



МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
“ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ”



ЗАТВЕРДЖУЮ
В. Ректор НТУ «ХПІ»

Євген СОКОЛ

“ 30 ” березня 2026 р.

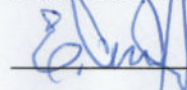
ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
“НАЦІОНАЛЬНА БЕЗПЕКА У СФЕРІ КІБЕРЗАХИСТУ”

першого (бакалаврського) рівня вищої освіти

за спеціальністю КЗ – Національна безпека (за окремими
сферами забезпечення і видами діяльності)
галузі знань К – Безпека та оборона
кваліфікація бакалавр з національної безпеки у сфері кіберзахисту

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 Національна безпека у сфері кіберзахисту

Рівень вищої освіти	Перший (бакалаврський)
Галузь знань	К – Безпека та оборона
Спеціальність	КЗ – “Національна безпека (за окремими сферами забезпечення видами діяльності)”
Кваліфікація	Бакалавр з національної безпеки у сфері кіберзахисту

СХВАЛЕНО

Робочою групою ОПП зі спеціальності
“Національна безпека (за окремими
сферами забезпечення і видами діяльності)”

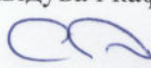
Гарант ОПП

 Сергій ЄВСЕЄВ

Протокол № 1_
« 16 » січня 2026 р.

ПОГОДЖЕНО

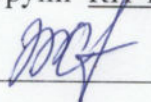
Завідувач кафедри кібербезпеки

 Сергій ЄВСЕЄВ

Протокол № 12_
« 23 » березня 2026 р.

ПОГОДЖЕНО

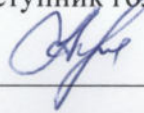
Здобувач вищої освіти
(член робочої групи ОПП)
№ групи КН-1323

 Никита ЖИЛЯЄВ

« 23 » березня 2026 р.

РЕКОМЕНДОВАНО

Методичною радою НТУ «ХПІ»
Заступник голови методичної ради

 Руслан МИГУЩЕНКО

Протокол № 3
« 25 » березня 2026 р.

ПОГОДЖЕНО

Директор навчально-наукового інституту
комп'ютерних наук та інформаційних
технологій

 Михайло ГОДЛЕВСЬКИЙ

« ____ » _____ 2026 р.

ЗАТВЕРДЖЕНО ТА НАДАНО ЧИННОСТІ

Наказом ректора Національного технічного університету «Харківський політехнічний інститут» від « 30 » березня 2026 року № 119 ОД.

Ця освітньо-професійна програма не може бути повністю або частково відтворена, тиражована та розповсюджена без дозволу Національного технічного університету «Харківський політехнічний інститут».

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, кандидат 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
“НАЦІОНАЛЬНА БЕЗПЕКА У СФЕРІ КІБЕРЗАХИСТУ”

першого (бакалаврського) рівня вищої освіти,
спеціальності КЗ “Національна безпека (за окремими сферами забезпечення і
видами діяльності)”

кафедри кібербезпеки Національного технічного університету
“Харківський політехнічний інститут”

Національна безпека держави є одним з головних завдань сучасної держави. В умовах ведення гібридних війн, появи кіберфізичних систем критичної інфраструктури та необхідності їх захисту від кібератак невіддільною частиною є підготовка фахівців у сфері національної безпеки, які спроможні виконувати завдання щодо забезпечення необхідного рівня захисту бізнес-процесів підприємств, як державної, так і власної форм власності.

Підготовка якісних спеціалістів за спеціальністю КЗ "Національна безпека (за окремими сферами забезпечення і видами діяльності)" повинна відбуватися у відповідно до поступового трансформування навчальних програм та навчальних планів дисциплін пов'язаних з напрямком "Національна безпека у сфері кіберзахисту ", що сформована кафедрою кібербезпеки Національного технічного університету "Харківський політехнічний інститут", відповідно до останніх тенденцій розвитку спеціальності.

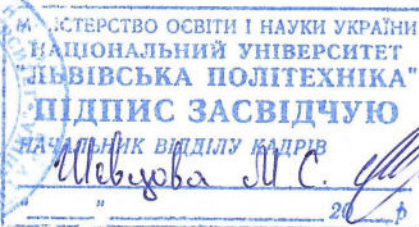
Запропонована освітньо-професійна програма спрямована на надання інтегральної компетенції щодо здатності здобувача освіти розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки та/або кібербезпеки у сфері національної безпеки, що характеризується комплексністю та неповною визначеністю умов. Насправді реальні сценарії кіберзагроз, характеризуються невизначеністю, синергетичним характером походження та несподшаними умовами втручання. Поруч із цим, є багато сценаріїв, що можна заздалегідь передбачити та побудувати надійний

контур безпеки, наприклад, як на рівні обчислювальної мережі невеликої компанії, так й розподіленої мережі корпоративного рівня.

Об'єкт вивчення за освітньо-професійною програмою "Національна безпека у сфері кіберзахисту": об'єкти національної безпеки, включаючи об'єкти критичної інфраструктури, інформаційно-комунікаційні системи, інформаційні ресурси та технології; технології забезпечення безпеки інформації; процеси управління інформаційною та/або кібербезпекою об'єктів, що підлягають захисту. Це свідчить, що майбутні фахівці з національної безпеки у сфері кіберзахисту будуть здатні використовувати та впроваджувати технології інформаційної та/або кібербезпеки у практичних ситуаціях на виробництві або на рівні налагодження інформаційної безпеки невеликої організації.

Слід підвести, що освітньо-професійна програма "Національна безпека у сфері кіберзахисту" першого (бакалаврського) рівня вищої освіти, що складена та запропонована кафедрою кібербезпеки Національного технічного університету "Харківський політехнічний інститут", має всі необхідні компоненти для підготовки кваліфікованих фахівців, які будуть впроваджені на сучасному ринку праці.

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



Іван ОПРСЬКИЙ

**РЕЦЕНЗІЯ-ВІДГУК
НА ОСВІТНЬО-ПРОФЕСІЙНУ ПРОГРАМУ
“НАЦІОНАЛЬНА БЕЗПЕКА У СФЕРІ КІБЕРЗАХИСТУ”**

першого (бакалаврського) рівня вищої освіти
спеціальності КЗ “Національна безпека (за окремими сферами забезпечення і
видами діяльності)”
кафедри кібербезпеки Національного технічного університету
“Харківський політехнічний інститут”

Відповідно до Закону України “Про національну безпеку України”, національними інтересами України є життєво важливі інтереси людини, суспільства і держави, реалізація яких забезпечує державний суверенітет України, її прогресивний демократичний розвиток, а також безпечні умови життєдіяльності та добробут її громадян. Саме питання забезпечення кіберзахисту національних інтересів є одним із важливих завдань держави.

Стрімкий розвиток інформаційних технологій і швидке зростання глобальної мережі Інтернет призвели до формування інформаційного середовища, що впливає на всі сфери людської діяльності. З одного боку, нові технологічні можливості полегшують поширення інформації, підвищують ефективність виробничих процесів, сприяють розширенню ділових операцій в процесі бізнесу. З іншої, інтенсивний розвиток комп’ютерних засобів й інформаційних технологій, вразливість сучасних інформаційних систем і комп’ютерних мереж, на жаль, не зменшується. Тому, проблеми забезпечення інформаційної безпеки привертають пильну увагу як фахівців у сфері національної безпеки, так і численних користувачів, включаючи компанії, що працюють у сфері електронного бізнесу.

Без знань і кваліфікованого застосування сучасних технологій, стандартів, протоколів і засобів захисту інформації неможливо досягти необхідного рівня національної безпеки та забезпечити надійний захист національних інтересів України.

Кафедрою кібербезпеки Національного технічного університету Харківський політехнічний інститут» розроблено освітньо-професійну програму “Національна безпека у сфері кіберзахисту” та навчальні плани

дисциплін, які пов'язані з напрямом п
широкого профілю, яка формує спектр
отримання результатів навчання, які і
“Національна безпека (за окремими
діяльності)”.

Освітньо-професійна програма готу
необхідний рівень кібербезпеки систем різного призначення та природи, в
першу чергу системи бізнес-процесів економічних систем та ін., на будь-
якому рівні управлінської ієрархії, враховуючи принципи застосування
криптографічних методів, сучасних технологій забезпечення кібербезпеки,
інформаційної безпеки та безпеки інформації в межах національних і
міжнародних стандартів й практик щодо здійснення професійної діяльності.

Слід підвести, що освітньо-професійна програма “Національна безпека у
сфері кіберзахисту” першого (бакалаврського) рівня вищої освіти, що
запропонована кафедрою кібербезпеки Національного технічного
університету “Харківський політехнічний інститут” має всі необхідні
компоненти для підготовки кваліфікованих фахівців, забезпечує надбання
ними відповідних компетенцій та спроможностей щодо вирішення актуальних
завдань забезпечення національної безпеки в сучасних умовах та перспектив
розвитку держави та може бути рекомендована до впровадження в освітній
процес.

Начальник інституту стратегічних комунікацій
кандидат військових наук, доцент

02 04 2025 рік



Олександр ВОЙТКО

РЕЦЕНЗІЯ-ВІДГУК
НА ОСВІТНЬО-ПРОФЕСІЙНУ ПРОГРАМУ
«НАЦІОНАЛЬНА БЕЗПЕКА У СФЕРІ КІБЕРЗАХИСТУ»

першого (бакалаврського) рівня вищої освіти
спеціальності КЗ «Національна безпека
(за окремими сферами забезпечення і видами діяльності)»
кафедри кібербезпеки Національного технічного університету
«Харківський політехнічний інститут»

Відповідно до рішення Ради національної безпеки та оборони України від 30 грудня 2021 року «Про План реалізації Стратегії кібербезпеки України» в державі здійснюються заходи щодо розбудови системи захисту об'єктів критичної інфраструктури від кібератак, стимулювання досліджень і розробок у сфері кібербезпеки з урахуванням появи нових кіберзагроз і викликів. Реалізація плану обумовлює потребу у фахівцях-управлінцях.

Освітньо-професійна програма «Національна безпека у сфері кіберзахисту» першого (бакалаврського) рівня вищої освіти, що запропонована кафедрою кібербезпеки Національного технічного університету «Харківський політехнічний інститут», є сучасним інструментом щодо формування у здобувачів вищої освіти компетенцій з національної безпеки у сфері кіберзахисту.

Освітньо-професійна програма передбачає планомірне та поступове оволодіння знаннями із засад національної безпеки держави, управління інформаційною безпекою, отримання інформації технічними засобами розвідки, конкурентної розвідки, методів технічного захисту інформації, криптології, баз даних та організації їх безпеки, організації документообігу з обмеженим доступом. Передбачається, що здобувачі вищої освіти отримають навички з: складання алгоритмів та їх верифікації, програмування, моделювання об'єктів критичної інфраструктури; криптографії та криптоаналізу; моніторингу відкритих ресурсів мережі Інтернет; адміністрування баз даних; антивірусного захисту інформації.

Очікувані компетентності надають можливість працевлаштування в: органах державної влади, що формують та реалізують державну політику у сфері національної безпеки, на посадах, які визначено у відповідних стандартах; центрах безпеки об'єднаних територіальних громад; громадських об'єднаннях, неурядових та міжнародних організаціях, діяльність яких пов'язана із забезпеченням національної безпеки; науково-освітніх установах, що досліджують проблеми національної безпеки.

Окрім технічних аспектів кіберзахисту, програма також приділяє увагу правовим і етичним аспектам інформаційної безпеки. Програма охоплює законодавство України та міжнародні нормати кібербезпеки, принципи етичного хакінгу, а також кіберінциденти в рамках правового поля. Це дозволяє працювати в умовах сучасного правового середовища, формуючи національну політику з кібербезпеки.

Розвиток співпраці з IT-компаніями, державними та міжнародними організаціями створює можливості стажування, що сприяє набуттю практичних навичок та конкурентоспроможності випускників на ринку праці. Використання технологій у навчальному процесі, зокрема віртуальних симуляторів кіберзагроз, забезпечує ефективну підготовку до роботи у динамічному середовищі цифрової безпеки.

Розроблена освітньо-професійна програма відносно підготовки фахівців у сфері національної безпеки потенційних роботодавців (стейкхолдерів), а також до впровадження в освітній процес.

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

_____ 2025 року



Євген МЕЛЕНТИ

Націона кандида

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 "НАЦІОНАЛЬНА БЕЗПЕКА У СФЕРІ КІБЕРЗАХИСТУ"

першого (бакалаврського) рівня вищої освіти
спеціальності КЗ "Національна безпека (за окремими сферами забезпечення і видами
діяльності)"

кафедри кібербезпеки Національного технічного університету
"Харківський політехнічний інститут"

В сучасному світі забезпечення національної безпеки держави неможливо без вирішення питань протидії кібернетичним загрозам, що існують на різних рівнях організації суспільства: починаючи від критичної інфраструктури держави, міністерств, відомств, органів державної влади та самоуправління на місцях, великих галузеутворюючих підприємств та фінансових установ, і до підприємств малого і середнього бізнесу (особливо задіяних у виконанні державних проектів, розробці інноваційних технологій, наукових дослідженнях, координації та логістиці критично важливих перевезень), комунальних підприємств та соціальних служб, і, навіть, на рівні окремих громадян, які можуть стати ціллю кібератак, спрямованих на отримання несанкціонованого доступу до персональної чи професійної інформації (що є у їх власному обігу громадянина), з метою прямих крадіжок коштів з банківських рахунків або більш досконалих шахрайських дій, чи навіть (промислового) шпигунства або шантажу публічних осіб. Отже забезпечення кіберзахисту інформаційних систем (та інформації, що в них циркулює), на всіх зазначених вище рівнях організації суспільства, є обов'язковою умовою національної безпеки держави. Тому

підготовка висококваліфікованих фахівців з національної безпеки у сфері кіберзахисту є одним з важливих та невідкладних завдань держави.

Фахівці у галузі кібербезпеки, які стоять на сторожі національної безпеки держави, 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. З метою кращого розуміння методів захисту інформації, необхідно надати студентам базові знання з математичних та фізичних основ побудови типових засобів кібербезпеки та сформувати навички власної розробки програмного забезпечення відповідного призначення. Саме з метою досягнення перелічених вище цілей, кафедрою кібербезпеки Національного технічного університету «Харківський політехнічний інститут» розроблено освітньо-професійну програму «Національна безпека у сфері кіберзахисту».

Програма формує висококваліфікованих спеціалістів, затребуваних на ринку праці, здатних ефективно впроваджувати сучасні технології захисту, зокрема інструменти на основі штучного інтелекту, тому вважаю, що освітньо-професійна програма «Національна безпека у сфері кіберзахисту» першого (бакалаврського) рівня вищої освіти спеціальності КЗ «Національна безпека (за окремими сферами забезпечення і видами діяльності)» містить усі необхідні елементи для підготовки сучасних фахівців, здатних вирішувати теоретичні й практичні завдання у сфері кіберзахисту.

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



Владислав КОВТУН

ПЕРЕДМОВА

Відповідає галузі знань Безпека та оборона, спеціальності Національна безпека (за окремими сферами забезпечення і видами діяльності) відповідно до національної рамки кваліфікації.

Розроблено робочою групою освітньо-професійної програми “Національна безпека у сфері кіберзахисту”

Навчально-наукового інституту комп’ютерних наук та інформаційних технологій

Національного технічного університету “Харківський політехнічний інститут” у складі:

Гарант освітньо-професійної програми

Сергій ЄВСЕЄВ, доктор технічних наук, професор, завідувач кафедри кібербезпеки.

Члени робочої групи ОПП:

1. Андрій ТКАЧОВ, кандидат технічних наук, старший науковий співробітник, доцент кафедри кібербезпеки.
2. Роман КОРОЛЬОВ, кандидат технічних наук, доцент кафедри кібербезпеки.
3. Никита ЖИЛЯЄВ, студент групи КН-1323.

**1. ПРОФІЛЬ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ ЗА
СПЕЦІАЛЬНІСТЮ КЗ – НАЦІОНАЛЬНА БЕЗПЕКА (ЗА ОКРЕМИМИ
СФЕРАМИ ЗАБЕЗПЕЧЕННЯ І ВИДАМИ ДІЯЛЬНОСТІ)**

1 – Загальна інформація	
Вищий навчальний заклад та структурний підрозділ	Національний технічний університет “Харківський політехнічний інститут”, Навчально-науковий інститут <u>комп’ютерних наук та інформаційних технологій</u> кафедра <u>кібербезпеки</u>
Ступінь вищої освіти та назва кваліфікації (освітньої, професійної) мовою оригіналу	Ступінь вищої освіти – Бакалавр Галузь знань - К Безпека та оборона Спеціальність – КЗ Національна безпека (за окремими сферами забезпечення і видами діяльності) Освітня кваліфікація – бакалавр з національної безпеки у сфері кіберзахисту.
Професійна кваліфікація	Відсутня
Форма навчання	Інституційна (очна (денна))
Офіційна назва освітньої програми	Національна безпека у сфері кіберзахисту
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 України – 6 рівень; EQF LLL – 6 рівень; FQ-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 освітньої програми	Переглядається щорічно
Посилання на постійне розміщення опису освітньої програми	https://blogs.kpi.kharkov.ua/v2/quality/dokumenty/diyuchy-osvitni-programy/osvitnij-riven-bakalavr/

2 – Мета освітньо-професійної програми	
Підготовка аналітиків із питань національної безпеки, фахівців із сучасних методів менеджменту національної безпеки, спеціалістів антикризового управління та системи безпеки, та створити передумови для подальшого вивчення державноуправлінських аспектів забезпечення національної безпеки на другому (магістерському) рівні вищої освіти у національній академії СБУ.	
3 – Характеристика освітньо-професійної програми	
Предметна область (галузь знань, спеціальність, спеціалізація або предметна спеціальність (за наявності))	Галузь знань: К “Безпека та оборона” Спеціальність: КЗ “Національна безпека (за окремими сферами забезпечення і видами діяльності)” Об’єкт вивчення: – національні цінності, інтереси та цілі; – загрози, ризики, негативні тенденції в окремих сферах національної безпеки; – безпекове середовище на національному, регіональному та глобальному рівнях; – державна політика, законодавство, концептуальні та інституційні засади забезпечення національної безпеки у мирний час та в особливий період відповідно до виду діяльності. Цілі навчання: підготовка фахівців здатних використовувати і впроваджувати технології кіберзахисту в галузі національної безпеки. Теоретичний зміст предметної області: Теорії, поняття, принципи, концепції, категорії національної безпеки за окремими сферами її забезпечення і видами діяльності. Методи, методики та технології: Методи, методики та технології моніторингу стану національної безпеки; виявлення та розпізнавання реальних і потенційних загроз і ризиків щодо національної безпеки, прогнозування та моделювання сценаріїв кризових ситуацій, прийняття управлінських рішень щодо національної безпеки, планування, організації та контролю виконання заходів з національної безпеки, мотивації персоналу, запобігання корупції та забезпечення доброчесності, адаптивного управління у кризових ситуаціях у сфері національної безпеки, комунікації (взаємодії, координації); оцінювання ефективності та результативності за окремими сферами забезпечення національної безпеки та видами діяльності. Інструменти та обладнання: Спеціалізовані: обладнання, програмне забезпечення, інформаційно-комунікаційні системи та електронні бази даних за окремими сферами забезпечення національної безпеки та видами діяльності.
Орієнтація освітньої програми	Освітньо-професійна. Підготовка фахівців у сфері національної безпеки (за окремими сферами забезпечення і

	видами діяльності)
Основний фокус освітньої програми та спеціалізації або предметна спеціальність (за наявності)	Спеціальна освіта за спеціальністю національна безпека (за окремими сферами забезпечення і видами діяльності), яка забезпечує підготовку професіонала, здатного розв'язувати задачі кіберзахисту у сфері національної безпеки, виявляти та протидіяти загрозам національній безпеці України (за окремими сферами забезпечення і видами діяльності). Ключові слова: управлінська діяльність у визначальних сферах національної безпеки (політичній, економічній, соціальній, гуманітарній), у тому числі в умовах кризових ситуацій.
Особливості програми	Особливістю програми спеціальності “Національна безпека (за окремими сферами забезпечення і видами діяльності)” є проходження виробничої практики в органах державної влади тривалістю 4 тижні.
4 – Придатність випускників до працевлаштування та академічні права випускників	
Придатність до працевлаштування	Фахівці з національної безпеки у сфері кіберзахисту 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 підтримки інфраструктури кіберзахисту; 2139.2 Фахівець з реагування на інциденти кібербезпеки; 2139.2 Фахівець з технічного 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 освітньо-професійною програмою та здобула ступінь бакалавра може продовжити навчання на другому (магістерському) рівні вищої освіти (при проходженні відбору у національній академії СБУ), а також має можливість набуття додаткових кваліфікацій в системі післядипломної освіти та підвищення кваліфікації.
5 – Викладання та оцінювання	
Викладання та навчання	Студентоцентроване навчання, самонавчання, проблемно-орієнтоване навчання, навчання через практикуми, які відбуваються на базах практики. На другому та 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 діяльність при вирішенні складних спеціалізованих завдань у визначальних сферах національної безпеки (політичній, економічній, соціальній, гуманітарній), у тому числі в умовах кризових ситуацій, що передбачає застосування теорій та наукових методів відповідної галузі і характеризується комплексністю та невизначеністю умов
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 адаптації та дії в новій ситуації. ЗК7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. ЗК8. Здатність використовувати інформаційні та комунікаційні технології і на цій основі формувати ефективну систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо запобігання, протидії та нейтралізації загроз національній безпеці. ЗК9. 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 виклики та загрози національній безпеці за напрямками професійної діяльності, синтезувати інформацію щодо розроблення та реалізації елементів стратегій у визначальних сферах національної безпеки (політичній, економічній, соціальній, гуманітарній). СК3. Здатність використовувати знання щодо ролі, місця та призначення політичних та безпекових інститутів України для ефективного здійснення заходів при виконанні обов'язків з питань забезпечення національної безпеки. СК4. Здатність демонструвати та застосовувати знання з основ теорії національної безпеки. СК5. Здатність використовувати історичний досвід військових та політичних стратегій іноземних держав з метою вирішення завдань з національної безпеки. СК6. Здатність використовувати іноземну мову для отримання додаткових знань і умінь з питань національної безпеки, взаємодіяти з іноземними партнерами. СК7. Здатність визначати необхідні правові та організаційні заходи врегулювання конфліктів, пов'язаних із забезпеченням національної безпеки. СК8. Здатність використовувати механізми забезпечення національної безпеки у її визначальних сферах. СК9. Здатність використовувати знання щодо безпекової складової зовнішньої політики України та інших держав. СК10. Здатність засвоювати основні теоретичні поняття та набуття практичних навичок дослідження, підготовки документів та їх використання в управлінській діяльності. СК11. Здатність використовувати практичні навички, тактику та прийоми роботи з людьми в інтересах службової діяльності. СК12. Здатність виконувати заходи територіальної оборони, а також цивільного захисту у межах професійної компетентності. СК13. Здатність оцінювати вплив глобальних проблем і трансформацій геополітичного та гео економічного простору на національну безпеку. СК14. Здатність здійснювати моніторинг зовнішньої та внутрішньої політики держави у контексті забезпечення національної безпеки, готувати пропозиції щодо підвищення її ефективності.
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. Вміти адаптовуватись до нових викликів та дій у певних ситуаціях. РН7. Вміти виявляти, ставити та вирішувати професійні завдання, вміти узагальнювати отримані результати, обробляти та аналізувати інформацію з різних джерел, оформлювати і презентувати результати досліджень відповідно до вимог. РН8. Вміти використовувати інформаційні та комунікаційні технології і на цій основі формувати ефективні системи інформаційно-аналітичного забезпечення підтримки прийняття рішень щодо запобігання, протидії та нейтралізації загроз національній безпеці. РН9. Вміти використовувати безпекові режими під час виконання службових обов'язків. РН10. Вміти аналізувати виклики та загрози національній безпеці за напрямками професійної діяльності та синтезувати інформацію щодо розроблення та реалізації стратегій у визначальних сферах національної безпеки (політичній, економічній, соціальній, гуманітарній). РН11. Вміти пояснювати роль, місце та призначення політичних та безпекових інститутів України для ефективного здійснення заходів при виконання обов'язків з питань забезпечення національної безпеки. РН12. Вміти застосовувати знання з основ теорії національної безпеки, зокрема: оцінювати обстановку, рівень викликів та загроз національній безпеці. РН13. Вміти використовувати історичний досвід військових та політичних стратегій іноземних держав з метою вирішення завдань з національної безпеки. РН14. Вміти читати й розуміти фахову іншомовну літературу, використовуючи її у соціальній і професійній сферах, а також демонструвати культуру мислення та виявляти навички щодо організації культурного діалогу з іноземними партнерами на рівні, необхідному для професійної діяльності. РН15. Вміти визначати необхідні правові та організаційні заходи врегулювання конфліктів, пов'язаних із забезпеченням національної безпеки.
--	--

	RH16. Використовувати у професійній діяльності окремі елементи механізму впливу та взаємодії у процесі забезпечення окремих складових національної безпеки. RH17. Вміти використовувати отримані знання щодо безпекової складової зовнішньої політики України та інших держав. RH18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності. RH19. Вміти використовувати у професійній діяльності методи та інструменти організації соціальної взаємодії, співробітництва та розв'язання конфліктів у сфері професійної діяльності, практичні навички, тактику та прийоми, роботи з людьми в інтересах службової діяльності: працювати у команді з позицій лідера, радника (консультанта), помічника, планувати використання часу та визначати стимули і бар'єри ефективної роботи, здійснювати розподіл (делегування) функцій, повноважень і відповідальності між виконавцями. RH20. Вміти виконувати заходи територіальної оборони, а також цивільного захисту у межах професійної компетентності. RH21. Вміти оцінювати вплив глобальних проблем і трансформацій геополітичного та гео економічного простору на національну безпеку, здійснювати моніторинг зовнішньої та внутрішньої політики держави у контексті забезпечення національної безпеки та готувати пропозиції щодо підвищення її ефективності.
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 Міністрів України 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-k3-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 «НАЦІОНАЛЬНА БЕЗПЕКА У СФЕРІ КІБЕРЗАХИСТУ» ТА ЇХ ЛОГІЧНА ПОСЛІДОВНІСТЬ

2.1 Перелік компонент освітньо-професійної програми

Код н/д	Компоненти освітньої 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 2	Історія української державності	4,0	Екзамен
ЗП 3	Українська мова (професійного спрямування)	3,0	Залік
ЗП 4	Іноземна мова	16,0	Залік, Екзамен
ЗП 5	Основи гуманітарно-філософських знань у професійній діяльності	4,0	Екзамен
ЗП 6	Вища математика	5,0	Залік
ЗП 7	Основи вищої алгебри	6,0	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	6,0	Екзамен
СП 3	Національна безпека держави	4,0	Екзамен
СП 4	Теорія інформації і кодування	5,0	Екзамен
СП 5	Фізичні основи технічних засобів розвідки	4,0	Залік
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	Математичні основи криптології	4,0	Екзамен
СП10	Технології програмування	4,0	Екзамен
СП 11	Методи соціальної інженерії в кібербезпеці	3,0	Екзамен
СП 12	Комп'ютерні мережі	4,0	Екзамен
СП 13	Розробка програмного забезпечення систем кібербезпеки	6,0	Екзамен
СП 14	Основи криптографічного захисту	5,0	Залік
СП 15	Цифрова криміналістика	5,0	Екзамен
СП 16	Основи стеганографічного захисту інформації	4,0	Екзамен
СП 17	Організація документообігу з обмеженням доступом	4,0	Екзамен
СП 18	Безпека смарт-технологій	5,0	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	Інформаційно-комунікаційні системи у сфері національної безпеки	4,0	Екзамен
СП 23	Безпека інтернет-речей	4,0	Екзамен
СП 24	Нейронні мережі	5,0	Залік
СП 25	Промисловий та офісний шпiонаж	4,0	Залік
СП 26	Гiбриднi вiйни та національна безпека	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			
Профільований пакет освітніх компонент 01 <u>“Штучний інтелект в системах захисту”</u>			
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
Профільований пакет освітніх компонент 02 <u>“Блокчейн-технологія та безпека банківських систем”</u>			
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 обмеженням доступом	3,0	Екзамен
ВП2.7	Безпека DevOps	3,0	Екзамен
Профільований пакет освітніх компонент 03 <u>“Innovation Campus”</u>			
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

ВПЗ.5	Архітектура корпоративних інформаційних систем	3,0	Екзамен
ВПЗ.6	Безпека та аудит бездротових та рухомих мереж	3,0	Екзамен
ВПЗ.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 вибіркового компонент:		61	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ:		240	

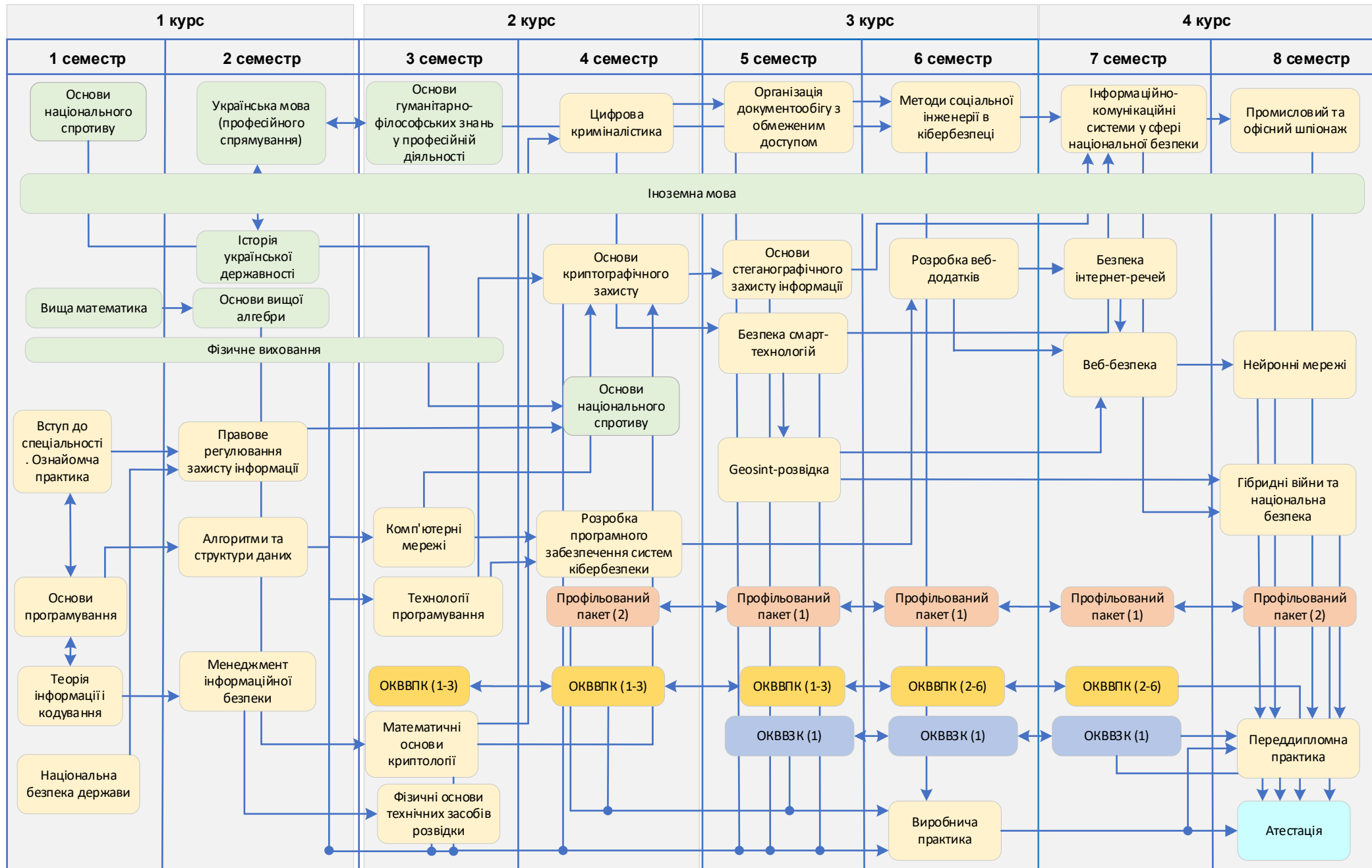
3. РОЗПОДІЛ ЗМІСТУ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ ЗА ГРУПАМИ КОМПОНЕНТІВ ТА ЦИКЛАМИ ПІДГОТОВКИ

№ п/п	Цикл підготовки	Обсяг навчального навантаження здобувача вищої освіти (кредитів ECTS / %)		
		Обов'язкові компоненти освітньо-професійної програми	Вибіркові компоненти освітньо-професійної програми	Всього за весь термін навчання
1	Загальна підготовка	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	+	+		+
ЗК9		+		+
СПЕЦІАЛЬНІ (ФАХОВІ) КОМПЕТЕНТНОСТІ				
СК1	+	+	+	+
СК2		+	+	+
СК3		+		+
СК4	+	+		
СК5	+	+		
СК6	+	+	+	+
СК7	+	+		+
СК8	+	+		+
СК9	+	+		+
СК10	+	+		+
СК11	+	+	+	+
СК12	+	+		+
СК13		+		+
СК14		+		+

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

[illegible]

Результати навчання	Компетентності																						
	Інтегральна компетентність																						
	Загальні									Спеціальні (фахові)													
	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	ЗК9	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10	СК11	СК12	СК13	СК14
						СП20 СП21 СП22 СП23 СП24 СП25 СП26 ПП1 ПП2																	
РН4	ЗП1 ЗП3 ЗП4 ЗП5 СП1 СП3 СП7 СП19 СП22	ЗП2 ЗП3 ЗП5 ЗП СП1 СП1 СП3		ЗП3 ЗП СП1 СП3 СП5 СП14 СП16 ПП1 ПП2					ЗП1 ЗП3 ЗП4 ЗП5 ЗП СП1 СП11														
РН5					ЗП4 ПП1 ПП2	ЗП1 ЗП СП1 СП7 СП18 СП23 ПП1 ПП2			ЗП1 ЗП3 ЗП4 ЗП5 ЗП СП1 СП11						СП3 СП8 СП19 СП22 СП26 ПП1 ПП2								
РН6						ЗП1 ЗП СП1 СП7 СП18 СП23 ПП1 ПП2																	
РН7			ЗП5 ЗП6 ЗП7 СП1				ЗП5 ЗП6 ЗП7 СП1	СП1 СП2 СП3 СП4			СП1 СП3 СП4 СП5	СП1 СП3 СП4 СП5	СП4 СП5 СП9 СП12	СП1 СП8 СП26		СП7 СП8 СП26 ПП1		СП1 СП3 СП4 СП5	СП2 СП6 СП7 СП8	СП8 СП11 СП14 СП16	СП8 СП26 ПП1 ПП2	СП1 СП3 СП8 СП19	СП7 СП8 СП26 ПП1

Результати навчання	Компетентності																								
	Інтегральна компетентність																								
	Загальні									Спеціальні (фахові)															
	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	ЗК9	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10	СК11	СК12	СК13	СК14		
			СП2 СП4 СП5 СП6 СП8 СП9 СП10 СП11 СП13 СП14 СП15 СП16 СП20 СП21 СП25 СП26				СП2 СП3 СП4 СП5 СП6 СП7 СП8 СП10 СП11 СП12 СП13 СП14 СП15 СП16 СП18 СП19 СП20 СП21 СП22 СП23 СП24 СП25 СП26 ПП1 ПП2				СП7 СП8 СП11 СП12 СП15 СП16 СП17 СП24 СП26				СП19 СП22 СП24 ПП1 ПП2			ПП2		СП7 СП8 СП17 СП26 ПП1 ПП2	СП10 СП13 СП17 СП18 СП20 СП23 СП26 ПП1 ПП2	СП17 СП25 СП26 ПП1 ПП2		СП22 СП26 ПП1 ПП2	ПП2
PH8								СП1 СП2 СП3 СП4 СП5 СП6 СП7 СП10 СП11 СП12 СП13 СП15 СП16		СП1 СП3 СП4 СП5 СП7 СП8 СП11 СП12 СП15 СП16 СП17 СП24 СП26						СП4 СП5 СП8 СП9 СП11 СП12 СП14 СП16 СП18 СП19 СП22 СП23 СП24	СП1 СП3 СП4 СП5 СП7 СП8 СП17 СП26 ПП1 ПП2	СП2 СП6 СП7 СП8 СП10 СП13 СП17 СП18 СП20 СП23 СП26 ПП1 ПП2		СП8 СП26 ПП1 ПП2	СП1 СП3 СП8 СП19 СП22 СП26 ПП1 ПП2				

Результати навчання	Компетентності																							
	Інтегральна компетентність																							
	Загальні									Спеціальні (фахові)														
	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	ЗК9	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10	СК11	СК12	СК13	СК14	
							СП17 СП19 СП20 СП21 СП22 СП24 ПП1 ПП2									СП26 ПП1 ПП2								
РН9						ЗП1 ЗП СП1 СП7 СП18 СП23 ПП1 ПП2				СП1 СП7 СП12 СП14 СП17 СП19 СП21 СП22 СП24														
РН10							ЗП5 ЗП6 ЗП7 СП1 СП2 СП3 СП4 СП5 СП6 СП7 СП8 СП10 СП11 СП12 СП13 СП14 СП15 СП16 СП18 СП19 СП20				СП1 СП3 СП4 СП5 СП7 СП8 СП11 СП12 СП15 СП16 СП17 СП24 СП26													

Результати навчання	Компетентності																							
	Інтегральна компетентність																							
	Загальні									Спеціальні (фахові)														
	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	ЗК9	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10	СК11	СК12	СК13	СК14	
						СП21 СП22 СП23 СП24 СП25 СП26 ПП1 ПП2																		
PH11											СП1 СП3 СП4 СП5													
PH12											СП4 СП5 СП9 СП12 СП19 СП22 СП24 ПП1 ПП2					СП4 СП5 СП8 СП9 СП11 СП12 СП14 СП16 СП18 СП19 СП22 СП23 СП24 СП26 ПП1 ПП2	СП1 СП3 СП4 СП5 СП7 СП8 СП17 СП26 ПП1 ПП2			СП8 СП26 ПП1 ПП2	СП1 СП3 СП8 СП19 СП22 СП26 ПП1 ПП2			
PH13													СП1 СП8 СП26											
PH14														СП3 СП8 СП19 СП22 СП26 ПП1 ПП2										

Результати навчання	Компетентності																						
	Інтегральна компетентність																						
	Загальні									Спеціальні (фахові)													
	ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	ЗК9	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10	СК11	СК12	СК13	СК14
РН15																СП7 СП8 СП26 ПП1 ПП2							
РН16																	СП4 СП5 СП8 СП9 СП11 СП12 СП14 СП16 СП18 СП19 СП22 СП23 СП24 СП26 ПП1 ПП2	СП1 СП3 СП4 СП5 СП7 СП8 СП17 СП26 ПП1 ПП2					
РН17														СП1 СП8 СП26	СП3 СП8 СП19 СП22 СП26 ПП1 ПП2	СП7 СП8 СП26 ПП1 ПП2	СП4 СП5 СП8 СП9 СП11 СП12 СП14 СП16 СП18 СП19 СП22 СП23 СП24 СП26 ПП1 ПП2	СП1 СП3 СП4 СП5 СП7 СП8 СП17 СП26 ПП1 ПП2					

Результати навчання	Компетентності																							
	Інтегральна компетентність																							
	Загальні									Спеціальні (фахові)														
ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	ЗК7	ЗК8	ЗК9	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9	СК10	СК11	СК12	СК13	СК14		
РН18																			СП2 СП6 СП7 СП8 СП10 СП13 СП17 СП18 СП20 СП23 СП26 ПП1 ПП2	СП8 СП11 СП14 СП16 СП17 СП25 СП26 ПП1 ПП2	СП8 СП26 ПП1 ПП2			
РН19									ЗП1 ЗП3 ЗП4 ЗП5 ЗП СП1 СП11	СП1 СП7 СП12 СП14 СП17 СП19 СП21 СП22 СП24										СП8 СП11 СП14 СП16 СП17 СП25 СП26 ПП1 ПП2				
РН20																					СП8 СП26 ПП1 ПП2			
РН21																						СП1 СП3 СП8 СП19 СП22 СП26 ПП1 ПП2	СП7 СП8 СП26 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., с.н.с., доц. Ткачов А. М., Завідувач кафедри, д.т.н., професор Євсєєв 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., с.н.с., доц. Ткачов А. М., Завідувач кафедри, д.т.н., професор Євсєєв 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., кандидат 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	Позитивний відгук. Без зауважень.	-	-

наук, доцент, директор ТОВ “Сайфер”			
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 кібербезпеки  Сергій ЄВСЕЄВ

Гарант освітньої програми  Сергій ЄВСЕЄВ

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/Обґрунтування 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

Сергій ЄВСЄВ