

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



ЗАТВЕРДЖУЮ
Ректор НТУ «ХПІ»

Євген СОКОЛ

“29” 04 2024 р.

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
“НАЦІОНАЛЬНА БЕЗПЕКА У СФЕРІ КІБЕРЗАХИСТУ”

першого (бакалаврського) рівня вищої освіти

за спеціальністю 256 – Національна безпека (за окремими сферами забезпечення і видами діяльності)

галузі знань 25 – Воєнні науки, національна безпека, безпека державного кордону

кваліфікація бакалавр з національної безпеки у сфері кіберзахисту

ЗАТВЕРДЖЕНО

Вченою радою НТУ «ХПІ»

Голова вченої ради

Леонід ТОВАЖНЯНСЬКИЙ

Протокол № 4 від «26» квітня 2024 р.

Харків 2024 р.

ЛИСТ ПОГОДЖЕННЯ

Освітньо-професійної програми Національна безпека (за окремими сферами забезпечення і видами діяльності)

Рівень вищої освіти	перший (бакалаврський)
Галузь знань	25 – Воєнні науки, національна безпека, безпека державного кордону
Спеціальність	256 “Національна безпека (за окремими сферами забезпечення і видами діяльності)”
Кваліфікація	бакалавр з національної безпеки у сфері кіберзахисту

ПОГОДЖЕНО

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

Гарант ОПП

 Андрій ТКАЧОВ

« 29 » 01 2024 р.

РЕКОМЕНДОВАНО

Методичною радою НТУ «ХПІ»
Заступник голови методичної ради

 Руслан МИГУЩЕНКО

« 29 » 01 2024 р.

ПОГОДЖЕНО

Завідувач кафедри кібербезпеки

 Сергій ЄВСЕЄВ

« 29 » 01 2024 р.

ПОГОДЖЕНО

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

 Михайло ГОДЛЕВСЬКИЙ

« 29 » 01 2024 р.

ПОГОДЖЕНО

Студент (член робочої групи ОПП)
№ групи КН-1323

 Никита ЖИЛЯЄВ

« 29 » 01 2024 р.

РЕЦЕНЗЕНТИ:

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

1. Микусь Сергій Анатолійович, доктор технічних наук, професор, заступник начальника інституту інформаційно-комунікаційних технологій та кібероборони.
2. Войтко Олександр Володимирович, кандидат військових наук, доцент, начальник навчально-наукового центру стратегічних комунікацій у сфері забезпечення національної безпеки та оборони.
3. Шестаков Валерій Іванович, доктор технічних наук, доцент, лауреат Державної премії України в галузі науки і техніки, заступник директора (з навчальної та наукової роботи) Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій Національної академії Служби безпеки України.
4. Головашич Сергій Олександрович, кандидат технічних наук, доцент директор ТОВ “Мікрокрипт Текнолоджіс”.



МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ОБОРОНИ УКРАЇНИ
ІМЕНІ ІВАНА ЧЕРНЯХОВСЬКОГО

Керівнику Національного технічного
університету “Харківський політехнічний
інститут”

Національний університет оборони України
імені Івана Черняховського
03049, Київ, Повітрофлотський проспект 28.

РЕЦЕНЗІЯ-ВІДГУК

на освітньо-професійну програму “Національна безпека у сфері кіберзахисту” бакалаврського (першого) рівня вищої освіти, яка запропонована кафедрою кібербезпеки Національного технічного університету “Харківський політехнічний інститут”.

Актуальність.

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 256 “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, повністю реалізує результати навчання передбачені стандартом вищої освіти.

Характеристика програми.

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 несподіваними 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-телекомунікаційні 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.

Висновок.

Вважаю, що Освітньо-професійна програма “Національна безпека у сфері кіберзахисту”, що складена та запропонована кафедрою кібербезпеки Національного технічного університету “Харківський політехнічний інститут”, має всі необхідні компоненти для підготовки кваліфікованих фахівців, які будуть впроваджені на ринку праці.

Відгук склав:

Заступник начальника інституту інформаційно-комунікаційних технологій та кібероборони, доктор технічних наук, професор

Сергій МИКУСЬ

14 березня 2024 року

Підпис доктора технічних наук, професора Микуса Сергія Анатолійовича засвідчую:

Начальник адміністративного управління Національного університету оборони України імені Івана Черняховського

Богдан БІЛЯВСЬКИЙ





МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ОБОРОНИ УКРАЇНИ
ІМЕНІ ІВАНА ЧЕРНЯХОВСЬКОГО

Керівнику Національного технічного
університету "Харківський політехнічний
інститут"

Національний університет оборони
України імені Івана Черняховського
03049, Київ, Повітрофлотський проспект 28.

РЕЦЕНЗІЯ-ВІДГУК

на освітньо-професійну програму "Національна безпека у сфері кіберзахисту" бакалаврського (першого) рівня вищої освіти, яка запропонована кафедрою кібербезпеки Національного технічного університету "Харківський політехнічний інститут".

Актуальність.

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 одними з 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 однієї сторони, 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.

Характеристика програми.

Кафедрою кібербезпеки Національного технічного університету "Харківський політехнічний інститут" розроблено навчальну програму "Національна безпека у сфері кіберзахисту" та навчальні плани дисциплін, які пов'язані з напрямом підготовки фахівця з кібербезпеки широкого профілю, яка формує спектр компетентностей та забезпечує отримання результатів навчання, які передбачаються стандартом вищої освіти за спеціальністю 256 "Національна безпека (за окремими сферами забезпечення і видами діяльності)".

Програма забезпечує підготовку фахівця, який здатен забезпечити необхідний рівень кібербезпеки систем різного призначення та природи, в першу чергу системи бізнес-процесів економічних систем, систем критичної інфраструктури, кіберфізичних 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.

Висновок.

Освітньо-професійна програма “Національна безпека у сфері кіберзахисту” першого (бакалаврського) рівня освіти, що складена та 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.

Відгук склав:

Начальник навчально-наукового центру стратегічних комунікацій у сфері забезпечення національної безпеки та оборони, кандидат військових наук, доцент



Олександр ВОЙТКО

___ березня 2024 року

Підпис кандидата військових наук, доцента Войтка Олександра Володимировича засвідчую:

Начальник адміністративного управління Національного університету оборони України імені Івана Черняховського



Богдан БІЛЯВСЬКИЙ

РЕЦЕНЗІЯ-ВІДГУК

на освітньо-професійну програму

“НАЦІОНАЛЬНА БЕЗПЕКА У СФЕРІ КІБЕРЗАХИСТУ”

бакалаврського (першого) рівня вищої освіти, яка запропонована кафедрою

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 кібер атак, стимулювання досліджень і розробок у сфері кібербезпеки з урахуванням появи нових кіберзагроз і викликів. Реалізація плану обумовлює потребу у фахівцях-управлінцях.

Освітня 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.

Вона 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 навичками 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 нададуть можливість працевлаштування в:

органах державної влади, що формують та реалізують державну політику у сфері національної безпеки, на посадах, які визначено у відповідних професійних 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.

Дана програма повністю відповідає сучасним вимогам щодо підготовки фахівців-управлінців у сфері національної безпеки, відповідає запитам потенційних роботодавців (стейкхолдерів), а відтак може бути рекомендована до впровадження в освітній процес.

РЕЦЕНЗЕНТ

Заступник директора (з навчальної та наукової роботи) Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій Національної академії Служби безпеки України, лауреат Державної премії України в галузі науки і техніки, доктор технічних наук, доцент

Валерій ШЕСТАКОВ

«27» 03 2024 року

Підпис Шестакова В. І. засвідчую.
Перший проректор (з навчальної роботи)
Національної академії Служби безпеки України
доктор юридичних наук, старший дослідник

Віталій ГРЕБЕНЮК

«27» 03 2024 року



ЗАТВЕРДЖУЮ:

Генеральний директор

ТОВ «Мікрокрипт Текнолоджіс»

Головашич С.О.

» _____ 2024 р.

РЕЦЕНЗІЯ-ВІДГУК

на освітньо-професійну програму “Національна безпека у сфері кіберзахисту” бакалаврського (першого) рівня вищої освіти, що запропонована кафедрою 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 проєктів, 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 цілком 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 навчальну програму «Національна безпека у сфері кіберзахисту». Навчальні плани та підбір дисциплін спрямовані на підготовку фахівців з кібербезпеки широкого профілю і надання їм теоретичних знань та формування практичних навичок, які передбачаються стандартом вищої освіти за спеціальністю 256 «Національна безпека (за окремими сферами забезпечення і видами діяльності)».

Вважаю, що освітньо-професійна програма «Національна безпека у сфері кіберзахисту», що розроблена та запропонована до впровадження кафедрою Кібербезпеки Національного технічного університету «Харківський політехнічний інститут», включає всі необхідні дисципліни в обсязі достатньому для підготовки кваліфікованих фахівців першого (бакалаврського) рівня освіти, які будуть мати великий попит на ринку праці.

Генеральний директор
ТОВ «Мікрокрипт Текнолоджіс»



Головашич С.О.

ПЕРЕДМОВА

Відповідає галузі знань Воєнні науки, національна безпека, безпека державного кордону, спеціальності Національна безпека (за окремими сферами забезпечення і видами діяльності) відповідно до національної рамки кваліфікації.

Освітньо-професійну програму “Національна безпека у сфері кіберзахисту” розроблено робочою групою зі спеціальності Національна безпека (за окремими сферами забезпечення і видами діяльності) навчально-наукового інституту комп’ютерних наук та інформаційних технологій Національного технічного університету “Харківський політехнічний інститут” у складі:

Гарант освітньо-професійної програми

Ткачов Андрій Михайлович, кандидат технічних наук, старший науковий співробітник, доцент кафедри кібербезпеки.

Члени робочої групи ОПП:

1. Король Ольга Григорівна, кандидат технічних наук, доцент, доцент кафедри кібербезпеки.
2. Мілов Олександр Володимирович, доктор технічних наук, професор, професор кафедри кібербезпеки.
3. Мілевський Станіслав Валерійович, кандидат економічних наук, доцент, доцент кафедри кібербезпеки.
4. Корольов Роман Володимирович, кандидат технічних наук, доцент кафедри кібербезпеки.

**1. ПРОФІЛЬ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ ЗА
СПЕЦІАЛЬНІСТЮ
256 – НАЦІОНАЛЬНА БЕЗПЕКА (ЗА ОКРЕМИМИ СФЕРАМИ ТА
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> <u>кафедра кібербезпеки</u>
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Бакалавр Освітня кваліфікація: бакалавр національної безпеки. Кваліфікація в дипломі: бакалавр національної безпеки
Офіційна назва освітньої програми	Національна безпека у сфері кіберзахисту
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний, 240 кредитів ЄКТС, термін навчання 3 роки 10 місяців
Наявність акредитації	відсутня
Цикл/рівень	Перший (бакалаврський) рівень вищої освіти, НРК – 6 рівень, EQF– 6 рівень, QF-EHEA – перший цикл.
Передумови	Для здобуття освітнього ступеня «бакалавр» можуть вступати особи, які здобули повну загальну середню освіту або освітній ступінь «молодший бакалавр», фаховий «молодший бакалавр», ОКР «молодший спеціаліст».
Мова викладання	Українська, англійська
Термін дії освітньої програми	Оновлюється щорічно
Посилання на постійне розміщення опису освітньої програми	Інтернет-адреса постійного розміщення опису освітньої програми https://cybersecurity.kpi.kharkov.ua
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)	Галузь знань: 25 “Воєнні науки, національна безпека, безпека державного кордону” Спеціальність: 256 “Національна безпека (за окремими сферами та видами діяльності)” Об’єкт вивчення: – теорія та практика національної безпеки (за окремими сферами забезпечення і видами діяльності); об’єкти критичної інфраструктури, інформаційно-комінікаційні системи та мережі; – технології забезпечення кіберзахисту;

	– процеси управління інформаційною та/або кібербезпекою об’єктів критичної інфраструктури. Цілі навчання: підготовка фахівців здатних використовувати і впроваджувати технології кіберзахисту в галузі національної безпеки. Теоретичний зміст предметної області: Знання: – законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; – принципів супроводу систем та комплексів кіберзахисту; – теорії, моделей та принципів управління доступом до інформаційних ресурсів; – теорії систем управління кіберзахистом в галузі національної безпеки; – методів та методик менеджменту кіберзахистом в галузі національної безпеки; – методів та засобів оцінювання та забезпечення необхідного рівня захищеності інформації; – методів та засобів криптографічного захисту інформації; – сучасних інформаційно-комунікаційних технологій; – сучасного програмно-апаратного забезпечення інформаційно-комунікаційних технологій. Методи, методики та технології: Методи, методики, інформаційно-комунікаційні технології та інші технології забезпечення кіберзахисту в галузі національної безпеки. Інструментарій та обладнання: системи розробки, забезпечення, моніторингу та контролю процесів кіберзахисту; – сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій; – спеціалізований клас (кіберполігон).
Орієнтація освітньої програми	Професійна підготовка фахівців у сфері національної безпеки (за окремими сферами та видами діяльності)
Основний фокус освітньої програми та спеціалізації	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 та видами діяльності)” є проходження виробничої практики в органах державної влади тривалістю 4 тижні.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Фахівці з національної безпеки у сфері кіберзахисту можуть працювати, згідно з чинною редакцією Національного класифікатора України: Класифікатор професій (Зміна № 10 до 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 з технічного захисту інформації; 2139.2 Фахівець сфери захисту інформації; 2149.2 Фахівець (сфера захисту інформації); 2419.3 Радник (органи державної влади); 3411 Фахівець з фінансово-економічної безпеки; 3439 Фахівець з режиму секретності; Фахівець із організації захисту інформації з обмеженим доступом; Фахівець із організації інформаційної безпеки.
Подальше навчання	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	Студенто-центричне 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	КЗ–1. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого (безпечного) розвитку, верховенства права, прав і свобод людини і громадянина в Україні. КЗ–2. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній

	системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя. КЗ–3. Здатність до абстрактного мислення, аналізу та синтезу. КЗ–4. Здатність спілкуватися державною мовою як усно, так і письмово. КЗ–5. Здатність спілкуватися іноземною мовою. КЗ–6. Здатність до адаптації та дії в новій ситуації. КЗ–7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. КЗ–8. 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. КЗ–9. Здатність до соціальної взаємодії, співробітництва, розв'язання конфліктів у сфері професійної діяльності, лідерства і командної роботи.
Спеціальні (фахові, предметні) компетентності	ФК–1. Здатність використовувати безпекові режими під час виконання службових обов'язків. ФК–2. 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). ФК–3. 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. ФК–4. Здатність демонструвати та застосовувати знання з основ теорії національної безпеки. ФК–5. Здатність використовувати історичний досвід військових та політичних стратегій іноземних держав з метою вирішення завдань з національної безпеки. ФК–6. Здатність використовувати іноземну мову для отримання додаткових знань і умінь з питань національної безпеки, взаємодіяти з іноземними партнерами. ФК–7. Здатність визначати необхідні правові та організаційні заходи врегулювання конфліктів, пов'язаних із забезпеченням національної безпеки. ФК–8. Здатність використовувати механізми забезпечення національної безпеки у її визначальних сферах. ФК–9. Здатність використовувати знання щодо безпекової складової зовнішньої політики України та інших держав. ФК–10. Здатність засвоювати основні теоретичні поняття та набуття практичних навичок дослідження, підготовки документів та їх використання в управлінській діяльності. ФК–11. Здатність використовувати практичні навички, тактику та прийоми роботи з людьми в інтересах службової діяльності. ФК–12. Здатність виконувати заходи територіальної оборони, а також цивільного захисту у межах професійної компетентності.

	ФК–13. Здатність оцінювати вплив глобальних проблем і трансформацій геополітичного та гео економічного простору на національну безпеку. ФК–14. Здатність здійснювати моніторинг зовнішньої та внутрішньої політики держави у контексті забезпечення національної безпеки, готувати пропозиції щодо підвищення її ефективності.
7 – Програмні результати навчання	
Програмні результати навчання за спеціальністю	ПРН–1. Вміти реалізовувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського суспільства (вільного демократичного) та необхідність його сталого (безпечного) розвитку, верховенства права, прав і свобод людини і громадянина в Україні. ПРН–2. Вміти використовувати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя. ПРН–3. Вміти за допомогою абстрактного мислення, аналізу та синтезу оцінювати результати професійної діяльності та забезпечувати її якість, бути критичним і самокритичним, наполегливим щодо поставлених завдань і взятих зобов'язань. ПРН–4. Вільно спілкуватися державною мовою. ПРН–5. Вільно спілкуватися іноземною мовою у межах потреби своєї професійної діяльності. ПРН–6. Вміти адаптовуватись до нових викликів та дій у певних ситуаціях. ПРН–7. 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. ПРН–8. 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. ПРН–9. Вміти використовувати безпекові режими під час виконання службових обов'язків. ПРН–10. 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). ПРН–11. Вміти пояснювати роль, місце та призначення політичних та безпекових інститутів України для ефективного здійснення заходів при виконання обов'язків з питань забезпечення національної безпеки. ПРН–12. Вміти застосовувати знання з основ теорії національної безпеки, зокрема: оцінювати обстановку, рівень викликів та загроз національній безпеці. ПРН–13. Вміти використовувати історичний досвід військових та

	політичних стратегій іноземних держав з метою вирішення завдань з національної безпеки. ПРН–14. 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. ПРН–15. Вміти визначати необхідні правові та організаційні заходи врегулювання конфліктів, пов'язаних із забезпеченням національної безпеки. ПРН–16. Використовувати у професійній діяльності окремі елементи механізму впливу та взаємодії у процесі забезпечення окремих складових національної безпеки. ПРН–17. Вміти використовувати отримані знання щодо безпекової складової зовнішньої політики України та інших держав. ПРН–18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності. ПРН–19. 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. ПРН–20. Вміти виконувати заходи територіальної оборони, а також цивільного захисту у межах професійної компетентності. ПРН–21. 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	Кадрове 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 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	Матеріально-технічне забезпечення освітньої програми відповідає постанові Кабінету Міністрів України від 30.12.2015 р. № 1187 «Про

забезпечення	затвердження Ліцензійних умов провадження освітньої діяльності закладів освіти» (зі змінами, внесеними згідно з Постановою КМ № 365 від 24.03.2021 Додаток 17). Навчально-науково-виробнича база у вигляді: –навчальні корпуси, комп’ютерні класи, об’єднані локальною обчислювальною мережею з виходом до Інтернету, мультимедійне обладнання;–спеціалізоване програмне забезпечення; –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, робочі програми навчальних дисциплін. Інформаційні ресурси розміщені у фондах наукової бібліотеки НТУ «ХПІ», сайтах випускових кафедр. У навчальному процесі застосовується LMS (Learning Management System).
9 – Академічна мобільність	
Національна кредитна мобільність	На основі двосторонніх договорів про академічну мобільність з університетами України. Меморандуму про співпрацю щодо реалізації програм внутрішньої академічної мобільності здобувачів вищої освіти за освітньою програмою “Кібербезпека” спеціальності 125 з національною академією СБУ.
Міжнародна кредитна мобільність	На основі двосторонніх договорів
Навчання іноземних здобувачів вищої освіти	Після отримання Сертифікату про акредитацію освітньої програми передбачається підготовка іноземців та осіб без громадянства.

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

2.1 Перелік компонент ОПП

Код н/д	Компоненти освітньої програми	Кількість кредитів	Форма підсумкового контролю
1	2	3	4
1. Обов'язкові компоненти ОПП (здобувачі вищої освіти, громадяни України)			
1.1 Загальна підготовка (здобувачі вищої освіти – громадяни України)			
ЗП 1	Історія та культура України	4	Екзамен
ЗП 2	Українська мова (професійного спрямування)	3	Залік
ЗП 3	Іноземна мова	16	Залік, Екзамен
ЗП 4	Основи гуманітарно-філософських знань у професійній діяльності	4	Екзамен
ЗП 5	Вища математика	12	Залік, Екзамен
ЗП	Фізичне виховання	8	Залік
1.2 Спеціальна (фахова) підготовка			
СП 1	Вступ до спеціальності. Ознайомча практика	3	Залік
СП 2	Основи програмування	4	Екзамен
СП 3	Національна безпека держави	6	Екзамен
СП 4	Теорія інформації і кодування	3	Екзамен
СП 5	Фізичні основи технічних засобів розвідки	5	Екзамен
СП 6	Алгоритми та структури даних	5	Екзамен
СП 7	Правове регулювання кібербезпеки	4	Залік
СП 8	Менеджмент інформаційної безпеки	3	Екзамен
СП 9	Математичні основи криптології	4	Екзамен
СП10	Технології програмування	5	Екзамен
СП 11	Основи соціальної інженерії	4	Залік
СП 12	Комп'ютерні мережі	5	Екзамен
СП 13	Інструментальні засоби програмування	6	Екзамен
СП 14	Основи криптографічного захисту	5	Залік
СП 15	Цифрова криміналістика	5	Залік
СП 16	Основи стеганографічного захисту інформації	4	Залік
СП 17	Організація документообігу з обмеженим доступом	5	Залік
СП 18	Безпека смарт-технологій	4	Екзамен
СП 19	Безпека в інформаційно-комунікаційних системах	4	Залік
СП 20	Розробка веб-додатків	6	Екзамен

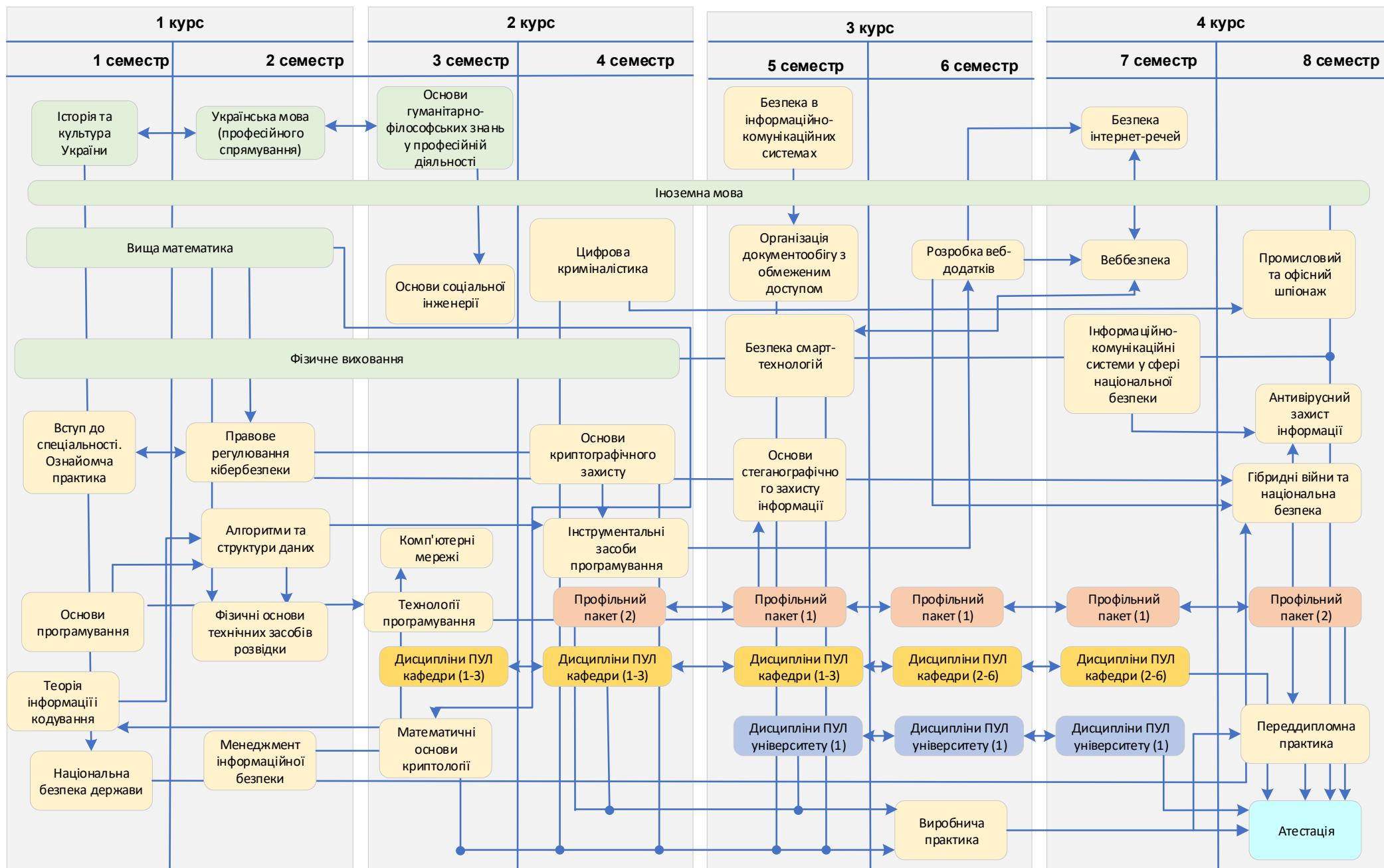
СП 21	Веббезпека	5	Залік
СП 22	Інформаційно-комунікаційні системи у сфері національної безпеки	4	Залік
СП 23	Безпека інтернет-речей	4	Залік
СП 24	Антивірусний захист інформації	5	Залік
СП 25	Промисловий та офісний шпiонаж	4	Екзамен
СП 26	Гiбриднi вiйни та нацiональна безпека	4	Залік
2. Практична пiдготовка			
ПП1	Виробнича практика*	6	Залік
ПП2	Переддипломна практика	6	Залік
3. Атестацiя			
	Атестацiя*	3	
Загальний обсяг обов'язкових компонент		178	
4. Вибірковi компоненти ОПП (здобувачi вищої освiти, як громадяни України, так i iноземцi)			
Профiльований пакет дисциплiн 01 "Штучний iнтелект в системах захисту"			
ВП1.1	Етичний хакiнг	3	Екзамен
ВП1.2	Дата майнинг	3	Екзамен
ВП1.3	Математичнi основи штучного iнтелекту	3	Екзамен
ВП1.4	Python для штучного iнтелекту та машинного навчання	4	Екзамен
ВП1.5	Генетичнi алгоритми	3	Екзамен
ВП1.6	Python для iнтернет-речей	3	Екзамен
ВП1.7	Системний iнжинiринг	3	Екзамен
Профiльований пакет дисциплiн 02 "Блокчейн-технологiя та безпека банкiвських систем"			
ВП2.1	Децентралiзованi системи	3	Екзамен
ВП2.2	Ризик-менеджмент	3	Екзамен
ВП2.3	Blockchain: основи та приклади застосування	3	Екзамен
ВП2.4	Безпека банкiвських систем	4	Екзамен
ВП2.5	Захист об'єктiв критичної iнфраструктури	3	Екзамен
ВП2.6	Органiзацiя документообiгу з обмеженням доступом	3	Екзамен
ВП2.7	Безпека в соцiальних мережах	3	Екзамен
Профiльований пакет дисциплiн 03 "Innovation Campus"			
ВП3.1	Основи кiбербезпеки	3	Екзамен
ВП3.2	Розробка корпоративних iнформацiйних систем (частина 1)	3	Екзамен
ВП3.3	Розробка корпоративних iнформацiйних систем (частина 2)	3	Екзамен
ВП3.4	Бази даних для корпоративних iнформацiйних систем	4	Екзамен
ВП3.5	Архiтектура корпоративних iнформацiйних систем	3	Екзамен
ВП3.6	Безпека та аудит бездротових та рухомих мереж	3	Екзамен

ВПЗ.7	Захист об'єктів критичної інфраструктури	3	Екзамен
Дисципліни вільного вибору студента профільної підготовки згідно переліку			
ОКВП1	ОК ВВ ПП 1	4	Залік
ОКВП2	ОК ВВ ПП 2	4	Залік
ОКВП3	ОК ВВ ПП 3	4	Залік
ОКВП4	ОК ВВ ПП 4	4	Залік
ОКВП5	ОК ВВ ПП 5	4	Залік
ОКВП6	ОК ВВ ПП 6	4	Залік
ОКВП7	ОК ВВ ПП 7	4	Залік
Дисципліни вільного вибору студента із загальноуніверситетського каталогу дисциплін			
ОКВ1	ОК ВВ ЗП 1	4	Залік
ОКВ2	ОК ВВ ЗП 2	4	Залік
ОКВ3	ОК ВВ ЗП 3	4	Залік
Загальний обсяг вибіркового компонента:		62	
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ:		240	

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

№ п/п	Цикл підготовки	Обсяг навчального навантаження здобувача вищої освіти (кредитів ECTS / %)		
		Обов'язкові компоненти освітньо-професійної програми	Вибіркові компоненти освітньо-професійної програми	Всього за весь термін навчання
1	Загальна підготовка	47 / 19,6	—	47 / 19,6
2	Спеціальна (фахова) підготовка	131 / 54,6	—	131 / 54,6
3	Дисципліни вільного вибору	—	62 / 25,8	62 / 25,8
Всього за весь термін навчання		178 / 74,2	62 / 25,8	240 / 100

5. СТРУКТУРНО-ЛОГІЧНА СХЕМА



Семестр	Зміст навчальної діяльності
1	ЗП 1, ЗП 3, ЗП 5, ЗП, СП 1, СП 2, СП 3, СП 4
2	ЗП 2, ЗП 3, ЗП 5, ЗП, СП 5, СП 6, СП 7, СП 8
3	ЗП 3, ЗП 4, ЗП, СП 9, СП 10, СП 11, СП 12
4	ЗП 3, ЗП, СП 13, СП 14, СП 15
5	ЗП 3, СП 16, СП 17, СП 18, СП 19
6	ЗП 3, СП 20, ПП 1
7	ЗП 3, СП 21, СП 22, СП 23
8	ЗП 3, СП 24, СП 25, СП 26, ПП 2, СП

6. ФОРМА АТЕСТАЦІЇ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

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

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

Класифікація компетентностей за НРК	Знання	Уміння	Комунікація	Автономія та відповідальність
ЗАГАЛЬНІ КОМПЕТЕНТНОСТІ				
КЗ–1. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого (безпечного) розвитку, верховенства права, прав і свобод людини і громадянина в Україні	+		+	
КЗ–2. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.	+	+	+	
КЗ–3. Здатність до абстрактного мислення, аналізу та синтезу.		+	+	
КЗ–4. Здатність спілкуватися державною мовою як усно, так і письмово.	+	+	+	
КЗ–5. Здатність спілкуватися іноземною мовою.	+	+	+	
КЗ–6. Здатність до адаптації та дії в новій ситуації.			+	+
КЗ–7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.		+		+
КЗ–8. 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.	+	+		+
КЗ–9. Здатність до соціальної взаємодії, співробітництва, розв'язання конфліктів у сфері професійної діяльності, лідерства і командної роботи.		+		+
СПЕЦІАЛЬНІ (ФАХОВІ, ПРЕДМЕТНІ) КОМПЕТЕНТНОСТІ				
ФК–1. Здатність використовувати безпекові режими під час виконання службових обов'язків.	+	+	+	+
ФК–2. 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).				
ФК–3. 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.		+		+
ФК–4. Здатність демонструвати та застосовувати знання з основ теорії національної безпеки.	+	+		
ФК–5. Здатність використовувати історичний досвід військових та політичних стратегій іноземних держав з метою вирішення завдань з національної безпеки.	+	+		
ФК–6. Здатність використовувати іноземну мову для отримання додаткових знань і умінь з питань національної безпеки, взаємодіяти з іноземними партнерами.	+	+	+	+
ФК–7. Здатність визначати необхідні правові та організаційні заходи врегулювання конфліктів, пов’язаних із забезпеченням національної безпеки.	+	+		+
ФК–8. Здатність використовувати механізми забезпечення національної безпеки у її визначальних сферах.	+	+		+
ФК–9. Здатність використовувати знання щодо безпекової складової зовнішньої політики України та інших держав.	+	+		+
ФК–10. Здатність засвоювати основні теоретичні поняття та набуття практичних навичок дослідження, підготовки документів та їх використання в управлінській діяльності.	+	+		+
ФК–11. Здатність використовувати практичні навички, тактику та прийоми роботи з людьми в інтересах службової діяльності.	+	+	+	+
ФК–12. Здатність виконувати заходи територіальної оборони, а також цивільного захисту у межах професійної компетентності.	+	+		+
ФК–13. Здатність оцінювати вплив глобальних проблем і трансформацій геополітичного та гео економічного простору на національну безпеку.		+		+
ФК–14. Здатність здійснювати моніторинг зовнішньої та внутрішньої політики держави у контексті забезпечення національної безпеки, готувати пропозиції щодо підвищення її ефективності.		+		+

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

[illegible]

				СП																			
ПРН5					ЗП5, ПП1, ПП2 СП	ЗП, СП1, СП17, СП19, СП26, ПП1, ПП2 СП			ЗП2, ЗП3, ЗП, СП1, СП13, ПП2 СП					СП3, СП12, СП23, СП24, ПП1, ПП2 СП									
ПРН6						ЗП, СП1, СП17, СП19, СП26, ПП1, ПП2 СП																	
ПРН7			ЗП4, ЗП5, СП1, СП2, СП4, СП5, СП6, СП7, СП8, СП9, СП10, СП11, СП12, СП13, СП15, СП16, СП20, СП21, СП23, СП25, ПП2 СП			ЗП4, ЗП5, СП1, СП2, СП3, СП4, СП5, СП7, СП8, СП10, СП11, СП12, СП13, СП14, СП15, СП16, СП17, СП19, СП20, СП21, СП22, СП23, СП24, ПП1, ПП2 СП	ЗП5, СП1, СП2, СП3, СП4, СП5, СП7, СП8, СП13, СП14, СП15, СП16, СП17, СП18, СП21, СП22, СП24, СП25, ПП1, ПП2 СП			СП1, СП3, СП4, СП12, СП13, СП14, СП15, СП16, СП18, СП22, СП23, СП25, ПП2 СП	СП1, СП3, СП4, ПП2 СП	СП4, СП9, СП14, СП22, СП24, ПП1, ПП2 СП	СП1, СП12, СП23, ПП2 СП		СП12, СП23, ПП1, ПП2 СП		СП1, СП3, СП4, СП12, СП18, СП23, ПП1, ПП2 СП	СП2, СП5, СП6, СП7, СП8, СП11, СП12, СП18, СП19, СП23, СП25, ПП1, ПП2 СП	СП10, СП12, СП13, СП15, СП18, СП20, СП23, СП26, ПП1, ПП2 СП	СП12, СП23, ПП1, ПП2 СП	СП1, СП3, СП11, СП12, СП23, СП24, СП26, ПП1, ПП2 СП	СП12, СП23, ПП1, ПП2 СП	
ПРН8							ЗП5, СП1, СП2, СП3, СП4, СП5, СП7, СП8, СП13, СП14, СП15, СП16, СП17, СП18, СП21, СП22, СП24,			СП1, СП3, СП4, СП12, СП13, СП14, СП15, СП16, СП18, СП22, СП23, СП25, ПП2 СП					СП4, СП10, СП11, СП12, СП13, СП14, СП15, СП19, СП22, СП23, СП24, СП25, ПП1, ПП2 СП	СП1, СП3, СП4, СП12, СП18, СП23, ПП1, ПП2 СП	СП2, СП5, СП6, СП7, СП8, СП11, СП12, СП18, СП19, СП23, СП25, ПП1, ПП2 СП		СП12, СП23, ПП1, ПП2 СП	СП1, СП3, СП11, СП12, СП23, СП24, СП26, ПП1, ПП2 СП			

								СП25, ПП1, ПП2 СП																
ПРН9						ЗП, СП1, СП17, СП19, СП26, ПП1, ПП2 СП				СП1, СП10, СП14, СП17, СП18, СП21, СП22, СП24, ПП2 СП														
ПРН10						ЗП4, ЗП5, СП1, СП2, СП3, СП4, СП5, СП7, СП8, СП10, СП11, СП12, СП13, СП14, СП15, СП16, СП17, СП19, СП20, СП21, СП22, СП23, СП24, ПП1, ПП2 СП				СП1, СП3, СП4, СП12, СП13, СП14, СП15, СП16, СП18, СП22, СП23, СП25, ПП2 СП														
ПРН11											СП1, СП3, СП4, ПП2 СП													
ПРН12											СП4, СП9, СП14, СП22, СП24, ПП1, ПП2 СП					СП4, СП10, СП11, СП12, СП13, СП14, СП15, СП19, СП22, СП23, СП24, СП25, ПП1, ПП2 СП	СП1, СП3, СП4, СП12, СП18, СП23, ПП1, ПП2 СП			СП12, СП23, ПП1, ПП2 СП	СП1, СП3, СП11, СП12, СП23, СП24, СП26, ПП1, ПП2 СП			

ПРН13														СП1, СП12, СП23, ПП2 СП												
ПРН14														СП3, СП12, СП23, СП24, ПП1, ПП2 СП												
ПРН15															СП12, СП23, ПП1, ПП2 СП											
ПРН16																СП4, СП10, СП11, СП12, СП13, СП14, СП15, СП19, СП22, СП23, СП24, СП25, ПП1, ПП2 СП	СП1, СП3, СП4, СП12, СП18, СП23, ПП1, ПП2 СП									
ПРН17														СП1, СП12, СП23, ПП2 СП	СП3, СП12, СП23, СП24, ПП1, ПП2 СП	СП12, СП23, ПП1, ПП2 СП	СП4, СП10, СП11, СП12, СП13, СП14, СП15, СП19, СП22, СП23, СП24, СП25, ПП1, ПП2 СП	СП1, СП3, СП4, СП12, СП18, СП23, ПП1, ПП2 СП								
ПРН18																		СП2, СП5, СП6, СП7, СП8, СП11, СП12, СП18, СП19, СП23, СП25, ПП1, ПП2 СП	СП10, СП12, СП13, СП15, СП18, СП20, СП23, СП26, ПП1, ПП2 СП	СП12, СП23, ПП1, ПП2 СП						

ПРН19									ЗП2, ЗП3, ЗП, СП1, СП13, ПП2 СП	СП1, СП10, СП14, СП17, СП18, СП21, СП22, СП24, ПП2 СП										СП10, СП12, СП13, СП15, СП18, СП20, СП23, СП26, ПП1, ПП2 СП			
ПРН20																				СП12, СП23, ПП1, ПП2 СП			
ПРН21																					СП1, СП3, СП11, СП12, СП23, СП24, СП26, ПП1, ПП2 СП	СП12, СП23, ПП1, ПП2 СП	