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

ЗАТВЕРДЖУЮ
Вр.Ректор НТУ «ХПІ»
_____ Євген СОКОЛ
«30» березня 2026 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 № 4
від « 27 » березня 2026 р.

Харків 2026 р.

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

Протокол №_1_
«_16_» ___січня____2026 р.

РЕКОМЕНДОВАНО
Методичною радою НТУ «ХПІ»
Заступник голови методичної ради

_____ Руслан МИГУЩЕНКО

Протокол № 3
«_25_» _березня_2026 р.

ПОГОДЖЕНО
Завідувач кафедри кібербезпека

_____Сергій ЄВСЕЄВ

Протокол №_12_
«_23_»___березня___2026 р.

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

_____ Михайло ГОДЛЕВСЬКИЙ

«____»_____2026 р.

ПОГОДЖЕНО
Студент (член робочої групи ОПП)
№ групи КН-1423

_____ Артур КОНЮШЕНКО

«_23_»___березня___2026 р.

ЗАТВЕРДЖЕНО ТА НАДАНО ЧИННОСТІ
Наказом ректора Національного технічного університету «Харківський політехнічний інститут» від «_30_» березня 2026 року № 119 ОД.

РЕЦЕНЗЕНТИ:

Продуктивні зауваження та відгуки на проєкт освітньо-професійної 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. Олександр ВОЙТКО, кадидат військових наук, доцент, начальник інституту стратегічних комунікацій Національного університету оборони України
3. Євген МЕЛЕНТІ, кандидат технічних наук, доцент, Перший проректор Національної академії Служби безпеки України.
4. Владислав КОВТУН, кандидат технічних наук, доцент, директор ТОВ "Сайфер".

РЕЦЕНЗІЯ-ВІДГУК

НА ОСВІТНЬО-ПРОФЕСІЙНУ ПРОГРАМУ

“УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ”

першого (бакалаврського) рівня вищої освіти,

спеціальності К4 “Управління інформаційною безпекою”

кафедри кібербезпеки Національного технічного університету

“Харківський політехнічний інститут”

Стрімке зростання кількості та серйозності кіберінцидентів зумовлює необхідність посилення заходів безпеки, особливо вразливих секторів, таких як критична інфраструктура. Однією з ключових проблем її захисту є недостатня обізнаність про можливі наслідки кібератак. Ескалація загроз у цій сфері може бути пов’язана з тим, що більшість систем управління більше не використовують стандартні рішення, що підвищує їхню вразливість перед кіберзагрозами.

У сучасному світі фізичні ресурси мають свої цифрові двійники, інтегруючись із традиційними системами документообігу та управління бізнес-процесами. Така трансформація значно ускладнює завдання кіберзахисту та створює нові виклики. Як наслідок, в Україні зростає потреба у висококваліфікованих фахівцях з кібербезпеки, здатних ефективно захищати підприємства, протидіяти несанкціонованим втручанням та забезпечувати стійкість інформаційної інфраструктури.

Освітньо-професійна програма «Управління інформаційною безпекою» першого (бакалаврського) рівня вищої освіти, що запропанована кафедрою кібербезпеки Національного технічного університету "Харківський політехнічний інститут" має всі потрібні компоненти щодо забезпечення навчального процесу професійної підготовки фахівців, які у компаніях зможуть займати посади: менеджера систем з інформаційної безпеки, адміністратора мереж і систем, фахівця з питань безпеки (інформаційно-комунікаційні

технології), фахівця з підтримки інфраструктури кіберзахисту, фахівця з реагування на інциденти кібербезпеки тощо.

Слід визначити, що в умовах сучасних гібридних війн управління інформаційною безпекою - це не тільки значний тренд у розвитку великих компаній та підприємств, а також розвиток систем управління безпекою їх бізнес-процесів. Окремим питанням є формування можливості подальшого навчання щодо підготовки фахівців державних силових відомств. Це дозволяє формувати технічну складову майбутніх держслужбовців у галузі кібербезпеки та захисту інформації, а також окремо отримання поглиблених знань у сфері управління інформаційною безпекою. Тому, слід вважати дуже своєчасними завдання по формуванню професійних компетентностей, що розглядаються в освітньо-професійній програмі «Управління інформаційною безпекою». Під час навчання студенти отримують фахові компетентності, які дозволять у майбутньому подальше навчання за спеціальностями як у галузі інформаційних технологій, так і у галузі безпека і оборона.

Слід підвести, що освітньо-професійна програма «Управління інформаційною безпекою» першого (бакалаврського) рівня вищої освіти що запропонована кафедрою кібербезпеки Національного технічного університету "Харківський політехнічний інститут" є сучасною, ефективною та потрібною на ринку праці у нашої країни щодо підготовки фахівців з кібербезпеки та захисту інформації, з поглибленим вивченням питань, які пов'язані з управлінням інформаційною безпекою.

ВІДДІЛ КАДРІВ 02071010

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКР.
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
"ЛЬВІВСЬКА ПОЛІТЕХНІКА"
ПІДПИС ЗАСВІДЧУЮ
НАЧАЛЬНИК ВІДДІЛУ КАДРІВ
Шевцова М.С.
"__" _____ 20__ р.

Завідувач кафедри захисту інформації
Інституту комп'ютерних технологій,
автоматики та метрології Національного
університету «Львівська політехніка»,
д.т.н., професор _____ Іван ОПІРСЬКИЙ

РЕЦЕНЗІЯ-ВІДГУК
НА ОСВІТНЬО-ПРОФЕСІЙНУ ПРОГРАМУ
“УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ”
першого (бакалаврського) рівня вищої освіти
спеціальності К4 “Управління інформаційною безпекою”
кафедри кібербезпеки Національного технічного університету
“Харківський політехнічний інститут”

Актуальність розробки та впровадження освітньо-професійної програми (ОПП) “Управління інформаційною безпекою” зумовлена ескалацією кількості та зростанням складності кіберінцидентів на глобальному рівні. Дана тенденція актуалізує потребу в посиленні заходів безпеки, особливо у стратегічно важливих та вразливих секторах, зокрема в об'єктах критичної інфраструктури. Ключовим викликом у забезпеченні їхнього захисту залишається недостатній рівень усвідомлення потенційних деструктивних наслідків реалізації кібератак. Інтенсифікація загроз у цій сфері посилюється відходом багатьох систем управління від стандартизованих рішень, що об'єктивно підвищує їхню вразливість до сучасних кіберзагроз.

У контексті цифрової трансформації, де фізичні активи отримують цифрові аналоги (цифрові двійники), що інтегруються з корпоративними системами документообігу та управління бізнес-процесами, завдання забезпечення кіберстійкості суттєво ускладнюється. Це формує нові, нетривіальні виклики для систем кіберзахисту. Внаслідок зазначених факторів, в Україні спостерігається об’єктивне зростання попиту на висококваліфікованих фахівців у галузі кібербезпеки, здатних розробляти та імплементувати ефективні стратегії захисту підприємств, здійснювати проактивну протидію несанкціонованим втручанням та гарантувати стабільність функціонування інформаційної інфраструктури.

Представлена кафедрою кібербезпеки Національного технічного університету “Харківський політехнічний інститут” ОПП “Управління інформаційною безпекою” першого (бакалаврського) рівня вищої освіти розроблена з урахуванням сучасних вимог ринку праці та містить комплекс дисциплін, необхідних для формування професійних компетентностей

майбутніх фахівців. Програма орієнтована на підготовку спеціалістів, здатних обіймати посади менеджера з інформаційної безпеки, адміністратора мереж і систем, фахівця з безпеки інформаційно-комунікаційних технологій, спеціаліста з підтримки інфраструктури кіберзахисту, фахівця з реагування на інциденти кібербезпеки та інші.

Слід підкреслити, що в умовах сучасних гібридних загроз управління інформаційною безпекою набуває стратегічного значення не лише для великих комерційних структур, але й стає фундаментальним елементом розбудови систем управління безпекою їхніх біз
орієнтація програми на підготовку ка
сприяє формуванню необхідної тех
майбутніх державних службовців
інформаційної безпеки, зокрема погли
управління інформаційною безпекою

Таким чином, завдання формув
основними цілями ОПП "Управлі
високий ступінь актуальності. У
комплекс знань та навичок, що
професійного розвитку як у сфері ін
безпеки та оборони.

Висновок: Освітньо-професійн
безпекою" першого (бакалаврськог
Національним технічним університет
характеризується актуальністю змісту
практичною значущістю для забез
кібербезпеки та захисту інформаці
інформаційної безпеки. Програма від
підготовки фахівців у даній галузі.

Начальник
кандидат ві
07 квіт

Начальник інституту стратегічних комунікацій,
кандидат військових наук, доцент _____ Олександр ВОЙТКО
07 квітня 2025 рік

РЕЦЕНЗІЯ-ВІДГУК
НА ОСВІТНЬО-ПРОФЕСІЙНУ ПРОГРАМУ
«УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ»
першого (бакалаврського) рівня вищої освіти
спеціальності К4 «Управління інформаційною безпекою»
кафедри кібербезпеки Національного технічного університету
«Харківський політехнічний інститут»

Відповідно до положень Стратегії інформаційної безпеки, яку затверджено Указом Президента України від 28.12.2021 № 685/2021, забезпечення інформаційної безпеки України є однією з найважливіших функцій держави.

Протидія інформаційним впливам деструктивного характеру, насамперед держави-агресора, вимагає: створення системи раннього виявлення, прогнозування та запобігання інформаційним та гібридним загрозам. Кадрове забезпечення таких систем можливо здійснити фахівцям в галузі знань К Безпека та оборона за спеціальністю К4 Управління інформаційною безпекою.

Такі фахівці повинні бути компетентними в питаннях правового регулювання діяльності з управління інформаційною безпекою, застосуванні інформаційних технологій.

Освітньо-професійна програма «Управління інформаційною безпекою» пердбачає опанування професійними компетентностями з управління інформаційною безпекою. Особливістю освітньо-професійної програми є планомірне та поступове вивчення спеціальних навчальних дисциплін щодо: нормативно-правової бази України, вимог відповідних міжнародних стандартів; алгоритмізації, програмування;застосування сучасних інформаційно-комунікаційних технологій; методів технічного захисту інформації, оцінювання рівня захищенності інформації; побудови та моделювання інформаційних систем; організації та ведення електронного документообігу, а також документообігу з обмеженим доступом.

Освітньо-професійна програма «Управління інформаційною безпекою» дозволить здобувачам вищої освіти оволодіти практичними навиками роботи з програмними системами розробки, забезпечення, моніторингу та контролю процесів інформаційної та /або кібербез

Значну увагу в освітньо-професій навчанню, яке включає виконання лабо проходження виробничої практики в д дозволяє студентам не лише засвоїт реальний досвід роботи з сучасними за управління інформаційними ризиками. та співпраця з експертами галузі тако навичок та компетентностей.

Перспективи працевлаштування широкими: вони можуть працювати н безпеки, фахівців із захисту інформаційн та консультантів з управління ризиками під час навчання, дозволяють ви магістерському рівні або займатися н інформаційної безпеки та кіберзахисту.

Слід підкреслити, що освітньо-пр кафедрою кібербезпеки Національного політехнічний інститут», відповідає суч першого (бакалаврського) рівня вищої о інформаційною безпекою.

Перший проректор (з навчальної роботи) Національної академії СБ України, кандидат технічних наук, доцент Євген МЕЛЕНТІ

__ _____ 2025 року

Перший пр

Національн

кандидат т

CIPHER

ТОВ «САЙФЕР ІТ»
Адреса: 04107, Київ, вул. Нагірна, 25-27
Тел.: +38 044 484 46 12, 484 46 17
E-mail: info@cipher.com.ua

Системи захисту інформації
www.cipher.com.ua

ТОВ «САЙФЕР ІТ»
Адреса: 04107, Київ, вул. Нагірна, 25-27
Тел./Факс: (044) 484-46-17, 484-46-12, 483-03-22
E-mail: info@cipher.com.ua
https://cipher.com.ua

РЕЦЕНЗІЯ-ВІДГУК
НА ОСВІТНЬО-ПРОФЕСІЙНУ ПРОГРАМУ
"УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ"

першого (бакалаврського) рівня вищої освіти
спеціальності К4 "Управління інформаційною безпекою"
кафедри кібербезпеки Національного технічного університету
"Харківський політехнічний інститут"

Стрімке проникнення автоматизації та інформаційних систем у всі без винятку галузі діяльності та комунікації сучасного суспільства нашої держави та інших країн, також, неминуче тягне за собою і пов'язані ризики інформаційної безпеки. Тому безпечне застосування інформаційних систем в сучасних умовах неможливо без вирішення питань протидії кібернетичним загрозам, що існують на різних організаціях суспільства: починаючи від критичної інфраструктури держави, міністерств, відомств, органів державної влади та самоуправління на місцях, великихгалузеутворюючих підприємств та фінансових установ, і до підприємств малого і середнього бізнесу. Саме тому комплексне забезпечення інформаційної безпеки (ІБ) стала сьогодні невід'ємною функцією будь-якої сучасної інформаційної системи, а ефективність застосування засобів комплексної ІБ безпосередньо залежить від грамотного налагодження та повсякденного керування, оновлення та постійної адаптації засобів ІБ до нових загроз та методів вторгнення, що постійно еволюціонують. В зв'язку з цим, підготовка висококваліфікованих фахівців з управління інформаційною безпекою є необхідною передумовою безпечної експлуатації інформаційних систем будь-якого маштабу.

Фахівці з управління інформаційною безпекою повинні мати тверді знання сучасних принципів, методів та засобів як захисту інформації, так організації/виконання кібератак, яким вони мають протистояти в своїй роботі.

Також, при підготовці фахівців цього профілю, особливу увагу слід приділяти вивченню: міжнародних та галузевих стандартів у сфері захисту інформації, криптографічних алгоритмів та протоколів, технічних засобів захисту, питанням розподілу повноважень та керування доступом, забезпеченню високого рівня надійності і доступності інформаційних систем. Обов'язковою умовою підготовки фахівців цього напрямку є надання студентам обширної інформації про сучасні засоби ІБ, представлені на ринку та формування практичних навичок з оптимального вибору, конфігурування та застосування них для вирішення окремих задач кіберзахисту та побудови комплексної ІБ. Саме з метою досягнення перелічених цілей, кафедрою кібербезпеки Національного технічного університету «Харківський політехнічний інститут» розроблено освітньо-професійну програму «Управління інформаційною безпекою». Навчальні плани та підбор дисциплін спрямовані на підготовку фахівців-практиків з управління інформаційною безпекою і надання їм теоретичних знань та формування практичних навичок відповідно до національної рамки кваліфікацій.

Випускники освітньо-професійної програми «управління інформаційною безпекою» мають знання, необхідні для аналізу, проєктування, розгортання і супроводу ІТ-систем у корпоративному середовищі відповідно до вимог національних та міжнародних стандартів у сфері кібербезпеки. Програма формує висококваліфікованих спеціалістів, затребуваних на ринку праці, здатних ефективно впроваджувати сучасні технології захисту, зокрема інструменти на основі штучного інтелекту.

Директор ТОВ "Сайфер ІТ",
кандидат технічних наук
2026 рік

Товариство з обмеженою відповідальністю «САЙФЕР ІТ» №43305772 Україна, м. Київ

Владислав КОВТУН

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

Роман КОРОЛЬОВ, кандидат технічних наук, доцент кафедри кібербезпеки.

Члени робочої групи ОПП:

1. Сергій ЄВСЕЄВ, доктор технічних наук, професор, завідувач кафедри кібербезпеки.
2. Андрій ТКАЧОВ, кандидат технічних наук, старший науковий співробітник, доцент кафедри кібербезпеки.
3. Артур КОНЮШЕНКО, 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 (освітньої, професійної) мовою оригіналу	Ступінь вищої освіти – Бакалавр Галузь знань - К Безпека та оборона Спеціальність – К4 Управління інформаційною безпекою. Освітня кваліфікація – бакалавр з управління інформаційною безпекою.
Професійна кваліфікація	Відсутня
Форма навчання	Інституційна (очна (денна))
Офіційна назва освітньої програми	Управління інформаційною безпекою
Назва спеціалізації (предметних спеціальностей)	Відсутня
Тип диплому одиничний, спільний (подвійний) за наявності та обсяг освітньої 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 мова
Термін дії освітньо-професійної програми	Переглядається 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 освітньо-професійної 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 освітньо-професійної програми	
Предметна область (галузь знань, спеціальність, спеціалізація або предметна спеціальність (за наявності))	**Галузь знань:** К "Безпека та оборона" **Спеціальність:** К4 "Управління інформаційною безпекою" **Об'єкт вивчення:** інформаційна безпека, стратегії і політики, правове регулювання, міжнародні стандарти у сфері інформаційної безпеки, загрози і ризики щодо інформаційної безпеки, інформаційні заходи оборони держави та захисту національного інформаційного простору, режими інформації з обмеженим доступом, стратегічні комунікації та інформаційно-аналітичні процеси в системі забезпечення та управління інформаційною безпекою. **Цілі навчання:** підготовка фахівців здатних використовувати і впроваджувати технології управління інформаційною безпекою. **Теоретичний зміст предметної області:** теорії, поняття, принципи, концепції, категорії управління інформаційною безпекою. **Методи, методики та технології:** Методи, методики та технології управління інформаційною безпекою, оцінювання загроз і ризиків щодо інформаційної безпеки, оцінювання стійкості до інформаційних загроз, виявлення та ідентифікації негативних інформаційних впливів та протидії їм, моніторингу та прогнозування змін інформаційного простору, комунікативного супроводження, збору, інтерпретації та представлення інформації. **Інструменти та обладнання:** прилади та програмне забезпечення для моніторингу інформаційних ресурсів, аудиту мереж і систем; платформи для аналізу і візуалізації даних; інструменти OSINT; програмні та апаратні засоби проведення спеціальних інформаційних операцій, інформаційно-аналітичного забезпечення та ситуаційної обізнаності.
Орієнтація освітньої програми	Професійна підготовка фахівців у сфері управління інформаційною безпекою
Основний фокус освітньої програми та спеціалізації або	Спеціальна освіта у галузі воєнних наук, національної безпеки, безпеки державного кордону зі спеціальності К4 "Управління інформаційною безпекою ". Спеціальна освіта

предметна спеціальність (за наявності)	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 академічні права випускників	
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.
Академічні права випускників	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 бепекою
Загальні компетентності	ЗК1. 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. ЗК2. 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. ЗК3. Здатність до абстрактного мислення, аналізу та синтезу. ЗК4. Здатність спілкуватися державною мовою як усно, так і письмово. ЗК5. Здатність спілкуватися іноземною мовою. ЗК6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. ЗК7. Здатність використовувати інформаційні та комунікаційні технології та формувати систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо системи управління інформаційною безпекою. ЗК8. Здатність до соціальної взаємодії, співробітництва, розв’язання конфліктів у сфері професійної діяльності,

	лідерства і командної роботи.
Спеціальні (фахові) компетентності	СК1. Здатність використовувати безпекові режими під час виконання службових обов'язків. СК2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації. СК3. Проектувати системи управління та захисту інформації на підприємстві установі, організації. СК4. Здатність прогнозувати реалізації управлінських рішень щодо захисту інформації. СК5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою. СК6. Здатність використовувати іноземну мову для отримання додаткових знань і умінь з питань управління інформаційною безпекою, взаємодіяти з іноземними партнерами. СК7. Здатність організовувати та проводити аналіз оточення організації установ з метою виявлення та закриття можливих каналів витоку інформації. СК8. Здатність використовувати механізми забезпечення управління інформаційною безпекою у її визначальних сферах. СК9. Здатність організації реагування на загрози на об'єктах критичної інфраструктури, установах та підприємствах. СК10. Здатність забезпечувати неперервність бізнесу згідно з встановленою політикою інформаційної безпеки. СК11. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації.
7 – Результати навчання	
Результати навчання за спеціальністю	РН1. 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. РН2. 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. РН3. 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. РН4. Вільно спілкуватися державною мовою.

	РН5. Вільно спілкуватися іноземною мовою у межах потреби своєї професійної діяльності. РН6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки. РН7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою. РН8. Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційної безпеки. РН9. Вміти використовувати безпекові режими під час виконання службових обов'язків. РН10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки. РН11. 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. РН12. Вміти використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів. РН-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. РН14. Вміти вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів та користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки. РН15. Вміти визначати необхідні правові та організаційні заходи врегулювання конфліктів, пов'язаних із забезпеченням національної безпеки. РН16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах. РН17. Вміти розв'язувати задачі управління інфораційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою. РН18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності. РН19. Вміти впроваджувати заходи та забезпечувати

	реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-мунікаційних системах. РН20. Вміти аналізувати та проводити оцінку ефективності та рівня захищеності інформаційних ресурсів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки. РН21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем. РН22. 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, силабуси освітніх компонентів (https://cybersecurity.khpi.edu.ua/sylabusy-osvitnikh-komponentiv-k4-bakalavr/). 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 здійснюється згідно з вимогами чинного законодавства за умови визнання попереднього освітнього рівня.

2. ПЕРЕЛІК ОСВІТНІХ КОМПОНЕНТ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ «УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ» ТА ЇХ ЛОГІЧНА ПОСЛІДОВНІСТЬ

2.1 Перелік компонент освітньо-професійної програми

Код н/д	Компоненти освітньо-професійної програми	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
1. Обов'язкові освітні компоненти ОПП			
1.1 Загальна підготовка			
ЗП 1	*Основи національного спротиву*	*5,0*	*Залік*
ЗП 1	*Історія української державності*	*4,0*	*Екзамен*
ЗП 2	*Українська мова (професійного спрямування)*	*3,0*	*Залік*
ЗП 3	*Іноземна мова*	*16,0*	*Залік, Екзамен*
ЗП 4	*Основи гуманітарно-філософських знань у професійній діяльності*	*4,0*	*Екзамен*
ЗП 5	*Вища математика*	*6,0*	*Залік*
ЗП 6	*Основи вищої алгебри*	*5,0*	*Екзамен*
ЗП	*Фізичне виховання*	*8,0*	*Залік*
1.2 Спеціальна (фахова) підготовка			
СП 1	*Вступ до спеціальності. Ознайомча практика*	*3,0*	*Залік*
СП 2	*Основи програмування*	*4,0*	*Екзамен*
СП 3	*Інформаційна безпека держави*	*4,0*	*Екзамен*
СП 4	*Теорія інформації і кодування*	*5,0*	*Екзамен*
СП 5	*Фізичні основи технічних засобів розвідки*	*5,0*	*Екзамен*
СП 6	*Алгоритми та структури даних*	*5,0*	*Екзамен*
СП 7	*Правове регулювання захисту інформації*	*4,0*	*Залік*
СП 8	*Менеджмент інформаційної безпеки*	*4,0*	*Екзамен*
СП 9	*Технології програмування*	*4,0*	*Екзамен*
СП 10	*Математичні основи криптології*	*4,0*	*Екзамен*
СП 11	*Методи соціальної інженерії в кібербезпеці*	*3,0*	*Екзамен*
СП 12	*Комп'ютерні мережі*	*5,0*	*Екзамен*
СП 13	*Розробка програмного забезпечення систем кібербезпеки*	*5,0*	*Екзамен*
СП 14	*Основи криптографічного захисту*	*6,0*	*Залік*
СП 15	*Цифрова криміналістика*	*5,0*	*Екзамен*
СП 16	*Моделювання інформаційних систем*	*4,0*	*Екзамен*
СП 17	*Організація документообігу з обмеженим доступом*	*5,0*	*Екзамен*
СП 18	*Інтернетика. Теорія пошуку. Моделі та алгоритми*	*4,0*	*Екзамен*
СП 19	*Geosint-розвідка*	*4,0*	*Залік*
СП 20	*Розробка веб-додатків*	*4,0*	*Екзамен*
СП 21	*Веб-безпека*	*5,0*	*Екзамен*
СП 22	*Блокчейн та смарт-технології в електронному документообігу*	*4,0*	*Екзамен*

СП 23	*Безпека інтернет-речей*	*4,0*	*Екзамен*
СП 24	*Нейронні мережі*	*5,0*	*Залік*
СП 25	*Гібридні війни та національна безпека*	*4,0*	*Екзамен*
СП 26	*Інтернет-розвідка*	*4,0*	*Залік*
2. Практична підготовка			
ПП 1	*Виробнича практика*	*6,0*	*Залік*
ПП 2	*Переддипломна практика*	*6,0*	*Залік*
3. Атестація			
	Атестація	*3,0*	
Загальний обсяг обов'язкових компонент		***179***	
4. Вибіркові освітні компоненти ОПП			
4.1. Профільна підготовка			
4.1.1 Профільований пакет освітніх компонент 01 "Штучний інтелект в системах захисту"			
ВП1.1	*Етичний хакінг*	*3,0*	*Екзамен*
ВП1.2	*Дата майнинг*	*3,0*	*Екзамен*
ВП1.3	*Математичні основи штучного інтелекту*	*3,0*	*Екзамен*
ВП1.4	*Python для штучного інтелекту та машинного навчання*	*3,0*	*Екзамен*
ВП1.5	*Генетичні алгоритми*	*3,0*	*Екзамен*
ВП1.6	*Python для інтернет-речей*	*3,0*	*Екзамен*
ВП1.7	*Системний інжинірінг*	*3,0*	*Екзамен*
4.1.1 Профільований пакет освітніх компонент 02 "Блокчейн-технологія та безпека банківських систем"			
ВП2.1	*Децентралізовані системи*	*3,0*	*Екзамен*
ВП2.2	*Ризик-менеджмент*	*3,0*	*Екзамен*
ВП2.3	*Blockchain: основи та приклади застосування*	*3,0*	*Екзамен*
ВП2.4	*Безпека банківських систем*	*3,0*	*Екзамен*
ВП2.5	*Захист об'єктів критичної інфраструктури*	*3,0*	*Екзамен*
ВП2.6	*Організація документообігу з обмеженим доступом*	*3,0*	*Екзамен*
ВП2.7	*Безпека DevOps*	*3,0*	*Екзамен*
4.1.1 Профільований пакет освітніх компонент 03 "Innovation Campus"			
ВП3.1	*Основи кібербезпеки*	*3,0*	*Екзамен*
ВП3.2	*Розробка корпоративних інформаційних систем (частина 1)*	*3,0*	*Екзамен*
ВП3.3	*Розробка корпоративних інформаційних систем (частина 2)*	*3,0*	*Екзамен*
ВП3.4	*Бази даних для корпоративних інформаційних систем*	*3,0*	*Екзамен*
ВП3.5	*Архітектура корпоративних інформаційних систем*	*3,0*	*Екзамен*
ВП3.6	*Безпека та аудит бездротових та рухомих мереж*	*3,0*	*Екзамен*
ВП3.7	*Захист об'єктів критичної інфраструктури*	*3,0*	*Екзамен*

4.2 Освітні компоненти вільного вибору професійної підготовки загальноінститутського каталогу			
ОКВП 1	*ОК ВВ ПК 1*	*4,0*	*Залік*
ОКВП 2	*ОК ВВ ПК 2*	*4,0*	*Залік*
ОКВП 3	*ОК ВВ ПК 3*	*4,0*	*Залік*
ОКВП 4	*ОК ВВ ПК 4*	*4,0*	*Залік*
ОКВП 5	*ОК ВВ ПК 5*	*4,0*	*Залік*
ОКВП 6	*ОК ВВ ПК 6*	*4,0*	*Залік*
ОКВП 7	*ОК ВВ ПК 7*	*4,0*	*Залік*
4.3 Освітні компоненти вільного вибору загальноуніверситетського каталогу			
ОКВЗ 1	*ОК ВВ ЗК 1*	*4,0*	*Залік*
ОКВЗ 2	*ОК ВВ ЗК 2*	*4,0*	*Залік*
ОКВЗ 3	*ОК ВВ ЗК 3*	*4,0*	*Залік*
Загальний обсяг вибіркових компонент:		***61***	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ:		***240***	

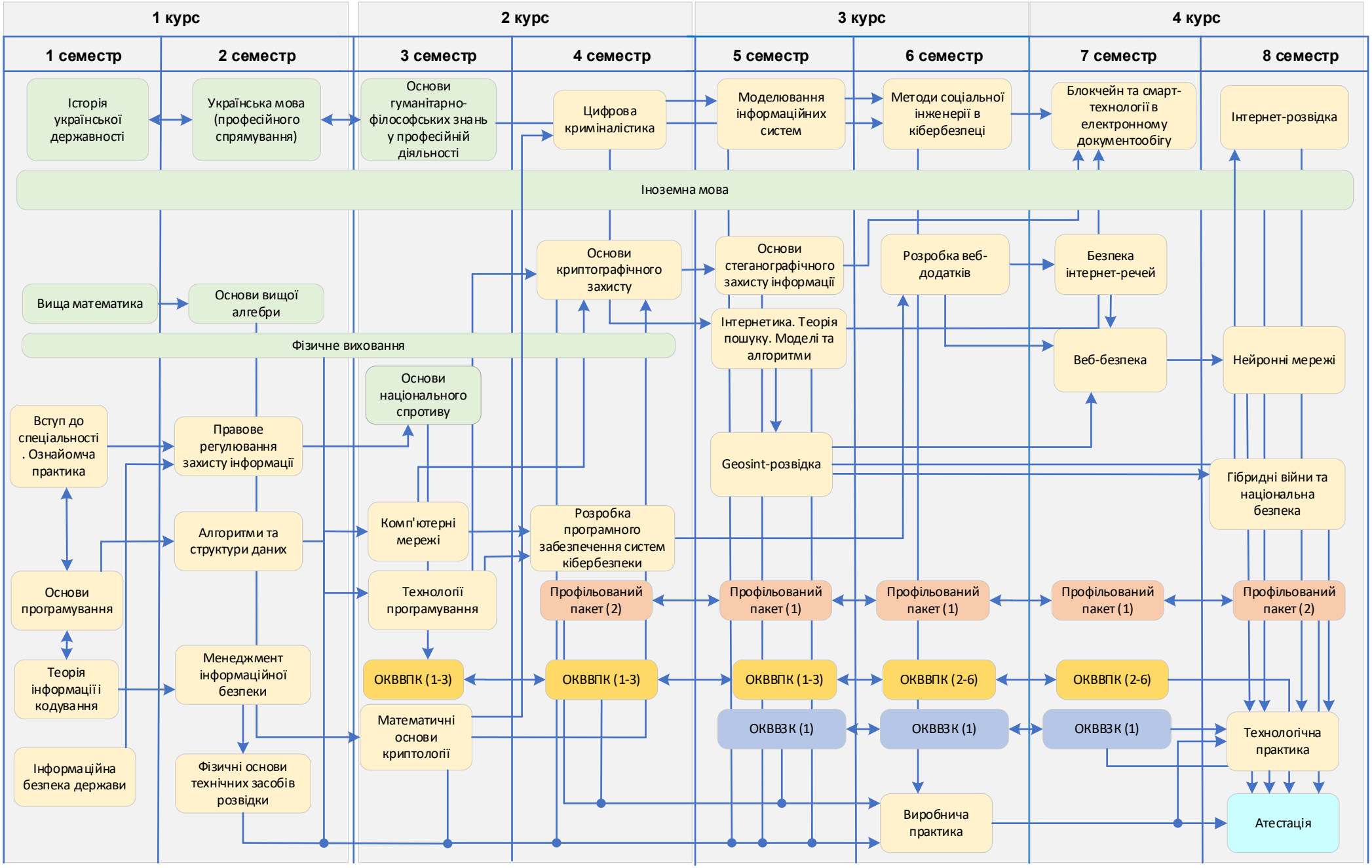
3. РОЗПОДІЛ ЗМІСТУ ОСВІТНЬОЇ ПРОГРАМИ ЗА ГРУПАМИ КОМПОНЕНТІВ ТА ЦИКЛАМИ ПІДГОТОВКИ

№ 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	51 / 21,3	–	**51 / 21,3**
2	Спеціальна (фахова) підготовка	113/ 47,1	–	**113/ 47,1**
3	Практична підготовка	12/5	-	**12/5**
4	Вибіркові освітні компоненти	-	61 / 25,4	**61 / 25,4**
5	Атестація	3/1,2	-	**3/1,2**
Всього за весь термін навчання		**179 / 74,6**	**61 / 25,4**	**240 / 100**

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 академічний плагіат та має бути оприлюднений (за виключенням робіт, що містять інформацію з обмеженим доступом) на офіційному сайті закладу вищої освіти або його структурного підрозділу, або у репозитарії закладу вищої освіти.

5. СТРУКТУРНО-ЛОГІЧНА СХЕМА



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

Класифікація компетентностей (результатів навчання) за НРК	**Знання** **Зн1.** Концептуальні наукові та практичні знання. **Зн2.** Критичне осмислення теорій, принципів, методів і понять у сфері професійної діяльності та/або навчання	**Уміння** **Ум1.** Поглиблені когнітивні та практичні уміння/навички, майстерність та інноваційність на рівні, необхідному для розв'язання складних спеціалізованих задач і практичних проблем у сфері професійної діяльності або навчання.	**Комунікація** **К1.** Донесення до фахівців і нефахівців інформації, ідей, проблем, рішень власного досвіду та аргументації. **К2.** Збір, інтерпретація та застосування даних. **К3.** Спілкування з професійних питань, у тому числі іноземною мовою	**Відповідальність і автономія** **АВ1.** Управління складною технічною або професійною діяльністю чи проектами. **АВ2.** Спроможність нести відповідальність за вироблення та ухвалення рішень у непередбачуваних робочих та/або навчальних контекстах. **АВ3.** Формування суджень, що враховують соціальні, наукові та етичні аспекти. **АВ4.** Організація та керівництво професійним розвитком осіб та груп. **АВ5.** Здатність продовжувати навчання із значним ступенем автономії.
ЗАГАЛЬНІ КОМПЕТЕНТНОСТІ				
ЗК1	+	+	+	+
ЗК2	+	+	+	+
ЗК3	+	+		+
ЗК4	+	+	+	+
ЗК5	+	+	+	+
ЗК6	+	+		+
ЗК7	+	+		
ЗК8		+	+	
СПЕЦІАЛЬНІ (ФАХОВІ) КОМПЕТЕНТНОСТІ				
СК1	+	+		+
СК2	+	+		+
СК3	+	+		+
СК4	+	+		
СК5	+	+	+	+
СК6	+	+		+
СК7	+	+		+
СК8	+			
СК9	+	+	+	+
СК10	+	+		
СК11	+	+		

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

Результати навчання	**Компетентності**																		
	Інтегральна компетентність																		
	Загальні								**Спеціальні (фахові)**										
	ЗК1	**ЗК2**	**ЗК3**	**ЗК4**	**ЗК5**	**ЗК6**	**ЗК7**	**ЗК8**	**СК1**	**СК2**	**СК3**	**СК4**	**СК5**	**СК6**	**СК7**	**СК8**	**СК9**	**СК10**	**СК11**
РН1	ЗП1 ЗП3 ЗП5 СП1 СП5 СП7 СП17 ПП1 ПП2							ЗП1 ЗП3 ЗП4 ЗП5 ЗП СП1 СП5 СП7 СП17 ПП6											
РН2		ЗП1 ЗП2 ЗП3 ЗП5 ЗП СП1 СП5 СП7 СП17 ПП1 ПП2																	
РН3			ЗП5 ЗП6 ЗП7 СП2 СП3 СП4 СП5 СП6 СП8 СП9 СП10 СП11 СП12 СП13			ЗП6 ЗП7 ЗП СП1 СП2 СП3 СП4 СП5 СП6 СП8 СП9 СП10 СП11 СП12	СП1 СП2 СП3 СП5 СП6 СП8 СП9 СП10 СП12 СП13 СП14 СП15 СП16 СП18	ЗП1 ЗП3 ЗП4 ЗП5 ЗП СП1 СП5 СП7 СП17 ПП6										

Результати навчання	Компетентності																		
	Інтегральна компетентність																		
	Загальні								Спеціальні (фахові)										
	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10	СК11
			СП14 СП15 СП16 СП18 СП19 СП21 СП22 СП23 СП24 СП25 СП26 ПП5 ПП2			СП13 СП14 СП15 СП16 СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП25 СП26 ПП2	СП19 СП20 СП21 СП22 СП23 СП24 ПП2												
РН4				ЗП3 ЗП5 ЗП СП3 СП4 СП5 СП7 СП8 СП12 СП13 СП14 СП17 СП18 СП19 СП20 СП22 СП23 СП24 СП25 СП26 ПП1 ПП2				ЗП1 ЗП3 ЗП4 ЗП5 ЗП СП1 СП5 СП7 СП17 ПП6										
РН5					ЗП4 СП3 СП5			ЗП1 ЗП3 ЗП4						СП4 СП5 СП8					

Результати навчання	Компетентності																		
	Інтегральна компетентність																		
	Загальні								Спеціальні (фахові)										
	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10	СК11
					СП8 СП12 СП13 СП14 СП18 СП19 СП22 СП23 ПП1 ПП2			ЗП5 ЗП СП1 СП5 СП7 СП17 ПП6						СП12 СП13 СП14 СП18 СП19 СП22 СП23 ПП2					
РН6							СП1 СП2 СП3 СП5 СП6 СП8 СП9 СП10 СП12 СП13 СП14 СП15 СП16 СП18 СП19 СП20 СП21 СП22 СП23 СП24 ПП2		СП2 СП4 СП5 СП6 СП9 СП18 СП21 СП23 СП24 ПП5 ПП2	СП1 СП2 СП4 СП5 СП6 СП7 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП17 СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП25 СП26 ПП5 ПП2								
РН7							СП1 СП2 СП3 СП5		СП2 СП4 СП5 СП6		СП1 СП2 СП4 СП5								

Результати навчання	Компетентності																		
	Інтегральна компетентність																		
	Загальні								Спеціальні (фахові)										
	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10	СК11
							СП6 СП8 СП9 СП10 СП12 СП13 СП14 СП15 СП16 СП18 СП19 СП20 СП21 СП22 СП23 СП24 ПП2		СП9 СП18 СП21 СП23 СП24 ПП5 ПП2		СП6 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП18 СП19 СП20 СП21 СП22 СП23 СП24 ПП5 ПП2								
РН8											СП1 СП2 СП4 СП5 СП6 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП18 СП19 СП20 СП21 СП22 СП23 СП24 ПП1 ПП2									
РН9									СП2										

Результати навчання	Компетентності																		
	Інтегральна компетентність																		
	Загальні								Спеціальні (фахові)										
	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10	СК11
									СП4 СП5 СП6 СП9 СП18 СП21 СП23 СП24 ПП1 ПП2										
РН10										СП1 СП2 СП4 СП5 СП6 СП7 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП17 СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП25 СП26 ПП1 ПП2	СП1 СП2 СП4 СП5 СП6 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП18 СП19 СП20 СП21 СП22 СП23 СП24 ПП1 ПП2								
РН11											СП1 СП2 СП4 СП5								

Результати навчання	Компетентності																		
	Інтегральна компетентність																		
	Загальні								Спеціальні (фахові)										
	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10	СК11
											СП6 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП18 СП19 СП20 СП21 СП22 СП23 СП24 ПП1 ПП2								
РН12											СП1 СП2 СП4 СП5 СП6 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП18 СП19 СП20 СП21 СП22 СП23 СП24 ПП1 ПП2								
РН13												СП3	СП3		СП1		СП3		

Результати навчання	Компетентності																		
	Інтегральна компетентність																		
	Загальні								Спеціальні (фахові)										
	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10	СК11
												СП4 СП5 СП7 СП11 СП17 СП20 ПП1 ПП2	СП4 СП5 СП8 СП9 СП11 СП12 СП13 СП14 СП15 СП18 СП19 СП22 СП23 СП24 ПП2		СП4 СП5 СП8 СП12 СП13 СП14 СП18 СП19 СП20 СП22 СП23 СП24 ПП1 ПП2		СП4 СП5 СП8 СП9 СП12 СП14 СП19 СП22 ПП2		
РН14																	СП3 СП4 СП5 СП8 СП9 СП12 СП14 СП19 СП22 ПП2	СП1 СП3 СП5 СП8 СП9 СП12 СП14 СП15 СП18 СП19 СП22 ПП2	СП4 СП5 СП8 СП12 СП13 СП14 СП18 СП19 СП21 СП22 СП23 ПП1 ПП2
РН15								ЗП1 ЗП3 ЗП4 ЗП5 ЗП СП1 СП5 СП7 СП17 ПП6											
РН16											СП1					СП1			

Результати навчання	Компетентності																		
	Інтегральна компетентність																		
	Загальні								Спеціальні (фахові)										
	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10	СК11
											СП2 СП4 СП5 СП6 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП18 СП19 СП20 СП21 СП22 СП23 СП24 ПП1 ПП2					СП3 СП4 СП5 СП8 СП10 СП11 СП12 СП14 СП16 СП19 СП20 СП22 ПП1 ПП2			
РН17											СП1 СП2 СП4 СП5 СП6 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП18 СП19 СП20 СП21 СП22 СП23 СП24	СП3 СП4 СП5 СП7 СП11 СП17 СП20 ПП1 ПП2	СП3 СП4 СП5 СП8 СП9 СП11 СП12 СП13 СП14 СП15 СП18 СП19 СП22 СП23 СП24 ПП2			СП1 СП3 СП4 СП5 СП8 СП10 СП11 СП12 СП14 СП16 СП19 СП20 СП22 ПП1 ПП2		СП1 СП3 СП5 СП8 СП9 СП12 СП14 СП15 СП18 СП19 СП22 ПП2	СП4 СП5 СП8 СП12 СП13 СП14 СП18 СП19 СП21 СП22 СП23 ПП1 ПП2

Результати навчання	Компетентності																		
	Інтегральна компетентність																		
	Загальні								Спеціальні (фахові)										
	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10	СК11
											ППІ1 ППІ2								
РН18							СП1 СП2 СП3 СП5 СП6 СП8 СП9 СП10 СП12 СП13 СП14 СП15 СП16 СП18 СП19 СП20 СП21 СП22 СП23 СП24 ППІ2		СП2 СП4 СП5 СП6 СП9 СП18 СП21 СП23 СП24 ППІ1 ППІ2		СП1 СП2 СП4 СП5 СП6 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП18 СП19 СП20 СП21 СП22 СП23 СП24 ППІ1 ППІ2	СП3 СП4 СП5 СП7 СП11 СП17 СП20 ППІ1 ППІ2	СП3 СП4 СП5 СП8 СП9 СП11 СП12 СП13 СП14 СП15 СП18 СП19 СП22 СП23 СП24 ППІ2	СП4 СП5 СП8 СП12 СП13 СП14 СП18 СП19 СП22 СП23 ППІ2					
РН19							СП1 СП2 СП3 СП5 СП6 СП8 СП9 СП10 СП12 СП13 СП14 СП15 СП16 СП18 СП19 СП20		СП2 СП4 СП5 СП6 СП9 СП18 СП21 СП23 СП24 ППІ1 ППІ2	СП1 СП2 СП4 СП5 СП6 СП7 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП17 СП18 СП19			СП3 СП4 СП5 СП8 СП9 СП11 СП12 СП13 СП14 СП15 СП18 СП19 СП22 СП23 СП24 ППІ2		СП1 СП4 СП5 СП8 СП12 СП13 СП14 СП18 СП19 СП20 СП22 СП23 СП24 ППІ1 ППІ2	СП1 СП3 СП4 СП5 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП16 СП19 СП20 СП22 ППІ1 ППІ2	СП3 СП4 СП5 СП8 СП9 СП12 СП14 СП19 СП22 ППІ2	СП1 СП3 СП5 СП8 СП9 СП12 СП14 СП15 СП18 СП19 СП22 ППІ2	СП4 СП5 СП8 СП12 СП13 СП14 СП18 СП19 СП21 СП22 СП23 ППІ1 ППІ2

Результати навчання	Компетентності																		
	Інтегральна компетентність																		
	Загальні								Спеціальні (фахові)										
	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10	СК11
							СП21 СП22 СП23 СП24 ПП2			СП20 СП21 СП22 СП23 СП24 СП25 СП26 ПП1 ПП2									
РН20																	СП3 СП4 СП5 СП8 СП9 СП12 СП14 СП19 СП22 ПП2	СП1 СП3 СП5 СП8 СП9 СП12 СП14 СП15 СП18 СП19 СП22 ПП2	СП4 СП5 СП8 СП12 СП13 СП14 СП18 СП19 СП21 СП22 СП23 ПП5 ПП2
РН21										СП1 СП2 СП4 СП5 СП6 СП7 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП17 СП18 СП19 СП20	СП1 СП2 СП4 СП5 СП6 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП18 СП19 СП20 СП21 СП22	СП3 СП4 СП5 СП7 СП11 СП17 СП20 ПП1 ПП2			СП1 СП4 СП5 СП8 СП12 СП13 СП14 СП18 СП19 СП20 СП22 СП23 СП24 ПП1 ПП2	СП1 СП3 СП4 СП5 СП8 СП10 СП11 СП12 СП14 СП16 СП19 СП20 СП22 ПП1 ПП2	СП3 СП4 СП5 СП8 СП9 СП12 СП14 СП19 СП22 ПП2	СП1 СП3 СП5 СП8 СП9 СП12 СП14 СП15 СП18 СП19 СП22 ПП2	СП4 СП5 СП8 СП12 СП13 СП14 СП18 СП19 СП21 СП22 СП23 ПП1 ПП2

Результати навчання	Компетентності																		
	Інтегральна компетентність																		
	Загальні								Спеціальні (фахові)										
	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10	СК11
										СП21 СП22 СП23 СП24 СП25 СП26 ПП1 ПП2	СП23 СП24 ПП1 ПП2								
РН22										СП1 СП2 СП4 СП5 СП6 СП7 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП17 СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП25 СП26 ПП1 ПП2	СП1 СП2 СП4 СП5 СП6 СП8 СП9 СП10 СП11 СП12 СП13 СП14 СП18 СП19 СП20 СП21 СП22 СП23 СП24 ПП1 ПП2	СП3 СП4 СП5 СП7 СП11 СП17 СП20 ПП1 ПП2			СП1 СП4 СП5 СП8 СП12 СП13 СП14 СП18 СП19 СП20 СП22 СП23 СП24 ПП1 ПП2	СП1 СП3 СП4 СП5 СП8 СП10 СП11 СП12 СП14 СП16 СП19 СП20 СП22 ПП1 ПП2	СП3 СП4 СП5 СП8 СП9 СП12 СП14 СП19 СП22 ПП2	СП1 СП3 СП5 СП8 СП9 СП12 СП14 СП15 СП18 СП19 СП22 ПП2	СП4 СП5 СП8 СП12 СП13 СП14 СП18 СП19 СП21 СП22 СП23 ПП1 ПП2

8. РЕЗУЛЬТАТИ ОБГОВОРЕННЯ ОСВІТНЬОЇ ПРОГРАМИ

Стейкхолдери (вказати ПІБ та посаду, місце роботи)	Зауваження/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.
Гарант ОПП, к.т.н., доц. Корольов Р. В., Завідувач кафедри, д.т.н., професор Євсеєв С. П. Члени робочої групи ОПП	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.
Войтко О. В., кадидат військових наук, доцент, начальник інституту стратегічних комунікацій Національного університету оборони України	Позитивний відгук. Без зауважень.	-	
Меленті Є. О., кандидат технічних наук, доцент, Перший проректор Національної академії Служби безпеки України	Позитивний відгук. Без зауважень.	-	
Ковтун В. Ю., кандидат технічних наук, доцент, директор ТОВ “Сайфер”	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.	-	

Завідувач кафедри кібербезпека _____ Сергій ЄВСЕЄВ

Гарант освітньої програми _____ Роман КОРОЛЬОВ

9. ПЛАН ВРАХУВАННЯ ЗАУВАЖЕНЬ/РЕКОМЕНДАЦІЙ ЗА РЕЗУЛЬТАТАМИ АКРЕДИТАЦІЙНОЇ ЕКСПЕРТИЗИ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

Рекомендації, надані під час останньої акредитації	Період врахування (короткостроковий/довгостроковий/не доцільно враховувати)	Заходи, що спрямовані на врахування рекомендацій/Обгрунтування щодо недоцільності впровадження рекомендації	Терміни впровадження заходів/відповідальні особи
Загальні рекомендації Експертної групи та Галузевої експертної групи (по кафедрі, галузі, інституту, університету)			
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