

НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ**ПРОЄКТ
ЗАТВЕРДЖЕНО**

Рішення Вченої ради Національної академії
СБ України від __. __.20__ р., протокол № ____
Ректор Національної академії СБ України

(науковий ступінь, вчене звання)

(військове звання, підпис, ініціали, прізвище)

« ____ » _____ 20__ року

**ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
«КІБЕРЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ»
ПЕРШОГО (БАКАЛАВРСЬКОГО) РІВНЯ ВИЩОЇ ОСВІТИ**

за спеціальністю	256 Національна безпека (за окремими сферами забезпечення і видами діяльності)
спеціалізацією	256.05 Національна безпека (забезпечення національної безпеки в інформаційній сфері та кіберпросторі)
галузі знань	25 Военні науки, національна безпека, безпека державного кордону
кваліфікація	бакалавр національної безпеки (забезпечення національної безпеки в інформаційній сфері та кіберпросторі); фахівець із організації інформаційної безпеки

Київ 2023 р.

Керівник проєктної групи

Олена КОБУС

ЗМІСТ

Передмова

- I. Профіль освітньої програми «Кіберзахист інформаційних ресурсів»
- II. Перелік компонентів освітньо-професійної програми та їх логічна послідовність
 - 2.1. Загальна характеристика освітньо-професійної програми
 - 2.2. Перелік компонентів освітньо-професійної програми
 - 2.3. Структурно-логічна схема освітньо-професійної програми
- III. Форма атестації здобувачів вищої освіти
- IV. Перелік компетентностей, визначених освітньо-професійною програмою (програмні компетентності), та їх відповідність дескрипторам шостого кваліфікаційного рівня Національної рамки кваліфікацій
- V. Матриця відповідності визначених освітньою програмою результатів навчання (програмні результати) та програмних компетентностей
- VI. Матриця забезпечення програмних результатів навчання відповідними компонентами освітньої програми
- VII. Матриця відповідності програмних компетентностей компонентам освітньої програми
- VIII. Система забезпечення якості вищої освіти за освітньо-професійною програмою, що передбачає здійснення процедур внутрішнього та зовнішнього забезпечення якості
- VIII. Вимоги професійних стандартів
 - X. Перелік нормативних, розпорядчих, інструктивних документів, на яких базується освітньо-професійна програма

I. Профіль освітньої програми «Кіберзахист інформаційних ресурсів» першого (бакалаврського) рівня вищої освіти за спеціальністю 256.05 Національна безпека (за окремими сферами забезпечення і видами діяльності) спеціалізацією 256.04 Національна безпека (кіберзахист, забезпечення державної безпеки в інформаційній сфері)

1 – Загальна інформація	
Повна назва вищого навчального закладу та структурного підрозділу	м. Київ, Національна академія Служби безпеки України Навчально-науковий інститут інформаційної безпеки та стратегічних комунікацій
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Бакалавр національної безпеки (забезпечення національної безпеки в інформаційній сфері та кіберпросторі), фахівець із організації інформаційної безпеки
Офіційна назва освітньої програми	Кіберзахист інформаційних ресурсів
Тип диплому та обсяг освітньої програми	Диплом бакалавра, одиничний ступінь, 240 кредитів ЄКТС; термін навчання 4 роки (денна форма навчання)
Наявність акредитації	Акредитується вперше
Цикл/рівень	НРК України – 7, FQ-EHEA – перший цикл, EQF LLL – 6 рівень.
Передумови	Наявність повної загальної середньої освіти або освітньо-кваліфікаційного рівня молодшого спеціаліста (освітнього ступеня молодшого бакалавра).
Мова(и) викладання	Українська
Термін дії освітньої програми	4 роки; оновлення освітньої програми (за потреби) на підставі змін законодавства у сфері освіти, пропозицій стейкхолдерів, здобувачів вищої освіти, інших учасників освітнього процесу. Перегляд освітньої програми здійснюється щорічно відповідно до планових позицій НА СБ України
Кваліфікація в дипломі	Ступінь вищої освіти – Бакалавр Галузь знань – 25 Воєнні науки, національна безпека, безпека державного кордону. Спеціальність – 256 Національна безпека (за окремими сферами забезпечення і видами діяльності); 256.04 Національна безпека (кіберзахист, забезпечення державної безпеки в інформаційній сфері). Професійна кваліфікація – фахівець із організації інформаційної безпеки.
Форми здобуття освіти	Очна
Інтернет-адреса постійного розміщення опису освітньої програми	https://academy.ssu.gov.ua/ (відповідно до умов і порядку, що визначаються нормативно-правовими актами Служби безпеки України).
2 – Мета освітньої програми	
Забезпечити підготовку висококваліфікованих фахівців у галузі національної безпеки зі спеціальності 256.04 «Національна безпека (забезпечення національної безпеки в інформаційній сфері та кіберпросторі)», здатних вирішувати складні спеціалізовані задачі та практичні проблеми організаційно-технічного забезпечення інформаційної безпеки та кібербезпеки, захищеності інформаційного і кіберпросторів держави в цілому або окремих суб'єктів їх інфраструктури від ризику стороннього інформаційного або кібернетичного впливу на основі застосування аналітичних процесів в управлінні інформаційною безпекою та	

кібербезпекою.	
3. – Характеристика освітньої програми	
Предметна область (галузь знань, спеціальність, спеціалізація)	<p>Галузь знань – 25 Воєнні науки, національна безпека, безпека державного кордону.</p> <p>Спеціальність 256 Національна безпека (за окремими сферами забезпечення і видами діяльності)</p> <p>Спеціалізація 256.04 Національна безпека (кіберзахист, забезпечення державної безпеки в інформаційній сфері)</p> <p>Додаткове професійне спрямування: <u>Об'єкт вивчення та/або діяльності:</u> процеси, явища та проблеми організаційно-технічного забезпечення національної безпеки в інформаційній сфері та кіберпросторі; <u>Цілі навчання:</u> підготовка фахівців з сучасним системним мисленням, теоретичними знаннями і практичними навичками, необхідними для вирішення складних завдань та практичних проблем у забезпеченні національної безпеки в інформаційній сфері та кіберпросторі. Особлива увага приділяється інформаційній безпеці, кібербезпеці, безпеці інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури; <u>Теоретичний зміст предметної області:</u> поняття, категорії, концепції, принципи, методи та засоби забезпечення національної безпеки в інформаційній сфері та кіберпросторі; <u>Методи, методика та технології:</u> сучасні цифрові технології, методи збирання, аналізу та захисту інформації, методи і технології забезпечення національної безпеки (кіберзахист, забезпечення державної безпеки в інформаційній сфері); <u>Інструменти та обладнання:</u> сучасне інформаційно-комунікаційне забезпечення та спеціалізоване програмне забезпечення, електронні бази даних; інтернетресурси; інструменти забезпечення національної безпеки (кіберзахист, забезпечення державної безпеки в інформаційній сфері)що застосовуються в професійній діяльності.</p>
Орієнтація освітньої програми	<p>Освітньо-професійна програма має прикладну орієнтацію з професійними акцентами:</p> <p>забезпеченні національних інтересів людини, суспільства і держави в інформаційній сфері;</p> <p>забезпеченні безпеки інформаційного простору методами інформаційного протиборства, інформаційно-комунікаційної інфраструктури та інформаційних ресурсів підприємств, установ та організацій, усіх форм власності від загроз конфіденційності, цілісності, доступності інформації.</p>
Основний фокус освітньої програми та спеціалізації	<p>Акцент на здатності організувати й підтримувати комплекс заходів щодо забезпечення інформаційної та кібербезпеки з урахуванням їхньої адміністративно-управлінської й технічної реалізації, можливих зовнішніх впливів, імовірних загроз і рівня розвитку технологій захисту інформації.</p>
Особливості програми	<p>Інтегрована підготовка фахівців до вирішення завдань у сфері інформаційної та кібербезпеки, що передбачає:</p> <p>мультидисциплінарний підхід, що поєднує знання з різних галузей кіберзахисту;</p> <p>практична спрямованість з акцентом на вирішення реальних завдань та проблем кібербезпеки;</p> <p>використання сучасних технологій, інструментів та програмного</p>

	<p>забезпечення; актуальна інформація про нові загрози та стратегії захисту; вивчення етичних аспектів кіберзахисту та усвідомлення важливості дотримання етичних норм; сприяння розвитку креативного мислення та інноваційних підходів до кіберзахисту; підготовка кваліфікованих фахівців, готових працювати в сфері кіберзахисту та вирішувати складні завдання безпеки інформаційних ресурсів.</p>
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	<p>Фахівець підготовлений до діяльності відповідно до Міжнародної стандартної класифікації (ЮНЕСКО) за кодами: 103 Служби безпеки, спеціалізації 1031 Військова справа та оборона і 1032 Охорона громадян та власності та до діяльності в галузі економіки за кодами (назвами) ДК-009 2010:</p> <ul style="list-style-type: none"> – 62.09 (діяльність у сфері інформаційних технологій і комп'ютерних систем); – 80.2 (обслуговування систем безпеки); – 84.24 (діяльність у сфері охорони громадського порядку та безпеки), та здатний виконувати професійну роботу і може призначатися на посади: <ul style="list-style-type: none"> – начальник відділу (в складі управління) підвідділу, сектору (в складі самостійного відділу) з інформаційної безпеки та начальник відділу (в складі управління) підвідділу, сектору (в складі самостійного відділу) з організації інформаційної безпеки код 1239, який класифікується як «Керівники інших функціональних підрозділів»; – фахівець з організації інформаційної безпеки код 3439, який класифікується, як «Фахівець організації інформаційної безпеки»; – інспектор з організації інформаційної безпеки код 3449, який класифікується, як «Інспектор з інформаційної безпеки»; – аналітик у сфері інформаційної безпеки код 2412.2, який класифікується, як «Аналітик у сфері інформаційної безпеки»; – менеджер (управитель) систем з інформаційної безпеки код 1495 який класифікується, як «Менеджер (управитель) систем з інформаційної безпеки».
Подальше навчання	<p>Можливість продовжити навчання на другому (магістерському) рівні вищої освіти. НРК України – 8, FQ-EHEA – 2 цикл, EQF LLL – 7 рівень.</p>
5 – Викладання та оцінювання	
Викладання та навчання	<p>Студентоцентроване, проблемно-орієнтоване навчання, ініціативне самонавчання. Лекційні заняття різних форм, які орієнтовані на покращення активності та ефективного засвоєння матеріалу (інтерактивні, віртуальні, Flip-лекції, гостьові, проєктні).</p>

	<p>Семінарські та практичні – проводяться в групах та підгрупах, де практикуються ситуаційні завдання, тренінги, групові дискусії, ділові ігри, кейс-студії, презентації-доповіді, командні проекти, симуляційні вправи, віртуальні практикуми, Capture the Flag (CTF) змагання також використовуються сучасні професійні програмні засоби, проводяться індивідуальні заняття, консультації з викладачами, проходження практик, підготовка кваліфікаційної роботи бакалавра (проєкту).</p> <p>Організація освітнього процесу ґрунтується на загальнопедагогічних принципах (системність, науковість, систематичність, послідовність, наочність, інтеграція теорії та практики, свідомість й активність, індивідуальний підхід, самостійність й активність суб'єктів навчання, міжпредметні зв'язки, позитивний емоційний фон навчання, забезпечення єдності освітніх, розвивальних і виховних функцій); спеціальних (контекстного навчання, комунікативної взаємодії, індивідуальної підтримки науково-педагогічним співробітником (працівником) навчальної діяльності здобувача вищої освіти, внутрішньої свободи особистості, позиційності, критичного самооцінювання).</p>
Оцінювання	<p>Накопичувальна модульно-рейтингова система, що передбачає оцінювання студентів за усіма видами аудиторної та позааудиторної (самостійної, індивідуальної) навчальної діяльності, спрямовані на опанування навчального матеріалу з освітньої програми: поточний контроль, модульний, підсумковий контроль, письмові та усні екзамени, тестування, реферати, презентації, проходження навчальних та виробничих практик, написання курсових робіт, підготовка та захист магістерської роботи. Рівень досягнутих результатів навчання вимірюється у трьох системах оцінювання: рейтингова шкала або 100-бальна, національна та шкала ЄКТС. Критерії та методи оцінювання розробляються кафедрами й визначаються в програмах навчальних дисциплін, практичної підготовки та атестації.</p>
6 – Програмні компетентності	
Інтегральна компетентність	<p>ІК01. Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі організаційно-технічного забезпечення національної безпеки в інформаційній сфері та кіберпросторі або у процесі навчання, що передбачає застосування певних теорій та методів забезпечення національної безпеки в інформаційній сфері та кіберпросторі і характеризуються комплексністю та невизначеністю умов.</p>
Загальні компетентності (ЗК)	<p>ЗК01. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.</p> <p>ЗК02. 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</p>

	<p>активного відпочинку та ведення здорового способу життя.</p> <p>ЗК03. Здатність до абстрактного мислення, пошуку, оброблення, аналізу та синтезу інформації.</p> <p>ЗК04. Здатність спілкуватися державною мовою як усно, так і письмово.</p> <p>ЗК05. Здатність спілкуватися іноземною мовою у сфері професійного спрямування.</p> <p>ЗК06. Здатність до адаптації та дії в новій ситуації, застосування знань державної та іноземних мов, інформаційно - комунікаційних технологій, комп'ютерної техніки для забезпечення професійної комунікації.</p> <p>ЗК07. Здатність до пошуку, оброблення, аналізу та застосовування інформації у практичних ситуаціях, постійно самовдосконалюватися, здобувати нові фахові знання з використанням різних джерел інформації.</p> <p>ЗК08. Здатність здійснювати професійну діяльність на основі здорового способу життя, знань сучасних інформаційно-комунікаційних технологій.</p> <p>ЗК09. Здатність до соціальної взаємодії, співробітництва, розв'язання конфліктів у сфері професійної діяльності, лідерства і командної роботи.</p> <p>ЗК10. Знання та розуміння предметної області та розуміння професії.</p> <p>ЗК11. Здатність використовувати інформаційні та комунікаційні технології і на цій основі формувати ефективну систему інформаційного забезпечення підтримки прийняття управлінських рішень щодо запобігання, протидії та нейтралізації загроз національній безпеці.</p> <p>ЗК12. Знання фундаментальних розділів математики в обсязі, необхідному для оволодіння методичним апаратом відповідної спеціалізації, здатність використовувати математичні та статистичні методи в професійній діяльності.</p> <p>ЗК13. Знання фундаментальних понять інформаційного протистояння як компонент гібридної війни, каналів, механізмів протидії інформаційним викликам гібридних воєн.</p>
<p>Фахові компетентності (ФК)</p>	<p>ФК01. Здатність критично та на межі предметних галузей осмислювати понятійно-категоріальний апарат загальної теорії національної безпеки, структури, об'єктів, суб'єктів та принципів забезпечення національної безпеки.</p> <p>ФК02. Здатність аналізувати виклики та загрози національній безпеці за напрямками професійної діяльності, синтезувати інформацію щодо розроблення та реалізації елементів стратегій у визначальних сферах національної безпеки.</p> <p>ФК03. Здатність до формування механізмів захищеності від руйнівних інформаційно-психологічних впливів та деструктивної пропаганди, до розвитку інформаційного суспільства, його технологічної інфраструктури.</p> <p>ФК04. Здатність здійснювати моніторинг загроз національним інтересам і національній безпеці в інформаційній сфері.</p> <p>ФК05. Здатність побудувати ефективну систему інформаційно-аналітичного забезпечення для підтримки процесів прий-</p>

	<p>няття рішень щодо запобігання, протидії та нейтралізації загроз державній безпеці в інформаційній сфері.</p> <p>ФК06. Здатність використовувати іноземну мову для отримання додаткових знань і умінь з питань національної безпеки, взаємодіяти з іноземними партнерами.</p> <p>ФК07. Здатність визначати необхідні правові та організаційні заходи врегулювання конфліктів, пов'язаних із забезпеченням національної безпеки.</p> <p>ФК08. Здатність аналізувати та прогнозувати різноманітні складові критичних ситуацій на об'єктах інформаційної діяльності.</p> <p>ФК09. Здатність забезпечувати захист різних видів інформації, формулювати, аналізувати та синтезувати вирішення проблем з організації та захисту інформації на підприємстві в установі, організації використовуючи вітчизняний та зарубіжний досвід.</p> <p>ФК10. Здатність засвоювати основні теоретичні поняття та набуття практичних навичок дослідження, підготовки документів та їх використання в управлінській діяльності.</p> <p>ФК11. Здатність використовувати практичні навички, тактику та прийоми роботи з людьми в інтересах службової діяльності.</p> <p>ФК12. Здатність професійно і чітко організувати роботу аналогічного підрозділу недержавної установи в інтересах забезпечення конфіденційності, цілісності, доступності інформації.</p> <p>ФК13. Здатність застосування методів теорії систем і системного аналізу при моделюванні, побудові та дослідженні складних інформаційно-комунікаційних систем та мереж.</p> <p>ФК14. Розуміння актуальних проблем комплексного захисту інформації з обмеженим доступом та здатність до їх розв'язання з використанням організаційних та аналітичних методів, сучасних інформаційно-технічних, криптографічних засобів і технологій, здатність організувати комплексну систему захисту інформації.</p> <p>ФК15. Здатність обґрунтовувати методи та засоби захисту від відповідних загроз, в тому числі загроз інформаційної безпеки та кіберзагроз, об'єктів критичної інформаційної інфраструктури та кіберінфраструктури.</p> <p>ФК16. Здатність визначати основні властивості інформації, інформаційних ресурсів та технологій, як об'єктів інформаційної безпеки.</p> <p>ФК17. Здатність визначати основні положення методів та заходів забезпечення інформаційної безпеки та кібербезпеки держави у різноманітних сферах життєдіяльності.</p> <p>ФК18. Здатність застосовувати методи розслідування і аналізу для збору, використання і збереження доказів протиправної діяльності в інформаційній сфері та кіберпросторі.</p> <p>ФК19. Здатність обґрунтовувати та здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.</p> <p>ФК20. Здатність обґрунтовувати застосування методів та засобів криптографічного та технічного захисту інформації на</p>
--	---

	<p>об'єктах інформаційної інфраструктури та кіберінфраструктури.</p> <p>ФК21. Здатність обґрунтовувати застосування методів та засобів забезпечення безпеки в глобальній мережі стосовно послуг мережі та відповідних систем інформаційно-комунікаційних технологій і мереж.</p> <p>ФК22. Здатність обґрунтовувати застосування методів та засобів забезпечення безпеки та захисту комп'ютерних мереж, пов'язаних з проектуванням, впровадженням і використанням мереж всередині організації, між організаціями, між організаціями і користувачами.</p> <p>ФК23. Здатність обґрунтовувати застосування методів та засобів захисту програмних засобів, а також інформаційно-програмних ресурсів і процесів, що беруть участь в життєвому циклі застосунків.</p> <p>ФК24. Здатність обґрунтовувати, впроваджувати та забезпечувати функціонування систем кіберзахисту інформаційних ресурсів організації.</p> <p>ФК25. Здатність розуміти та вирішувати проблеми захисту безпеки України з урахуванням змін обстановки в державі.</p>
7 – Програмні результати навчання	
ПРН, визначені закладом вищої освіти	<p>ПРН01. Вміти реалізовувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського суспільства (вільного, демократичного), необхідність його сталого (безпечного) розвитку, верховенства права, прав і свобод людини і громадянина в Україні, організувати свою професійну діяльність з дотриманням прав і свобод людини і громадянина, поваги до гідності особи, захисту її інтересів, а також законних інтересів суспільства та держави, забезпечення її суверенітету і територіальної цілісності.</p> <p>ПРН02. Застосовувати культурні, духовні, моральні цінності Українського народу, історико-культурну спадщину з метою формування позитивного іміджу держави в умовах інформаційної глобалізації, розвитку власної інформаційної культури та здорового способу життя.</p> <p>ПРН03. Застосовувати результати алгоритмічного та абстрактного мислення, самостійного пошуку, аналізу та синтезу, методів теорії інформації, теорії систем та системного аналізу для ефективного вирішення завдань професійної діяльності, бути критичним і самокритичним, наполегливим щодо поставлених завдань і взятих зобов'язань.</p> <p>ПРН04. Вільно володіти державною мовою як усно, так і письмово.</p> <p>ПРН05. Вільно володіти іноземною мовою у межах потреби своєї професійної діяльності.</p> <p>ПРН06. Адаптуватись до нових викликів та дій у певних ситуаціях, застосовувати знання державної та іноземних мов, інформаційно - комунікаційних технологій, комп'ютерної техніки для забезпечення професійної комунікації.</p> <p>ПРН07. Використання знань з основних методів наукового пошуку; вміння узагальнювати отримані результати, обробки та аналізу інформації з різних джерел, оформлення та презентації.</p>

	<p>тування результатів наукової діяльності, здатності використовувати статистичні методи в професійній діяльності.</p> <p>ПРН08. Вміти використовувати інформаційні та комунікаційні технології і на цій основі формувати ефективну систему інформаційно-аналітичного забезпечення підтримки прийняття рішень щодо запобігання, протидії та нейтралізації загроз національній безпеці.</p> <p>ПРН09. Використовувати знання фундаментальних розділів математики в обсязі, необхідному для володіння математичним апаратом відповідної галузі знань, вміння використовувати статистичні та математичні методи в професійній діяльності.</p> <p>ПРН10. Вміти аналізувати виклики та загрози національній безпеці за напрямками професійної діяльності та синтезувати інформацію щодо розроблення та реалізації стратегій у визначальних сферах національної безпеки.</p> <p>ПРН11. Вміти пояснювати роль, місце та призначення політичних та безпекових інститутів України для ефективного здійснення заходів при виконання обов'язків з питань забезпечення національної безпеки.</p> <p>ПРН12. Вміти застосовувати знання з основ теорії національної безпеки, зокрема: оцінювати обстановку, рівень викликів та загроз національній безпеці.</p> <p>ПРН13. Відтворювати понятійно-категоріальний апарат загальної теорії національної безпеки щодо структури національної безпеки, об'єктів, суб'єктів та принципів забезпечення національної безпеки.</p> <p>ПРН14. 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.</p> <p>ПРН15. Аналізувати основні напрями забезпечення національної безпеки в державі, включаючи правові основи забезпечення національної безпеки, рівні та види національної безпеки, методи забезпечення національної безпеки, управління безпекою особистості, суспільства та держави через баланс їхніх життєво важливих інтересів, характеристики та критерії забезпечення національної безпеки.</p> <p>ПРН16. Планувати та організовувати особисту діяльність в умовах протиборства в інформаційній сфері та кіберпросторі для забезпечення інформаційної безпеки та кібербезпеки держави та організації.</p> <p>ПРН17. Оцінювати стан безпеки особистості, суспільства та держави за окремими сферами забезпечення і видами діяльності на основі положень теорії безпеки окремих сфер забезпечення національної безпеки і видів діяльності.</p> <p>ПРН18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.</p> <p>ПРН19. Вміти використовувати у професійній діяльності методи та інструменти організації соціальної взаємодії, співробітницт-</p>
--	---

	<p>ва 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.</p> <p>ПРН20. Аналізувати та упорядковувати основні властивості об'єктів безпеки окремих сфер забезпечення національної безпеки і видів діяльності та здійснювати класифікацію загроз об'єктам безпеки, класифікацію та ранжирування джерел загроз і уразливостей безпеки.</p> <p>ПРН21. Розробляти основні положення методів та заходів забезпечення інформаційної безпеки та кібербезпеки держави у різноманітних сферах життєдіяльності.</p> <p>ПРН22. Характеризувати систему забезпечення безпеки в інформаційній сфері та кіберпросторі, включаючи повноваження і функції суб'єктів забезпечення безпеки, контроль за здійсненням заходів забезпечення безпеки, основні завдання суб'єктів національної системи забезпечення кібербезпеки України.</p> <p>ПРН23. Визначати структуру, обґрунтовувати основні вимоги та архітектуру безпеки інформаційної інфраструктури та кіберінфраструктури.</p> <p>ПРН24. Обґрунтовувати застосування методів, заходів та засобів безпеки систем та мереж інформаційної інфраструктури та кіберінфраструктури.</p> <p>ПРН25. Здійснювати заходи щодо запобігання розголошення секретної інформації, випадкам втрат матеріальних носіїв цієї інформації, заволодіння цією інформацією іноземними державами, іноземними юридичними особами, іноземцями, особами без громадянства та громадянами України, яким не надано допуск та доступ до неї.</p> <p>ПРН26. Обґрунтовувати побудову систем та засобів фізичного захисту та захисту від зовнішніх впливів об'єктів інформаційної інфраструктури та кіберінфраструктури.</p> <p>ПРН27. Визначати комплекс завдань щодо управління у сфері інформаційної безпеки та кібербезпеки, методи, заходи і засоби щодо їх реалізації на різних організаційних рівнях, що охоплюють окремі організації, державні і міжнародні структури.</p> <p>ПРН28. Обґрунтовувати та визначати основні напрями створення та експлуатації системи та основних підсистем управління інформаційною безпекою та кібербезпекою.</p> <p>ПРН29. Визначати комплекс завдань щодо побудови системи технічного захисту інформації, методів, заходів і засобів щодо її реалізації на об'єктах інформаційної інфраструктури та кіберінфраструктури.</p> <p>ПРН30. Вирішувати завдання захисту інформації, що обробляється на об'єктах інформаційної інфраструктури та кіберінфраструктури з використанням методів, засобів і механізмів криптографічного захисту інформації.</p>
--	--

	<p>ПРН31. Обґрунтовувати застосування методів та засобів захисту програмних засобів, оцінки забезпечення якості програмного забезпечення а також інформаційно-програмних ресурсів і процесів, що беруть участь в життєвому циклі застосунків.</p> <p>ПРН32. Вирішувати завдання протидії несанкціонованому доступу до інформаційних ресурсів і процесів в системах інформаційної безпеки та кібербезпеки згідно встановленої політики інформаційної безпеки та кібербезпеки.</p> <p>ПРН33. Здійснювати відбір, оцінку, систематизацію та аналіз інформації в глобальній мережі для ефективного вирішення різних професійних завдань у сфері інформаційної безпеки.</p> <p>ПРН34. Захищати авторські права, комерційну таємницю, розробляти договори щодо розпорядження правами інтелектуальної власності в ІТ сфері.</p> <p>ПРН35. Використовувати професійно профільовані знання й уміння для організації та функціонування системи технічного захисту інформації.</p> <p>ПРН36. Забезпечувати процеси захисту та функціонування інформаційно-комунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.</p> <p>ПРН37. Вирішувати задачі захисту потоків даних в інформаційних, автоматизованих системах.</p> <p>ПРН38. Володіти методам та розуміти, застосовувати в дослідницькій і прикладній діяльності сучасний системи цифрової криміналістики.</p> <p>ПРН39. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки для розслідування внутрішніх та зовнішніх інцидентів в сфері кібербезпеки.</p> <p>ПРН40. Розрізняти етапи інформаційного протистояння, давати характеристику масово-інформаційних потоків в контексті інформаційного протистояння, виявляти реалізацію прийомів роботи зі смислами в інформаційному просторі.</p>
8 – Ресурсне забезпечення реалізації програми	
Кадрове забезпечення	<p>До освітнього процесу залучають науково-педагогічних та/або наукових співробітників (працівників), які мають відповідну освітню та/або професійну кваліфікацію та рівень досягнень у професійній діяльності за останні п'ять років, що засвідчується виконанням не менше чотирьох видів та результатів із перелічених у пункті 38 Ліцензійних умов провадження освітньої діяльності, затверджених постановою Кабінету Міністрів України від 30.12.2015 № 1187 (у редакції постанови Кабінету Міністрів України від 24.03.2021 № 365).</p> <p>Науково-педагогічні та/або наукові співробітники (працівники), задіяні до реалізації освітньої програми, не рідше одного разу на п'ять років проходять підвищення кваліфікації шляхом навчання за програмою підвищення кваліфікації та/або стажування.</p>
Матеріально-технічне забезпечення	<p>Для забезпечення освітнього процесу використовуються об'єкти Національної академії Служби безпеки України, зокрема навчальні</p>

	<p>приміщення для занять здобувачів вищої освіти (лекційні, аудиторні приміщення, спеціалізовані кабінети, лабораторії, комп'ютерні класи, спортивні зали тощо), укомплектовані технічними засобами навчання й контролю, мультимедійним обладнанням; приміщення для науково-педагогічних співробітників (працівників); бібліотека із читальними залами; службові приміщення. Доступ до мережі Інтернет.</p> <p>Соціальна інфраструктура об'єктів Національної академії Служби безпеки України охоплює гуртожитки для здобувачів вищої освіти, їдальні та буфети, спортивні споруди, студентський клуб, медичні пункти тощо.</p>
Інформаційне та навчально-методичне забезпечення	Використання традиційних та електронних інформаційних ресурсів загальної бібліотеки, сектору спеціальних навчальних фондів та авторських розробок науково-педагогічних співробітників (працівників) Національної академії Служби безпеки України.
9 – Особливості освітньої програми	
Академічна мобільність	У межах України на загальних підставах. Відповідно до законодавства України та розпорядчих документів Національної академії Служби безпеки України.
Міжнародна кредитна мобільність	Відповідно до Положення про порядок реалізації права на академічну мобільність, затвердженого постановою Кабінету Міністрів України від 12.08.2015 року № 579
Навчання іноземних здобувачів вищої освіти	Відповідно до Правил прийому до Національної академії Служби безпеки України на всі рівні вищої освіти приймаються на навчання виключно громадяни України.

II. Перелік компонентів освітньої програми та їх логічна послідовність

2.1. Загальна характеристика освітньої програми

№ з/п	Назва показника	Значення показника
1. Показники освітньої програми (у кредитах ЄКТС/годинах)		
1.1.	Загальний обсяг за весь термін навчання	240/7200
1.2.	Обсяг нормативної (обов'язкової) складової	180/5400
1.3.	Обсяг вибіркової складової, у тому числі:	60/1800
1.4.	Обсяг циклу загальної підготовки	64/1920
1.5.	Обсяг циклу професійної підготовки	116/3480
2. Показники навчального навантаження здобувачів вищої освіти (у кредитах ЄКТС/годинах)		
2.1.	Обсяг по рокам навчання	
2.1.1.	1 рік навчання	62/1860
2.1.2.	2 рік навчання	58/1740
2.1.3.	3 рік навчання	62/1860
2.1.4.	4 рік навчання	58/1740
2.2.	Тижневе навантаження	
2.2.1	максимальне	1/30
3. Показник співвідношення між навчальними заняттями і годинами самостійної роботи здобувачів вищої освіти (у кредитах ЄКТС/годинах)		
3.1.	Обсяг навчальних занять	115/3456
3.2.	Обсяг самостійної роботи	125/3744
4. Загальні показники компонент вищої освіти		

4.1.	Мінімальний обсяг навчальної дисципліни (спецкурсу), (у кредитах ЄКТС/годинах)	3/90
4.2.	Орієнтовна кількість навчальних дисциплін (спецкурсів) / із них за вільним вибором здобувачів вищої освіти	52/20
4.3.	Види практичної підготовки (тривалість у тижнях)	
4.3.1	Ознайомча практика	3/90
4.3.2.	Навчально-дослідна практика	3/90
4.3.3.	Виробнича практика	6/180
4.4.	Форма і назва атестації (тривалість підготовки до неї в днях)	
4.4.1.	Кіберзахист інформаційних ресурсів (комплексний екзамен)	5

2.2. Перелік компонент освітньої програми

Код н/д	Компоненти освітньої програми (навчальні дисципліни, спецкурси, курсові роботи, практики, кваліфікаційна робота)	Кількість кредитів ЄКТС	Форма підсумкового контролю	Номер додатка до освітньої програми
Обов'язкові компоненти освітньої програми				
Цикл загальної підготовки				
ОК-1	Історія української національної ідентичності	4	екзамен	Додаток 1
ОК-2	Академічні студії	4	диф. залік	Додаток 2
ОК-3	Правознавство	5	екзамен	Додаток 3
ОК-4	Вища математика	10	диф. залік/екзамен	Додаток 4
ОК-5	Філософія	4	екзамен	Додаток 5
ОК-6	Інформаційні технології	9	диф. залік/екзамен	Додаток 6
ОК-7	Українська мова професійного спрямування	4	диф. залік	Додаток 7
ОК-8	Іноземна мова (професійного спрямування)	14	диф. залік/екзамен	Додаток 8
ОК-9	Фізичне виховання	10	диф. залік	Додаток 9
Цикл професійної підготовки				
ОК-10	Фізичні основи захисту інформації	4	екзамен	Додаток 10
ОК-11	Теорія ймовірностей та математична статистика	4	диф. залік	Додаток 11
ОК-12	Мережеві технології та протоколи	5	диф. залік	Додаток 12
ОК-13	Алгоритмізація та основи програмування	5	екзамен	Додаток 13
ОК-14	Національна безпека	4	екзамен	Додаток 14
ОК-15	Теорія інформації та кодування	4	екзамен	Додаток 15
ОК-16	Програмні засоби захисту інформації	4	екзамен	Додаток 16
ОК-17	Технології програмування	6	екзамен	Додаток 17
ОК-18	Операційні системи і віртуалізація	5	екзамен	Додаток 18
ОК-19	Інформаційна безпека	4	екзамен	Додаток 19
ОК-20	Системний аналіз та прийняття рішень в інформаційній безпеці	5	екзамен	Додаток 20
ОК-21	Системи управління інформаційною безпекою	5	екзамен/курсора	Додаток 21
ОК-22	Проектування та безпека баз даних	5	диф. залік	Додаток 22
ОК-23	Моделювання систем критичної інфраструктури	4	екзамен/курсора	Додаток 23
ОК-24	Web - програмування	4	екзамен	Додаток 24

ОК-25	Безпека смарт-технологій та Інтернет речей	4	диф. залік	Додаток 25
ОК-26	Безпека інформації в інформаційно-комунікаційних системах	6	екзамен	Додаток 26
ОК-27	Кіберзахист інформаційних ресурсів	4	екзамен	Додаток 27
ОК-28	Технічний захист інформації	5	екзамен	Додаток 28
ОК-29	Хмарні технології та захист веб-додатків	4	диф. залік	Додаток 29
ОК-30	Інформаційне протиборство	4	диф. залік	Додаток 30
ОК-31	Комп'ютерна та мережева криміналістика	4	екзамен	Додаток 31
ОК-32	Комплексні системи захисту інформації	5	екзамен	Додаток 32
ОК-33	Ознайомча практика	3	диф. залік	Додаток 33
ОК-34	Навчальна практика	3	диф. залік	Додаток 34
ОК-35	Виробнича практика	6	диф. залік	Додаток 35
Всього обов'язкові компоненти		180		
Вибіркові компоненти освітньої програми				
Дисципліни вільного вибору (формується відповідно до переліку)		60	диф. заліки	
Всього		240		

*Згідно з Законом України «Про вищу освіту» здобувачі вищої освіти мають право на «вибір навчальних дисциплін у межах, передбачених відповідною освітньою програмою та робочим навчальним планом, в обсязі, що становить не менш як 25 відсотків загальної кількості кредитів ЄКТС, передбачених для даного рівня вищої освіти. При цьому здобувачі певного рівня вищої освіти мають право вибирати навчальні дисципліни, що пропонуються для інших рівнів вищої освіти та з інших спеціальностей та з переліку, сформованого закладом вищої освіти.

Механізм реалізації права здобувачів вищої освіти на вибір навчальних дисциплін визначається відповідним розпорядчим документом Національної академії СБ України. Вибіркові дисципліни можуть формуватися у блоки, тоді здобувач вищої освіти вибирає блок дисциплін, після чого усі дисципліни блоку стають обов'язковими для вивчення.

2.3. Структурно-логічна схема освітньої програми

Блоки дисциплін		1 семестр	2 семестр	3 семестр	4 семестр	5 семестр	6 семестр	7 семестр	8 семестр		
64 кредити	Цикл загальної підготовки	ОК-1 Історія української національної ідентичності	ОК-5 Філософія								
		ОК-2 Академічні студії	ОК-7 Українська мова професійного спрямування								
		ОК-3 Правознавство									
		ОК-4 Вища математика									
		ОК-6 Інформаційні технології									
		ОК-8 Іноземна мова (професійного спрямування)									
		ОК-9 Фізичне виховання									
116 кредитів	Цикл професійного спрямування	ОК-10 Фізичні основи захисту інформації	ОК-11 Теорія ймовірності та математичної статистики	ОК-13 Алгоритмізація та основи програмування	ОК-16 Програмні засоби захисту інформації	ОК-19 Інформаційна безпека	ОК-23 Моделювання систем критичної інфраструктури	ОК-27 Кіберзахист інформаційних ресурсів	ОК-30 Інформаційне протиборство		
			ОК-12 Мережеві технології та протоколи	ОК-14 Національна безпека	ОК-17 Технології програмування	ОК-20 Системний аналіз та прийняття рішень в інформаційній безпеці	ОК-24 Web-програмування	ОК-28 Технічний захист інформації	ОК-31 Компютерна та мережева криміналістика		
				ОК-15 Теорія інформації та кодування	ОК-18 Операційні системи і віртуалізація	ОК-21 Системи управління інформаційною безпекою	ОК-25 Безпека смарт технологій та Інтернет речей	ОК-29 Хмарні технології і захист веб-додатків	ОК-32 Комплексні системи захисту інформації		
					ОК-33 Ознайомча практика	ОК-22 Проектування та безпека баз даних	ОК-26 Безпека інформації в інформаційно-комунікаційних системах		ОК-35 Виробнича практика		
							ОК-34 Навчальна практика				
60 кредитів	Дисципліни вільного вибору			Дисципліни з переліку, 9 кредитів	Дисципліни з переліку, 9 кредитів	Дисципліни з переліку, 9 кредитів	Дисципліни з переліку, 9 кредитів	Дисципліни з переліку, 12 кредитів	Дисципліни з переліку, 12 кредитів		

III. Форми атестації здобувачів вищої освіти:

<p>Форми атестації здобувачів вищої освіти</p>	<p>Атестація – це встановлення відповідності засвоєних здобувачами освіти рівня та обсягу знань, умінь, інших компетентностей вимогам освітньої програми.</p> <p>Атестація випускників спеціальністю 256 Національна безпека (за окремими сферами забезпечення і видами діяльності); 256.04 забезпечення державної безпеки в інформаційній сфері здійснюється у формі екзамену:</p> <p>Кіберзахист інформаційних ресурсів (Комплексний атестаційний екзамен)</p> <p>Метою комплексних екзаменів (екзамену) та ЄДКІ є оцінювання рівня засвоєних здобувачами вищої освіти фахових і загальних компетентностей, визначених освітньою програмою, достатніх для розв’язання ситуативних задач оперативно-службової діяльності із застосуванням сучасних форм і методів оперативної роботи у сфері забезпечення державної безпеки, а також навчання на другому (магістерському) рівні вищої освіти.</p> <p>Здобувач вищої освіти допускається до складання комплексних екзаменів (екзамену) та ЄДКІ за умови відсутності в нього академічної заборгованості.</p>
<p>Вимоги до кваліфікаційної роботи</p>	<p>Організація і проведення атестаційного екзамену здобувачів вищої освіти здійснюється НА СБУ у порядку, встановленому законодавством України та Положенням про екзаменаційну комісію Національної академії Служби безпеки України, затвердженим наказом НА СБУ від 16.01.2016 № 20 (зі змінами) (далі – Положення 20-2016). Атестаційний екзамен проводиться відповідно до затвердженої програми, форма якої визначена додатком 1 до Положення 20-2016. Програма атестаційного екзамену розробляється відповідною кафедрою окремо з кожної освітньої програми підготовки фахівців.</p> <p>Програма атестаційного екзамену охоплює: цільову настанову та зміст програми, що розкривають питання програм навчальних дисциплін професійної підготовки за відповідною освітньою програмою (спеціалізацією); форму проведення (усна, письмова, поетапна тощо); єдині вимоги до критеріїв та порядку оцінювання рівня сформованості знань та умінь здобувачів вищої освіти відповідно до компетентностей, що визначені освітньо-професійною програмою; перелік нормативно-правових актів, навчальної, основної та додаткової літератури.</p> <p>Атестаційний екзамен приймається за білетами, кожний з яких містить теоретичні питання, що стосується різних розділів курсу і залежать від специфіки навчальної дисципліни. Для виявлення рівня практичної підготовки за фахом у білеті може бути передбачено виконання практичного завдання чи розв’язання задачі. Кількість питань у білеті визначає програма атестаційного екзамену (комплексного атестаційного екзамену).</p> <p>Зміст екзаменаційних білетів повинен відповідати програмі атестаційного екзамену.</p>

Вимоги до атестаційного/єдиного державного кваліфікаційного іспиту (іспитів) (за наявності)	Атестаційний іспит має бути спрямований на перевірку здатності розв'язувати складні задачі дослідницького та/або інноваційного характеру у галузі національної безпеки (кіберзахист, забезпечення державної безпеки в інформаційній сфері)
--	--

Атестація випускника освітньо-професійної програми завершується видачею документа встановленого зразка про присудження йому ступеня бакалавра із присвоєнням освітньої кваліфікації бакалавр з національної безпеки (кіберзахист, забезпечення державної безпеки в інформаційній сфері), фахівець із організації захисту інформації.

IV. Перелік компетентностей, визначених освітньою програмою (програмні компетентності), та їх відповідність дескрипторам шостого кваліфікаційного рівня Національної рамки кваліфікацій

Класифікація компетентностей (результатів навчання) за НРК	Знання	Уміння/навички	Комунікація	Відповідальність та автономія
	Зн1. Концептуальні наукові та практичні знання Зн2. Критичне осмислення теорій, принципів, методів і понять у сфері професійної діяльності та/або навчання	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	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, усно та письмово	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				
ЗК01.	Зн1		К2	АВ3
ЗК02.	Зн2		К2	АВ3
ЗК03.	Зн2	Ум1	К1, К2	АВ3
ЗК04.	Зн2	Ум1	К1,К2	АВ3
ЗК05.	Зн2	Ум1	К1, К2, К3	АВ3, АВ4
ЗК06.	Зн1	Ум1	К2,К3	АВ2,АВ3
ЗК07.	Зн1	Ум1	К2,К3	АВ3, АВ5
ЗК08.	Зн2	Ум1	К1, К2	АВ1,АВ2,АВ3
ЗК09.	Зн2	Ум1	К1	АВ2, АВ3,АВ5
ЗК10.	Зн2	Ум1	К2	АВ1,АВ2,АВ4
ЗК11.	Зн2	Ум1	К1,К2,К3	АВ3
ЗК12.	Зн1	Ум1	К1,К2	АВ3
ЗК13.	Зн2	Ум1	К1,К2	АВ3,АВ4
Фахові компетентності				
ФК01.	Зн2		К1	АВ3
ФК02.	Зн2	Ум1	К1	АВ5
ФК03.	Зн1	Ум1	К2	АВ1

Класифікація компетентностей (результатів навчання) за НРК	Знання	Уміння/навички	Комунікація	Відповідальність та автономія
ФК04.	Зн1		К1, К2	АВ2
ФК05.	Зн1		К1,К2	АВ1, АВ4
ФК06.	Зн1	Ум1	К1, К2, К3	АВ1
ФК07.	Зн2	Ум1	К2, К3	АВ3
ФК08.	Зн2	Ум1	К1, К2	АВ1
ФК09.	Зн2	Ум1	К2,К3	АВ2
ФК10.	Зн1	Ум1	К1, К3	АВ2
ФК11.	Зн2	Ум1	К1, К2	АВ2
ФК12.	Зн2		К1, К2	АВ4, АВ5
ФК13.	Зн2	Ум1	К2	АВ1, АВ2
ФК14.	Зн2		К1, К2	АВ4, АВ5
ФК15.	Зн2	Ум1	К1, К2,К3	АВ2,АВ3
ФК16.	Зн1	Ум1	К1, К2	АВ3
ФК17.	Зн2	Ум1	К1, К2	АВ2,АВ3
ФК18.	Зн2	Ум1	К1, К2,К3	АВ2,АВ3,АВ4
ФК19.	Зн2	Ум1	К1,К2	АВ2,АВ4
ФК20.	Зн2	Ум1	К2	АВ3
ФК21.	Зн2	Ум1	К2,К3	АВ1,АВ2,АВ5
ФК22.	Зн2	Ум1	К1,К2,К3	АВ1,АВ2,АВ4,АВ5
ФК23.	Зн1	Ум1	К1,К2	АВ3,АВ4
ФК24.	Зн2	Ум1	К1,К3	АВ1,АВ2
ФК25.	Зн2	Ум1	К1,К3	АВ1,АВ4,АВ5

V. Матриця відповідності визначених освітньою програмою результатів навчання та програмних компетентностей

Результати навчання	Компетентності																																								
	Інтегральна компетентність																																								
	Загальні компетентності													Спеціальні (фахові, предметні) компетентності																											
	ЗК01	ЗК02	ЗК03	ЗК04	ЗК05	ЗК06	ЗК07	ЗК08	ЗК09	ЗК10	ЗК11	ЗК12	ЗК13	ФК01	ФК02	ФК03	ФК04	ФК05	ФК06	ФК07	ФК08	ФК09	ФК10	ФК11	ФК12	ФК13	ФК14	ФК15	ФК16	ФК17	ФК18	ФК19	ФК20	ФК21	ФК22	ФК23	ФК24	ФК25			
PH01	+	+	+			+	+	+	+							+							+																		
PH02	+	+						+																																	
PH03			+			+	+	+		+		+			+						+	+																			
PH04				+																	+		+	+	+																
PH05					+	+	+		+		+								+	+		+	+					+								+	+		+	+	
PH06			+		+	+			+	+				+								+		+																	
PH07			+			+				+		+				+						+					+	+													
PH08								+			+						+									+		+	+												
PH09			+					+				+																													
PH10			+								+			+															+												
PH11	+													+																							+		+		
PH12	+									+					+		+					+						+								+	+		+		
PH13						+				+			+	+	+	+					+	+				+	+	+							+						
PH14					+		+			+								+	+		+	+		+				+								+	+		+	+	
PH15	+	+						+		+	+			+	+	+	+	+			+	+																			
PH16	+	+	+			+			+	+						+						+			+	+	+														
PH17	+		+			+	+			+	+				+	+	+					+			+		+		+						+						
PH18				+		+				+													+			+															
PH19	+	+		+	+				+										+	+		+		+			+	+							+	+	+	+	+	+	
PH20														+	+	+	+	+				+														+					
PH21											+		+					+					+	+	+			+												+	
PH22															+	+	+					+	+													+					
PH23																														+						+	+	+	+	+	+
PH24																											+	+							+		+	+	+		

Керівник проєктної групи

Олена КОБУС

Результати на- вчання	Компетентності																																							
	Інтегральна компетентність																																							
	Загальні компетентності													Спеціальні (фахові, предметні) компетентності																										
	ЗК01	ЗК02	ЗК03	ЗК04	ЗК05	ЗК06	ЗК07	ЗК08	ЗК09	ЗК10	ЗК11	ЗК12	ЗК13	ФК01	ФК02	ФК03	ФК04	ФК05	ФК06	ФК07	ФК08	ФК09	ФК10	ФК11	ФК12	ФК13	ФК14	ФК15	ФК16	ФК17	ФК18	ФК19	ФК20	ФК21	ФК22	ФК23	ФК24	ФК25		
PH25					+	+	+			+		+				+		+	+		+		+																	+
PH26											+				+						+	+			+		+													
PH27	+											+																+						+			+	+		
PH28		+		+	+																														+		+			
PH29	+											+																									+			
PH30		+								+				+									+			+											+		+	
PH31		+																										+								+	+			
PH32				+	+												+									+														
PH33																																				+		+	+	
PH34	+													+												+														
PH35																						+				+	+	+								+				
PH36													+	+																								+	+	
PH37												+						+				+	+				+									+		+	+	
PH38			+						+																			+						+					+	+
PH39					+	+	+	+		+				+	+	+	+	+	+	+				+															+	+
PH40														+	+												+	+											+	+

VI. Матриця відповідності програмних результатів навчання відповідним компонентам освітньої програми

	ОК-01	ОК-02	ОК-03	ОК-04	ОК-05	ОК-06	ОК-07	ОК-08	ОК-09	ОК-10	ОК-11	ОК-12	ОК-13	ОК-14	ОК-15	ОК-16	ОК-17	ОК-18	ОК-19	ОК-20	ОК-21	ОК-22	ОК-23	ОК-24	ОК-25	ОК-26	ОК-27	ОК-28	ОК-29	ОК-30	ОК-31	ОК-32	ОК-33	ОК-34	ОК-35			
ЗК01	+	+	+											+																+	+							
ЗК02	+	+			+		+		+																													
ЗК03		+		+		+				+	+		+					+		+			+							+	+		+	+	+			
ЗК04	+	+					+																															
ЗК05								+					+				+								+				+		+				+			
ЗК06		+			+	+		+				+		+	+	+		+				+	+		+	+	+	+		+	+	+	+	+	+	+		
ЗК07		+	+	+		+	+	+		+	+				+				+	+					+	+	+	+		+	+		+	+				
ЗК08		+							+					+																	+							
ЗК09		+	+		+		+	+						+					+	+	+	+					+			+	+		+	+				
ЗК10														+					+		+		+				+			+		+			+			
ЗК11																									+	+	+	+	+	+	+	+				+		
ЗК12				+							+		+		+									+								+	+					
ЗК13																														+	+	+				+		
ФК01		+												+					+	+										+	+	+				+		
ФК02														+					+	+	+		+									+						
ФК03	+	+	+																	+	+		+							+		+				+		
ФК04										+			+			+			+			+	+		+	+	+	+	+	+								
ФК05				+		+						+			+	+				+	+		+															
ФК06								+						+					+													+					+	
ФК07			+											+					+												+							
ФК08																				+	+		+									+					+	
ФК09	+		+					+						+					+	+	+		+						+			+					+	
ФК10		+	+				+	+						+					+		+																	

Керівник проєктної групи

Олена КОБУС

	OK-01	OK-02	OK-03	OK-04	OK-05	OK-06	OK-07	OK-08	OK-09	OK-10	OK-11	OK-12	OK-13	OK-14	OK-15	OK-16	OK-17	OK-18	OK-19	OK-20	OK-21	OK-22	OK-23	OK-24	OK-25	OK-26	OK-27	OK-28	OK-29	OK-30	OK-31	OK-32	OK-33	OK-34	OK-35	
ФК11		+					+	+	+					+								+					+		+	+					+	
ФК12																					+	+	+								+				+	
ФК13						+						+									+						+									
ФК14																															+			+	+	
ФК15														+					+												+				+	
ФК16						+										+		+				+					+				+			+	+	
ФК17	+	+	+																+												+	+			+	
ФК18										+																		+		+						
ФК19																				+	+															
ФК20										+					+													+				+				+
ФК21												+													+		+		+							
ФК22												+											+			+		+								
ФК23																+		+									+									
ФК24																												+				+				+
ФК25																											+					+				+

VII. Матриця забезпечення програмних результатів навчання відповідними компонентами освітньої програми

	ОК-01	ОК-02	ОК-03	ОК-04	ОК-05	ОК-06	ОК-07	ОК-08	ОК-09	ОК-10	ОК-11	ОК-12	ОК-13	ОК-14	ОК-15	ОК-16	ОК-17	ОК-18	ОК-19	ОК-20	ОК-21	ОК-22	ОК-23	ОК-24	ОК-25	ОК-26	ОК-27	ОК-28	ОК-29	ОК-30	ОК-31	ОК-32	ОК-33	ОК-34	ОК-35	
ПРН01	+	+	+				+							+																+	+					
ПРН02	+	+			+		+		+																											
ПРН03		+		+		+				+	+		+					+		+				+						+	+			+	+	+
ПРН04	+	+					+																													
ПРН05									+				+				+								+							+	+			+
ПРН06		+			+	+		+				+		+	+	+		+				+	+		+	+	+	+	+		+	+	+	+	+	+
ПРН07		+	+	+		+	+	+		+	+				+				+	+					+		+	+	+	+				+	+	
ПРН08				+		+						+		+	+					+	+			+												
ПРН09				+							+		+		+										+							+	+			
ПРН10														+					+	+	+		+									+				
ПРН11	+		+											+					+		+															
ПРН12														+					+																	
ПРН13														+					+																	
ПРН14	+						+	+																							+	+	+			+
ПРН15			+											+							+															
ПРН16		+							+								+								+			+					+			+
ПРН17			+												+				+																	+
ПРН18		+	+				+	+						+					+		+															
ПРН19		+	+		+		+	+						+					+	+	+	+						+		+	+		+	+		
ПРН20						+				+		+				+		+							+		+	+	+							
ПРН21	+	+	+																+													+	+			+
ПРН22												+											+				+									
ПРН23													+							+	+			+												
ПРН24												+													+	+	+		+							

	OK-01	OK-02	OK-03	OK-04	OK-05	OK-06	OK-07	OK-08	OK-09	OK-10	OK-11	OK-12	OK-13	OK-14	OK-15	OK-16	OK-17	OK-18	OK-19	OK-20	OK-21	OK-22	OK-23	OK-24	OK-25	OK-26	OK-27	OK-28	OK-29	OK-30	OK-31	OK-32	OK-33	OK-34	OK-35		
ПРН25								+		+				+		+		+							+	+	+	+	+	+					+		
ПРН26										+																	+				+					+	
ПРН27														+				+			+								+		+					+	
ПРН28																					+		+								+					+	
ПРН29										+																						+		+		+	
ПРН30															+												+	+			+	+					
ПРН31																+		+									+	+									
ПРН32														+					+				+				+				+						
ПРН33												+													+	+	+		+								
ПРН34							+	+							+										+	+	+	+	+	+							
ПРН35										+																			+			+					+
ПРН36												+				+		+				+	+			+	+		+	+							
ПРН37																					+	+		+													
ПРН38																						+	+									+					
ПРН39								+						+					+									+			+						+
ПРН40																														+					+		

VIII. Система забезпечення якості вищої освіти за освітньою програмою, що передбачає здійснення процедур внутрішнього та зовнішнього забезпечення якості:

- здійснення щорічного моніторингу відповідності кадрового, навчально-методичного, інформаційного та матеріально-технічного забезпечення Ліцензійним умовам провадження освітньої діяльності закладів освіти та вироблення на його основі заходів, спрямованих на покращання складових освітньої діяльності;
- забезпечення аналізу виконання здобувачами освіти навчального (робочих навчальних) планів освітньо-професійної програми, контролю якості викладання навчальних дисциплін в порядку та строки, визначені розпорядчими документами Національної академії СБ України;
- моніторинг та періодичний перегляд освітньої програми на підставі змін законодавства у сфері освіти, нормативно-правових актів СБ України щодо підготовки оперативного складу, а також пропозицій стейкхолдерів, здобувачів вищої освіти, інших учасників освітнього процесу;
- щорічне оцінювання здобувачів освіти, науково-педагогічних співробітників (працівників) Національної академії СБ України та регулярне оприлюднення результатів таких оцінювань на інформаційних стендах та/або в будь-який інший спосіб;
- забезпечення (не рідше одного разу на п'ять років) підвищення кваліфікації науково-педагогічних співробітників (працівників) НА СБУ шляхом навчання за програмою підвищення кваліфікації та/або стажування;
- забезпечення наявності необхідних ресурсів для організації освітнього процесу, зокрема самостійної роботи здобувачів вищої освіти;
- забезпечення наявності інформаційних систем для ефективного управління освітнім процесом;
- забезпечення публічності інформації про освітню програму, ступінь вищої освіти та кваліфікацію (освітню, професійну, у документі про освіту), з урахуванням вимог законодавства щодо інформації з обмеженим доступом;
- дотримання етичних принципів і правил академічної доброчесності науковими, науково-педагогічними співробітниками (працівниками), здобувачами вищої освіти;
- створення ефективної системи запобігання та виявлення академічного плагіату в наукових працях співробітників (працівників) НА СБУ і кваліфікаційних роботах здобувачів вищої освіти;
- проведення інших процедур і заходів.

VIII. Вимоги професійних стандартів (за наявності)

Професійних стандартів немає.

X. Перелік нормативних, розпорядчих, інструктивних документів, на яких базується освітня програма

1. Закон України від 01.07.2014 № 1556-VII «Про вищу освіту»;
2. Положення про проходження військової служби (навчання) курсантами вищих військових навчальних закладів (військових навчальних підрозділів закладів вищої освіти) Служби безпеки України, затверджене Указом Президента України від 09.10.2019 № 739;
3. Постанова Кабінету Міністрів України від 23.11.2011 № 1341 «Про затвердження Національної рамки кваліфікацій» (у редакції постанови Кабінету Міністрів України від 25.06.2020 № 519);
4. Постанова Кабінету Міністрів України від 29.04.2015 № 266 «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти»;
5. Постанова Кабінету Міністрів України від 30.12.2015 № 1187 «Про затвердження Ліцензійних умов провадження освітньої діяльності» (у редакції постанови Кабінету Міністрів України від 24.03.2021 № 365);
6. Постанова Кабінету Міністрів України від 19.05.2021 р. № 497 «Про атестацію здобувачів ступеня фахової передвищої освіти та ступенів вищої освіти на першому (бакалаврському) та другому (магістерському) рівнях у формі єдиного державного кваліфікаційного іспиту»;
7. Національний класифікатор України: «Класифікація видів економічної діяльності» ДК 009: 2010;
8. Національний класифікатор України «Класифікатор професій», затверджений наказом Держспоживстандарту України від 28.07.2010 № 237 (зі змінами);
9. Наказ Центрального управління Служби безпеки України від 30.03.2019 № 525/ДСК «Про затвердження Довідника кваліфікаційних характеристик до типових військових посад Служби безпеки України»;
10. Наказ Центрального управління Служби безпеки України від 02.11.2021 № 377, зареєстрований в Міністерстві юстиції України 16.11.2021 р. за № 1505/37128 «Про затвердження Положення з організації та проведення практичної підготовки курсантів вищих військових навчальних закладів (військових навчальних підрозділів закладів вищої освіти) Служби безпеки України»;
11. Наказ Міністерства освіти і науки України від 01.06.2016 № 600 (у редакції наказу Міністерства освіти і науки України від 30.04.2020 р. № 584) «Про затвердження та введення в дію Методичних рекомендацій щодо розроблення стандартів вищої освіти»;
12. Наказ Міністерства освіти і науки України від 22.05.2020 № 673, зареєстрований у Міністерстві юстиції України 09.06.2020 року за № 502/34785, «Про затвердження Переліку спеціальностей, здобуття ступеня освіти з

- яких необхідне для доступу до професій, для яких запроваджено додаткове регулювання»;
13. Лист МОН України від 28.04.2017 № 1/9-239 щодо примірного зразка освітньо-професійної програми для першого (бакалаврського) та другого (магістерського) рівнів вищої освіти;
 14. Лист Міністерства освіти і науки України від 05.06.2018 № 1/9-377 «Щодо надання роз'яснень стосовно освітніх програм»;
 15. Лист Міністерства освіти і науки України від 09.07.2018 № 1/9-434 «Щодо рекомендацій з навчально-методичного забезпечення»;
 16. Наказ Національної академії Служби безпеки України від 31.08.2015 № 234 (зі змінами) «Про затвердження Положення про організацію освітнього процесу в Національній академії Служби безпеки України»;
 17. Наказ Національної академії Служби безпеки України від 16.01.2016 № 20 (зі змінами) «Про затвердження Положення про екзаменаційну комісію Національної академії Служби безпеки України»;
 18. Наказ Національної академії Служби безпеки України від 06.12.2019 № 340 «Про затвердження Кодексу академічної доброчесності в Національній академії Служби безпеки України»;
 19. Наказ Національної академії Служби безпеки України від 17.04.2015 № 137 «Про затвердження Положення про ректорський контроль рівня знань курсантів, слухачів, студентів Національної академії Служби безпеки України»;
 20. Наказ Національної академії Служби безпеки України від 30.06.2020 № 164 «про затвердження Положення про наукове товариство студентів (курсантів, слухачів), аспірантів, докторантів і молодих вчених Національної академії СБ України»;
 21. Наказ Національної академії Служби безпеки України від 15.11.2016 № 337 «Про затвердження Порядку конкурсу педагогічної майстерності»;
 22. Наказ Національної академії Служби безпеки України від 29.12.2016 № 406 «Про затвердження Порядку організації контрольних, взаємних відвідувань і відкритих навчальних занять»;
 23. Наказ Національної академії Служби безпеки України від 29.12. 2017 № 430 «Про затвердження Порядку планування й обліку роботи науково-педагогічних співробітників (працівників) Національної академії Служби безпеки України»;
 24. Наказ Національної академії Служби безпеки України від 23.08.2017 № 273 «Про затвердження Порядку організації самостійної роботи здобувачів освіти Національної академії Служби безпеки України»;
 25. Наказ Національної академії Служби безпеки України від 02.11.2018 № 277 «Про затвердження Порядку самоаналізу діяльності за освітньою програмою (спеціальністю)»;
 26. Наказ Національної академії Служби безпеки України від 12.10.2016 № 293 «Про затвердження Правил ведення журналів обліку роботи академічних груп здобувачів освіти Національної академії Служби безпеки України»;

27. Наказ Національної академії Служби безпеки України від 15.11.2015 № 339 «Методичні рекомендації щодо оцінювання здобувачів освіти в Національній академії Служби безпеки України»;
28. Наказ проректора з наукової роботи Національної академії Служби безпеки України від 11.12.2018 «Методичні рекомендації з організації перевірки відкритих електронних рукописів на відсутність плагіату на базі системи виявлення збігів/ідентичності/схожості «Unicheck» у Національній академії СБ України»;
29. Рішення Науково-методичної ради НА СБ України від 22.10.2014, протокол № 2 «Про схвалення Концепції системи внутрішнього забезпечення якості вищої освіти в Національній академії Служби безпеки України»;
30. Національний освітній глосарій: вища освіта / 2-е вид., перероб. і доп. / авт.-уклад.: В. М. Захарченко, С. А. Калашнікова, В. І. Луговий,
31. А. В. Ставицький, Ю. М. Рашкевич, Ж. В. Таланова / За ред. В. Г. Кременя. – К.: ТОВ «Видавничий дім «Плеяди», 2014. – 100 с.;
32. Проект Європейської Комісії «Гармонізація освітніх структур в Європі» (Tuning Educational Structures in Europe, TUNING). TUNING (для ознайомлення зі спеціальними (фаховими) компетентностями та прикладами стандартів);
33. Європейська кредитна трансферно-накопичувальна система: довідник користувача / пер. з англ.; за ред. д-ра техн. наук, проф. Ю. М. Рашкевича та д-ра пед. наук, доц. Ж. В. Таланової. – Львів: видавництво Львівської політехніки, 2015. – 106 с.;
34. Стандарти і рекомендації щодо забезпечення якості в Європейському просторі вищої освіти (ESG). – К.: ТОВ «ЦС», 2015. – 32 с. Standards and Guidelines for Quality Assurance in the European Higher Education Area (ESG) – К.: CS Ltd., 2015. – 32 p. переклад «Стандартів і рекомендацій щодо забезпечення якості в Європейському просторі вищої освіти» здійснено Британською Радою в Україні за співпраці з Національним Еразмус+Офісом в Україні та Інститутом вищої освіти НАПН України;
35. Рашкевич Ю.М. Болонський процес та нова парадигма вищої освіти; Розвиток системи забезпечення якості вищої освіти в Україні: інформаційно-аналітичний огляд – 2015;
36. Методичні рекомендації для розроблення профілів ступеневих програм, включаючи програмні компетентності та програмні результати навчання/ пер. з англ. Національного експерта з реформування вищої освіти Програми Еразмус+, д-ра техн. наук, проф. Ю. М. Рашкевича. – Київ: ТОВ «Поліграф плюс», 2016. – 80 с. ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity“, 50 p.
37. Cybersecurity: A Generic Reference Curriculum (RC). Dear Partners/NATO Members, 4500-1 (OSEM PED), Oct. 2016, 73 p.

ДОДАТКИ:

1. Каталоги освітніх компонентів
2. Рецензії – відгуки зовнішніх стейкхолдерів