	+	+
КЗ–6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.	+	+		+
КЗ–7. Здатність використовувати інформаційні та комунікаційні технології та формувати систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо системи управління інформаційною безпекою.	+	+		
КЗ-8. Здатність до соціальної взаємодії, співробітництва, розв'язання конфліктів у сфері професійної діяльності, лідерства і командної роботи.		+	+	
СПЕЦІАЛЬНІ (ФАХОВІ) КОМПЕТЕНТНОСТІ				
ФК–1. Здатність використовувати безпекові режими під час виконання службових обов'язків.	+	+		+
ФК-2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.	+	+		+
ФК-3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.	+	+		+
ФК-4. Здатність прогнозувати реалізації	+	+		

управлінських рішень щодо захисту інформації.				
ФК-5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою.	+	+	+	+
ФК-6. Здатність використовувати іноземну мову для отримання додаткових знань і умінь з питань управління інформаційною безпекою, взаємодіяти з іноземними партнерами.	+	+		+
ФК-7. Здатність організовувати та проводити аналіз оточення організації установ з метою виявлення та закриття можливих каналів витоку інформації.	+	+		+
ФК-8. Здатність використовувати механізми забезпечення управління інформаційною безпекою у її визначальних сферах.	+			
ФК-9. Здатність організації реагування на загрози на об’єктах критичної інфраструктури, установах та підприємствах.	+	+	+	+
ФК-10. Здатність забезпечувати неперервність бізнесу згідно з встановленою політикою інформаційної безпеки.	+	+		
ФК-11. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації	+	+		

ПРОЄКТ
Розглянуто на засіданні кафедри 17.01.2025 Протокол № 8

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

Результати навчання	**Компетентності**																		
	Загальні								**Спеціальні (фахові)**										
	КЗ1	КЗ2	КЗ3	КЗ4	КЗ5	КЗ6	КЗ7	КЗ8	ФК1	ФК2	ФК3	ФК4	ФК5	ФК6	ФК7	ФК8	ФК9	ФК10	ФК11
ПРН1	ЗП1 ЗП2 ЗП5 СП1 СП5 СП7 СП17 ПП1 ПП2 СП							ЗП2 ЗП3 ЗП5 ЗП СП1 СП5 СП7 СП17 ПП2 СП										
ПРН2		ЗП1 ЗП2 ЗП5 ЗП СП1 СП5 СП7 СП17 ПП1 ПП2 СП																	
ПРН3			ЗП4 ЗП5 ЗП СП2 СП3 СП4 СП5 СП6 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП15 СП16 СП18			ЗП4 ЗП5 ЗП СП1 СП2 СП3 СП4 СП5 СП6 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП15 СП16	СП1 СП2 СП3 СП5 СП6 СП8 СП9 СП10 СП12 СП13 СП14 СП16 СП18 СП19 СП20 СП21 СП22 СП23	ЗП2 ЗП3 ЗП5 ЗП СП1 СП5 СП7 СП17 ПП2 СП										

			СП19 СП21 СП22 СП23 СП24 СП25 СП26 ПП1 ПП2 СП			СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП26 ПП2 СП	СП24 СП25 ПП2 СП												
ПРН4				ЗП1 ЗП2 ЗП4 ЗП5 ЗП СП1 СП3 СП4 СП5 СП7 СП8 СП10 СП12 СП13 СП14 СП17 СП18 СП19 СП20 СП22 СП23 СП24 СП26 ПП1 ПП2 СП				ЗП2 ЗП3 ЗП5 ЗП СП1 СП5 СП7 СП17 ПП2 СП										
ПРН5					ЗП3 СП3 СП5 СП8 СП12 СП13 СП14 СП18 СП19 СП22			ЗП2 ЗП3 ЗП5 ЗП СП1 СП5 СП7 СП17 ПП2 СП						СП5 СП8 СП12 СП13 СП14 СП18 СП19 СП22 СП23 ПП2					

					СП23 ПП1 ПП2 СП									СП					
ПРН6							СП1 СП2 СП3 СП5 СП6 СП8 СП9 СП10 СП12 СП13 СП14 СП16 СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП25 ПП2 СП		СП2 СП4 СП5 СП6 СП9 СП18 СП21 СП23 СП24 СП25 ПП1 ПП2 СП	СП1 СП2 СП4 СП5 СП6 СП7 СП8 СП9 СП10 СП12 СП13 СП14 СП17 СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП26 ПП1 ПП2 СП									
ПРН7							СП1 СП2 СП3 СП5 СП6 СП8 СП9 СП10 СП12 СП13 СП14 СП16 СП18 СП19 СП20 СП21 СП22 СП23		СП2 СП4 СП5 СП6 СП9 СП18 СП21 СП23 СП24 СП25 ПП1 ПП2 СП		СП1 СП2 СП4 СП5 СП6 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП18 СП19 СП20 СП21 СП22 СП23								

							СП24 СП25 ПП2 СП				СП24 СП25 ПП1 ПП2 СП								
ПРН8											СП1 СП2 СП4 СП5 СП6 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП25 ПП1 ПП2 СП								
ПРН9									СП2 СП4 СП5 СП6 СП9 СП18 СП21 СП23 СП24 СП25 ПП1 ПП2 СП									
ПРН10										СП1 СП2 СП4 СП5 СП6 СП7	СП1 СП2 СП4 СП5 СП6 СП8								

										СП8 СП9 СП10 СП12 СП13 СП14 СП17 СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП26 ПП1 ПП2 СП	СП9 СП10 СП11 СП12 СП13 СП14 СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП25 ПП1 ПП2 СП								
ПРН11											СП1 СП2 СП4 СП5 СП6 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП25 ПП1 ПП2 СП								
ПРН12											СП1 СП2 СП4 СП5 СП6 СП8								

											СП9 СП10 СП11 СП12 СП13 СП14 СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП25 ПП1 ПП2 СП								
ПРН13												СП3 СП4 СП5 СП7 СП11 СП17 СП20 ПП1 ПП2 СП	СП3 СП4 СП5 СП7 СП8 СП9 СП11 СП12 СП13 СП14 СП15 СП18 СП19 СП21 СП22 СП23 СП24 ПП2 СП		СП1 СП4 СП5 СП8 СП12 СП13 СП14 СП18 СП19 СП20 СП22 СП23 СП24 СП25 ПП1 ПП2 СП		СП3 СП4 СП5 СП8 СП9 СП12 СП14 СП19 СП22 ПП2 СП		
ПРН14																		СП1 СП3 СП5 СП8 СП9 СП12 СП14 СП15 СП19 СП22 ПП2	СП4 СП5 СП8 СП12 СП13 СП14 СП18 СП19 СП21 СП22 СП23

																		СП	СП25 ПП1 ПП2 СП
ПРН15								ЗП2 ЗП3 ЗП5 ЗП СП1 СП5 СП7 СП17 ПП2 СП											
ПРН16											СП1 СП2 СП4 СП5 СП6 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП25 ПП1 ПП2 СП					СП3 СП4 СП5 СП8 СП10 СП11 СП12 СП14 СП16 СП19 СП20 СП21 СП22 ПП1 ПП2 СП			
ПРН17											СП1 СП2 СП4 СП5 СП6 СП8 СП9 СП10 СП11	СП3 СП4 СП5 СП7 СП11 СП17 СП20 ПП1 ПП2	СП3 СП4 СП5 СП7 СП8 СП10 СП11 СП12 СП13			СП3 СП4 СП5 СП8 СП10 СП11 СП12 СП14 СП16		СП1 СП3 СП5 СП8 СП9 СП12 СП14 СП15 СП19	СП4 СП5 СП8 СП12 СП13 СП14 СП18 СП19 СП21

											СП12 СП13 СП14 СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП25 ПП1 ПП2 СП	СП	СП14 СП15 СП18 СП19 СП21 СП22 СП23 СП24 ПП2 СП			СП19 СП20 СП21 СП22 ПП1 ПП2 СП		СП22 ПП2 СП	СП22 СП23 СП25 ПП1 ПП2 СП
ПРН18							СП1 СП2 СП3 СП5 СП6 СП8 СП9 СП10 СП12 СП13 СП14 СП16 СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП25 ПП2 СП		СП2 СП4 СП5 СП6 СП9 СП18 СП21 СП23 СП24 СП25 ПП1 ПП2 СП		СП1 СП2 СП4 СП5 СП6 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП25 ПП1 ПП2 СП	СП3 СП4 СП5 СП7 СП11 СП17 СП20 ПП1 ПП2 СП	СП3 СП4 СП5 СП7 СП8 СП10 СП11 СП12 СП13 СП14 СП15 СП18 СП19 СП21 СП22 СП23 СП24 ПП2 СП	СП5 СП8 СП12 СП13 СП14 СП18 СП19 СП22 СП23 ПП2 СП					
ПРН19							СП1 СП2 СП3 СП5 СП6 СП8 СП9 СП10 СП12 СП13		СП2 СП4 СП5 СП6 СП9 СП18 СП21 СП23 СП24 СП25	СП1 СП2 СП4 СП5 СП6 СП7 СП8 СП9 СП10 СП12			СП3 СП4 СП5 СП7 СП8 СП10 СП11 СП12 СП13 СП14		СП1 СП4 СП5 СП8 СП12 СП13 СП14 СП18 СП19 СП20	СП3 СП4 СП5 СП8 СП10 СП11 СП12 СП14 СП16 СП19	СП3 СП4 СП5 СП8 СП9 СП12 СП14 СП19 СП22 ПП2	СП1 СП3 СП8 СП9 СП12 СП14 СП15 СП19 СП22 ПП2	СП4 СП5 СП8 СП12 СП13 СП14 СП18 СП19 СП21 СП22

							СП14 СП16 СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП25 ПП2 СП		ПП1 ПП2 СП	СП13 СП14 СП17 СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП26 ПП1 ПП2 СП			СП15 СП18 СП19 СП21 СП22 СП23 СП24 ПП2 СП		СП22 СП23 СП24 СП25 ПП1 ПП2 СП	СП20 СП21 СП22 ПП1 ПП2 СП	СП	СП	СП23 СП25 ПП1 ПП2 СП
ПРН20																	СП3 СП4 СП5 СП8 СП9 СП12 СП14 СП19 СП22 ПП2 СП	СП1 СП3 СП5 СП8 СП9 СП12 СП14 СП15 СП19 СП22 ПП2 СП	СП4 СП5 СП8 СП12 СП13 СП14 СП18 СП19 СП21 СП22 СП23 СП25 ПП1 ПП2 СП
ПРН21										СП1 СП2 СП4 СП5 СП6 СП7 СП8 СП9 СП10 СП12 СП13 СП14 СП17 СП18 СП19 СП20 СП21 СП22	СП1 СП2 СП4 СП5 СП6 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП18 СП19 СП20 СП21 СП22 СП23	СП3 СП4 СП5 СП7 СП11 СП17 СП20 ПП1 ПП2 СП			СП1 СП4 СП5 СП8 СП12 СП13 СП14 СП18 СП19 СП20 СП22 СП23 СП24 СП25 ПП1 ПП2 СП	СП3 СП4 СП5 СП8 СП10 СП11 СП12 СП14 СП16 СП19 СП20 СП21 СП22 ПП1 ПП2 СП	СП3 СП4 СП5 СП8 СП9 СП12 СП14 СП19 СП22 ПП2 СП	СП1 СП3 СП5 СП8 СП9 СП12 СП14 СП15 СП19 СП22 ПП2 СП	СП4 СП5 СП8 СП12 СП13 СП14 СП18 СП19 СП21 СП22 СП23 СП25 ПП1 ПП2 СП

										СП23 СП24 СП26 ПП1 ПП2 СП	СП24 СП25 ПП1 ПП2 СП								
ПРН22										СП1 СП2 СП4 СП5 СП6 СП7 СП8 СП9 СП10 СП12 СП13 СП14 СП18 СП17 СП19 СП20 СП21 СП22 СП23 СП24 СП26 ПП1 ПП2 СП	СП1 СП2 СП4 СП5 СП6 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП25 ПП1 ПП2 СП	СП3 СП4 СП5 СП7 СП11 СП17 СП20 ПП1 ПП2 СП			СП1 СП4 СП5 СП8 СП12 СП13 СП14 СП18 СП19 СП20 СП22 СП23 СП24 СП25 ПП1 ПП2 СП	СП3 СП4 СП5 СП8 СП10 СП11 СП12 СП14 СП16 СП19 СП20 СП21 СП22 ПП1 ПП2 СП	СП3 СП4 СП5 СП8 СП9 СП12 СП14 СП19 СП22 ПП2 СП	СП1 СП3 СП5 СП8 СП9 СП12 СП14 СП15 СП19 СП22 ПП2 СП	СП4 СП5 СП8 СП12 СП13 СП14 СП18 СП19 СП21 СП22 СП23 СП25 ПП1 ПП2 СП

7. РЕЗУЛЬТАТИ ОБГОВОРЕННЯ ОСВІТНЬОЇ ПРОГРАМИ

Стейкхолдери (вказати ПІБ та посаду, місце роботи)	Рекомендація	враховано / частково враховано / не враховано	Примітка
Гарант ОПП, к.т.н., доц. Корольов Р. В., 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.	
Машталір В. В., д. і. н., професор, заслужений винахідник України, начальник інституту інформаційно-комунікаційних технологій та кібероборони	Позитивний відгук. Без зауважень.	-	
Пунда Ю. В., д. в. н., старший науковий співробітник, начальник навчально-наукового центру підготовки офіцерів багатонаціональних штабів	Позитивний відгук. Без зауважень.	-	
Шестаков В. І., д. т. н., доцент, лауреат Державної премії України в галузі науки і техніки, заступник директора (з навчальної та наукової роботи) Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій Національної академії Служби безпеки України	Позитивний відгук. Без зауважень.	-	
Головашич С. О., к. т. н., доцент директор ТОВ “Мікрокрипт Текнолоджіс”.	Позитивний відгук. Без зауважень.	-	

8. 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 2027 навчальний рік.

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

Гарант освітньої програми _____Роман КОРОЛЬОВ