Прим. № 1

НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

ЗАТВЕРДЖЕНО

Рішення Вченої ради Національної академії Служби безпеки України
від 24.06.2021 р., протокол № 8

Ректор Національної академії Служби безпеки України
06.07.2021 р.

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
«КІБЕРЗАХИСТ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА КІБЕРПРОСТОРІ»
ДРУГОГО (МАГІСТЕРСЬКОГО) РІВНЯ ВИЩОЇ ОСВІТИ

Галузі знань	25 Воєнні науки, національна безпека, безпека державного кордону
Спеціальність	256 Національна безпека (за окремими сферами забезпечення і видами діяльності)
Спеціалізація	256.04 Національна безпека (кіберзахист, забезпечення державної безпеки в інформаційній сфері)
Кваліфікація	Магістр з національної безпеки (кіберзахист, забезпечення державної безпеки в інформаційній сфері)
Професійна кваліфікація	Професіонал з організації інформаційної безпеки

Київ 2021 р.

ЗМІСТ

ПЕРЕДМОВА

Введено вперше, як тимчасовий документ до введення в дію стандарту вищої освіти України за відповідним рівнем вищої освіти за спеціальністю 256 Національна безпека (за окремими сферами забезпечення і видами діяльності).

Розробники – проєктна група у складі науково-педагогічних співробітників (працівників) Національної академії Служби безпеки України, зацікавлених стейкхолдерів.

Рецензії-відгуки зовнішніх стейкхолдерів: Національний координаційних центр кібербезпеки Ради національної безпеки і оборони України, Громадська організація «ІСАКА КИЇВ».

1. Профіль освітньої програми «Кіберзахист у сфері інформаційних технологій та кіберпросторі»

1 – Загальна інформація	
Повна назва закладу вищої освіти	м. Київ, Національна академія Служби безпеки України
Ступінь вищої освіти та назва кваліфікації мовою оригіналу	Магістр з національної безпеки (кіберзахист, забезпечення державної безпеки в інформаційній сфері). Професіонал з організації інформаційної безпеки
Офіційна назва освітньої програми	Кіберзахист у сфері інформаційних технологій та кіберпросторі
Тип диплома та обсяг освітньої програми	диплом магістра, одиничний ступінь, 90 кредитів ЄКТС; термін навчання: 1 рік 6 місяців (денна форма навчання), 2 роки (заочна форма навчання)
Наявність акредитації	освітньо-професійна програма впроваджується з 2021 року
Цикл / рівень	НРК України – 7, FQ-EHEA – другий цикл, EQF LLL – 7 рівень
Передумови	Наявність освітнього ступеня бакалавра, магістра (освітньо-кваліфікаційного рівня спеціаліста)
Мова (и) викладання	українська
Термін дії освітньої програми	5 років; оновлення освітньої програми (за потреби) на підставі змін законодавства у сфері освіти, інформаційної безпеки та кібербезпеки, а також пропозицій стейкхолдерів, здобувачів вищої освіти, інших учасників освітнього процесу. Перегляд освітньої програми здійснюється щорічно відповідно до планових позицій НА СБУ
Інтернет-адреса постійного розміщення опису освітньої програми	ttps://academy.ssu.gov.ua/ (відповідно до умов і порядку, що визначаються нормативно-правовими актами Служби безпеки України).
2 – Мета освітньої програми	
Забезпечити підготовку висококваліфікованих професіоналів у галузі національної безпеки зі спеціальності 256.04 Національна безпека (кіберзахист, забезпечення державної безпеки в інформаційній сфері), здатних розв'язувати задачі дослідницького та/або інноваційного характеру та практичні проблеми організаційно-технічного забезпечення інформаційної безпеки та кібербезпеки, захищеності інформаційного простору 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 (за наявності)	*Галузь знань:* 25 Воєнні науки, національна безпека, безпека державного кордону. *Спеціальність:* 256.04 Національна безпека (кіберзахист, забезпечення державної безпеки в інформаційній сфері). *Міжнародна стандартна класифікація освіти:* 1031 Military and defence. *Об'єкт вивчення:* процеси, явища, проблеми забезпечення національної безпеки в інформаційній сфері та кіберпросторі. *Цілі навчання:* підготовка професіоналів, які володіють сучасним системним мисленням, теоретичними знаннями і практичними навичками, необхідними для розв'язання задач дослідницького та/або інноваційного характеру та практичних проблем забезпечення національної безпеки в інформаційній сфері, включаючи інформаційну безпеку, кібербезпеку,

	безпеку інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури. *Теоретичний зміст предметної області:* поняття, категорії, концепції, принципи, методи та засоби забезпечення національної безпеки в інформаційній сфері та кіберпросторі. *Методи, методики та технології:* наукового пізнання, управління та прийняття рішень, аналітичного оброблення інформації, організаційного, технічного та правового забезпечення безпеки, управління безпекою. *Інструменти та обладнання:* сучасне інформаційно-комунікаційне забезпечення та програмні продукти, що застосовуються в професійній діяльності.
Орієнтація освітньої програми	Освітньо-професійна, прикладна орієнтація.
Основний фокус освітньої програми та спеціалізації	Акцент на здатності організовувати й підтримувати комплекс інноваційних заходів щодо забезпечення інформаційної та кібербезпеки з урахуванням їхньої правової обґрунтованості, адміністративно-управлінської й технічної реалізації, економічної доцільності, можливих зовнішніх впливів, імовірних загроз і рівня розвитку технологій інформаційної безпеки та кібербезпеки на основі ризик-орієнтованого підходу.
Особливості освітньої програми	Інтегрована підготовка професіоналів до вирішення інноваційних завдань у сфері інформаційної безпеки та кібербезпеки, що передбачає використання аналітичних процесів при розробленні, впровадженні та експлуатації систем захисту інформації та кіберзахисту в організаціях та управління їх інформаційною та кібербезпекою.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Професіонал 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; Національного класифікатора ДК-009:2010 «Класифікація видів економічної діяльності»: 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). Здатний виконувати професійну роботу і може обіймати первинні посади відповідно до Національного класифікатора ДК 003:2010 «Класифікатор професій»: 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»; професіонал з організації інформаційної безпеки, код 2149.2, який класифікується, як «Професіонал з 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	Навчання на третьому (освітньо-науковому) рівні вищої освіти, набуття додаткових кваліфікацій у системі післядипломної освіти.
5 – Викладання та оцінювання	
Викладання та навчання	Студентоцентроване навчання, електронне навчання on-line, самонавчання, навчання на основі досліджень. Викладання проводиться у вигляді: лекцій, мультимедійних та/або інтерактивних лекцій, семінарів, практичних занять, лабораторних робіт, самостійного навчання на основі підручників та конспектів, консультацій з викладачами, підготовки кваліфікаційної (магістерської) роботи (проєкту).
Оцінювання	Оцінювання навчальних досягнень здійснюється за 100-бальною (рейтинговою) шкалою ЄКТС (ECTS), національною 4-х бальною шкалою («відмінно», «добре», «задовільно», «незадовільно») і вербальною («зараховано», «незараховано»). Види контролю: поточний, тематичний, періодичний, підсумковий. Форми контролю: усне та письмове опитування, тестові завдання, лабораторні звіти, презентації, захист курсової роботи, звіту з науково-дослідної практики, кваліфікаційної (магістерської) роботи.
6. Програмні компетентності	
Інтегральна компетентність	Здатність розв’язувати задачі дослідницького та/або інноваційного характеру та практичні проблеми забезпечення національної безпеки в інформаційній сфері та кіберпросторі та/або у процесі навчання.
Загальні компетентності (ЗК)	ЗК-01. Здатність формулювати задачу, для її вирішення та досягнення обґрунтованого висновку використовувати потрібну інформацію та методологію. ЗК-02. Знання стандартів, необхідних для наукового дослідження і публікування, включаючи критичну обізнаність та інтелектуальну чесність. ЗК-03. Здатність працювати в команді, виконуючи провідну роль, у міжнародній та мультикультурній групі. ЗК-04. Здатність спілкуватися державною та іноземною мовами згідно з різними комунікаційними стилями (неофіційним, офіційним, науковим). ЗК-05. Здатність скеровувати зусилля, поєднуючи результати різних досліджень та аналізу, вчасно подавати результат.
Фахові компетентності спеціальності (ФК)	СК-01. Здатність до аналізу об’єктів національної безпеки та оборони держави як сукупності елементів, що утворюють систему, здійснювати оцінку поведінки об’єкта за факторами, що впливають на його функціонування, визначати умови сприйняття та засвоєння деструктивних впливів на об’єкти національної безпеки та оборони. СК-02. Здатність робити оцінки у сфері національної безпеки і оборони та знаходити відповідні рішення із чітким визначенням припущень та використанням спеціальних і граничних випадків.

	СК-03. Здатність розуміти та використовувати математичні та числові методи, які часто використовуються в інформаційних, соціальних та психологічних технологіях у сфері національної безпеки і оборони. СК-04. Здатність до аналізу об’єктів інформаційного та кіберпростору, здійснювати оцінку поведінки об’єкта як системи з усіма факторами, що впливають на його функціонування, визначати умови сприйняття та засвоєння деструктивних впливів інформаційною сферою з метою забезпечення національної безпеки в цілому. СК-05. Здатність вирішувати широке коло загальних проблем і задач (завдань) протиборства в інформаційній сфері та кіберпросторі шляхом розуміння їх фундаментальних основ та використання як теоретичних, так і експериментальних методів. СК-06. Здатність використовувати відповідне програмне забезпечення (мови програмування, пакети) для реалізації загальних завдань протиборства в інформаційній сфері та спеціальних задач (операцій) у кіберпросторі. СК-07. Здатність описати широке коло методологічних, наукових та технічних основ побудови інформаційно-комунікаційних систем та їх безпеки, процеси протиборства в інформаційній сфері та кіберпросторі, систему стандартизації у галузі кібербезпеки провідних країн світу, методи та засоби забезпечення інформаційної безпеки, інформаційно-психологічної безпеки, кібербезпеки особистості, суспільства та держави в інформаційній сфері та кіберпросторі. СК-08. Здатність шляхом самостійної роботи розробляти та впроваджувати новітні заходи, методи та засоби щодо аналізу та організації заходів забезпечення національної безпеки в інформаційній сфері та кіберпросторі. СК-09. Здатність вирішувати широке коло проблем організаційно- технічного моделювання, створення та випробування систем забезпечення інформаційної та кібербезпеки. СК-10. Здатність вирішувати широке коло проблем, пов’язаних з організацією та реалізацією аудиторської діяльності у сфері інформаційної безпеки та кібербезпеки. СК-11. Здатність обґрунтовувати та впроваджувати заходи, методи та засоби щодо аналізу та організації протидії спеціальним операціям в інформаційній сфері та кіберпросторі. СК-12. Здатність обґрунтовувати та впроваджувати заходи, методи та засоби щодо організації антитерористичної діяльності в інформаційній сфері та кіберпросторі з метою забезпечення національної безпеки в цілому. СК-13. Здатність обґрунтовувати та впроваджувати заходи, методи та засоби щодо організації системи кіберзахисту об’єктів критичної інфраструктури. СК-14. Здатність обґрунтовувати та впроваджувати методи та моделі щодо організації науково-практичної діяльності у галузі кібербезпеки та національної безпеки в цілому.

7 – Програмні результати навчання	
	РН-01. Володіти системним знанням і здатністю відтворювати методологічні та теоретичні основи сучасних проблем забезпечення національної безпеки у державі. РН-02. Аналізувати об’єкти національної безпеки з метою оцінки поведінки об’єкта за факторами, що впливають на його функціонування, визначати умови сприйняття та засвоєння деструктивних впливів на об’єкти національної безпеки та оборони. РН-03. Робити оцінки у сфері національної безпеки і оборони та знаходити відповідні рішення із чітким визначенням припущень та використанням спеціальних і граничних випадків. РН-04. Застосовувати математичні та числові методи, які часто використовуються в інформаційних, соціальних та психологічних технологіях у сфері національної безпеки і оборони. РН-05. Проводити дослідження об’єктів інформаційної сфери та кіберпростору, здійснювати оцінку поведінки об’єкта як системи з усіма факторами, що впливають на його функціонування, визначати умови сприйняття та засвоєння деструктивних впливів інформаційною сферою та кіберпростором. РН-06. Вирішувати загальні проблеми і конкретні задачі (завдання) протиборства в інформаційній сфері та кіберпросторі шляхом розуміння їх фундаментальних основ та використання як теоретичних, так експериментальних методів. РН-07. Характеризувати широке коло методологічних, наукових та технічних основ побудови інформаційної сфери та кіберпростору, а також процеси протиборства в інформаційній сфері та кіберпросторі. РН-08. Оцінювати організацію протиборства в інформаційній сфері та кіберпросторі провідних країн світу. РН-09. Характеризувати інформаційні, інформаційно-психологічні операції та кібероперації в інформаційній сфері та кіберпросторі. РН-10. Брати участь в розробленні та реалізації методів та засобів забезпечення інформаційної безпеки, інформаційно-психологічної безпеки та кібербезпеки особистості суспільства та держави в інформаційні сфері та кіберпросторі. РН-11. Використовувати відповідне програмне забезпечення (мови програмування, пакети) для реалізації загальних завдань протиборства в інформаційній сфері та спеціальних задач (операцій) у кіберпросторі. РН-12. Розробляти та впроваджувати методи та заходи забезпечення інформаційної безпеки та безпеки електронних інформаційних ресурсів. РН-13. Розробляти та впроваджувати методи та заходи фізичної безпеки та кібербезпеки об’єктів критичної інформаційної інфраструктури. РН-14. Розробляти та впроваджувати інноваційні заходи, методи та засоби щодо аналізу та організації заходів

	забезпечення національної безпеки в інформаційній сфері та кіберпросторі. РН-15. Вирішувати широке коло проблем організаційно-технічного моделювання, створення та випробування систем забезпечення інформаційної та кібербезпеки. РН-16. Вирішувати широке коло проблем пов'язаних з організацією та реалізацією аудиторської діяльності у сфері інформаційної безпеки та кібербезпеки. РН-17. Володіти достатніми науковими знаннями щодо сфери правових, соціальних та політичних відносин в інформаційній сфері та кіберпросторі як середовища для проведення спеціальних операцій. РН-18. Визначати об'єкти протиборства і спеціальних операцій в інформаційній сфері та кіберпросторі, знати основні принципи, процеси та методи вивчення цих об'єктів. РН-19. Планувати, організовувати та реалізовувати протидію спеціальним операціям в кіберпросторі. РН-20. Розробляти загальні підходи до створення державної політики забезпечення протидії спеціальним операціям в інформаційній сфері та кіберпросторі. РН-21. Демонструвати достатні знання щодо класифікації та основних характеристик напрямів та видів розвідки кіберпростору, зокрема розвідки систем комунікацій, мережної розвідки та кіберрозвідки (розвідки застосунків), з метою виявлення об'єктів контррозвідувального захисту. РН-22. Обґрунтовувати та використовувати методи та засоби розвідки та контррозвідувального захисту в інформаційній сфері та кіберпросторі з метою планування та реалізації розвідувальних та контррозвідувальних операцій в кіберпросторі. РН-23. Обґрунтовувати та впроваджувати заходи, методи та засоби щодо організації антитерористичної діяльності в інформаційній сфері та кіберпросторі. РН-24. Обґрунтовувати та впроваджувати заходи, методи та засоби щодо організації оперативно-розшукової діяльності інформаційній сфері та кіберпросторі і розкриття кіберзлочинів, спрямованих проти національної безпеки. РН-25. Обґрунтовувати та впроваджувати заходи, методи та засоби щодо організації контролю кіберзахисту електронних інформаційних ресурсів. РН-26. Обґрунтовувати та впроваджувати заходи, методи та засоби щодо організації контроля кіберзахисту об'єктів критичної інфраструктури.
8 – Ресурсне забезпечення реалізації освітньої програми	
Кадрове забезпечення	До освітнього процесу залучаються науково-педагогічні, наукові співробітники (працівники), 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).

	Науково-педагогічні, наукові співробітники (працівники), задіяні до реалізації освітньої програми, не рідше одного разу на п’ять років підвищують кваліфікацію шляхом навчання за програмою підвищення кваліфікації та/або стажування.
Матеріально-технічне забезпечення	Для забезпечення освітнього процесу використовуються об’єкти НА СБУ, зокрема навчальні приміщення (лекційні зали, аудиторні, спеціалізовані кабінети, лабораторії, комп’ютерні класи тощо), укомплектовані технічними засобами навчання й контролю, мультимедійним обладнанням; бібліотека із читальними залами; приміщення для науково-педагогічних співробітників (працівників); службові приміщення. Соціальна інфраструктура об’єктів НА СБУ охоплює гуртожитки для здобувачів вищої освіти, їдальні та буфети, спортивні споруди, студентський клуб, медичні пункти тощо.
Інформаційне та навчально-методичне забезпечення	Для забезпечення освітнього процесу використовуються традиційні та електронні інформаційні ресурси бібліотеки, авторські розробки науково-педагогічних співробітників (працівників) НА СБУ.
9 – Академічна мобільність	
Національна кредитна мобільність	У межах України на загальних підставах. Відповідно до законодавства України та розпорядчих документів НА СБУ.
Міжнародна кредитна мобільність	Відповідно до Положення про порядок реалізації права на академічну мобільність, затвердженого постановою Кабінету Міністрів України від 12.08.2015 № 579. Здійснюється з дозволу керівництва СБУ за сприяння Центру міжнародного співробітництв СБУ на підставі укладених міжнародних угод з іноземними партнерами.
Навчання іноземних здобувачів вищої освіти	Відповідно до правил прийому на навчання до НА СБУ приймаються виключно громадяни України.

2. 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	92/2760
1.2.	Обсяг обов’язкової складової	34/1020
1.3.	Обсяг вибіркової складової, зокрема:	58/1740
1.3.1.	визначеної закладом вищої освіти	34/1020
1.3.2.	вільного вибору здобувача вищої освіти	24/720
1.4.	Обсяг циклу загальної підготовки	9/270
1.5.	Обсяг циклу професійної підготовки	83/2490
2. Показники навчального навантаження здобувача вищої освіти *(у кредитах ЄКТС/годинах)*		
2.1.	Обсяг по рокам навчання:	
2.1.1.	1 рік навчання	61/1830
2.1.2.	2 рік навчання	31/930
2.2.	Тижневе навантаження *(у годинах):*	
2.2.1.	максимальне	1,95/59
2.2.2.	мінімальне	1,6/48

3. Показник співвідношення між навчальними заняттями і годинами самостійної роботи здобувача вищої освіти *(у кредитах ЄКТС / годинах)*		
3.1.	Обсяг навчальних занять	1044
3.2.	Обсяг самостійної роботи	1716
4. Загальні показники компонентів освітньої програми		
4.1.	Мінімальний обсяг освітнього компонента *(у кредитах ЄКТС/годинах)*	3/90
4.2.	Максимальний обсяг освітнього компонента *(у кредитах ЄКТС/годинах)*	9/270
4.3.	Кількість обов'язкових освітніх компонентів	16
4.4.	Орієнтовна кількість освітніх компонентів вільного вибору здобувача вищої освіти	8
4.5.	Форма та назва атестації *(у кредитах ЄКТС/годинах)*	
4.5.1.	Кваліфікаційна (магістерська) робота	6/180

2.2. Перелік компонентів освітньої програми

Код	Компоненти освітньої програми	Кількість кредитів ЄКТС	Форма підсумкового контролю (семестр)	Каталог освітнього компонента
Обов'язкові компоненти				
Цикл загальної підготовки				
ОК-01	Методологія наукових досліджень	3	диф. залік (1)	Додаток 1
ОК-02	Ідентифікація та автентифікація цифрових образів	3	диф. залік (1)	Додаток 2
ОК-03	Іноземна мова (професійного спрямування)	3	екзамен (1)	Додаток 3
Всього за циклом загальної підготовки		9		
Цикл професійної підготовки				
ОК-04	Система стандартизації галузі кібербезпеки	3	диф. залік (2)	Додаток 4
ОК-05	Кіберзахист об'єктів критичної інфраструктури	4	екзамен (2)	Додаток 5
ОК-06	Соціальний інженірінг	3	диф. залік (3)	Додаток 6
ОК-07	Науково-дослідна практика	9	диф. залік (3)	Додаток 7
ОК-08	Кваліфікаційна (магістерська) робота	6	публічний захист	Додаток 8
Всього за циклом професійної підготовки		25		
Всього за обов'язковими компонентами		**34**		
Вибіркові компоненти				
Вибір закладу вищої освіти				
ОК-09	Побудова та впровадження системи менеджменту інформаційної безпеки	4	екзамен (1)	Додаток 9
ОК-10	Математичне моделювання систем і процесів	4	диф. залік (1)	Додаток 10
ОК-11	Розробка інформаційно-пошукових систем	4	екзамен (1)	Додаток 11
ОК-12	Безпека інформаційно-комунікаційних систем	5	курсова робота (1) екзамен (1)	Додаток 12
ОК-13	Методи та моделі протидії кібератакам	5	екзамен (2)	Додаток 13
ОК-14	Технології аудиту кібернетичної безпеки	3	диф. залік (2)	Додаток 14
ОК-15	Технології стеганографічного захисту інформації	5	екзамен (2)	Додаток 15
ОК-16	Управління кіберінцидентами	4	екзамен (3)	Додаток 16
Вільний вибір здобувача вищої освіти[1]				
ВК-01	Освітній компонент 1	24	диф. заліки (2, 3)	Робочі програми навчальних дисциплін
ВК-02	Освітній компонент 2			
…	…			
ВК-n	Освітній компонент n			
Всього за вибірковими компонентами		**58**		
ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ		**92**		

[1] Здобувач вищої освіти відповідно до власних освітніх або професійних, або наукових інтересів обирає освітні компоненти сумарним обсягом 24 ЄКТС / 720 год. із Переліку навчальних дисциплін (спецкурсів) вільного вибору здобувачів вищої освіти за спеціальністю 256.04 Національна безпека (кіберзахист, забезпечення державної безпеки в інформаційній сфері) для другого (магістерського) рівня вищої освіти.

2.3. Структурно-логічна схема освітньої програми

<table>
<tr><th>Складові освітньої програми</th><th>Цикли підготовки</th><th colspan="2">1 КУРС</th><th>2 КУРС</th></tr>
<tr><th></th><th></th><th>1 семестр</th><th>2 семестр</th><th>3 семестр</th></tr>
<tr><td rowspan="4">Обов'язкова</td><td rowspan="3">Загальна (9 ЄКТС)</td><td>ОК-01. Методологія наукових досліджень (3 ЄКТС, диф. залік)</td><td rowspan="3"></td><td rowspan="3"></td></tr>
<tr><td>ОК-02. Ідентифікація та автентифікації цифрових образів (3 ЄКТС, диф. залік)</td></tr>
<tr><td>ОК-03. Іноземна мова (професійного спрямування) (3 ЄКТС, екзамен)</td></tr>
<tr><td>Професійна (25 ЄКТС)</td><td rowspan="2"></td><td>ОК-04. Система стандартизації галузі кібербезпеки (3 ЄКТС, диф. залік)</td><td>ОК-06. Соціальний інженірінг (3 ЄКТС, диф. залік)</td></tr>
<tr><td rowspan="2">ОК-05. Кіберзахист об'єктів критичної інфраструктури (4 ЄКТС, екзамен)</td><td>ОК-07. Науково-дослідна практика (9 ЄКТС, диф. залік)</td></tr>
<tr><td>Разом:</td><td>34</td><td>9</td><td>7</td><td>ОК-08. Кваліфікаційна (магістерська) робота (6 ЄКТС, захист)
18</td></tr>
<tr><td rowspan="5">Вибіркова</td><td rowspan="4">Вибір НА СБУ (34 ЄКТС)</td><td>ОК-09. Побудова та впровадження системи менеджменту інформаційної безпеки (4 ЄКТС, екзамен)</td><td>ОК-13. Методи та моделі протидії кібератакам (5 ЄКТС, екзамен)</td><td>ОК-16. Управління кіберінцидентами (4 ЄКТС, екзамен)</td></tr>
<tr><td>ОК-10. Математичне моделювання систем і процесів (4 ЄКТС, диф. залік)</td><td>ОК-14. Технології аудиту кібернетичної безпеки (3 ЄКТС, диф. залік)</td><td rowspan="2"></td></tr>
<tr><td>ОК-11. Розробка інформаційно-пошукових систем (4 ЄКТС, екзамен)</td><td rowspan="2">ОК-15. Технології стеганографічного захисту інформації (5 ЄКТС, екзамен)</td></tr>
<tr><td>ОК-12. Безпека інформаційно-комунікаційних систем (5 ЄКТС, курсова робота, екзамен)</td></tr>
<tr><td>Вибір здобувача вищої освіти вищої освіти (24 ЄКТС)</td><td></td><td>Освітні компоненти вільного вибору здобувача вищої освіти (12 ЄКТС, диф. заліки)</td><td>Освітні компоненти вільного вибору здобувача вищої освіти (12 ЄКТС, диф. заліки)</td></tr>
<tr><td>Разом:</td><td>58</td><td>17</td><td>25</td><td>16</td></tr>
<tr><td>РАЗОМ:</td><td>92</td><td>26</td><td>32</td><td>34</td></tr>
</table>

3. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація – це встановлення відповідності результатів навчання здобувача вищої освіти вимогам освітньої програми. Атестація випускника освітньої програми «Кіберзахист у сфері інформаційних технологій та кіберпросторі» проводиться у формі захисту кваліфікаційної (магістерської) роботи.
Вимоги до кваліфікаційної роботи *(за наявності)*	Визначаються Положенням про кваліфікаційні роботи здобувачів вищої освіти в Національній академії Служби безпеки України, затвердженим наказом НА СБУ від 01.11.2016 № 313, Методичними рекомендаціями щодо етапів виконання, структури та технічних вимог до кваліфікаційних робіт здобувачів вищої освіти в Національній академії Служби безпеки України, схваленими Науково-методичною радою НА СБУ від 19.05.2016 р.
Вимоги до захисту кваліфікаційних *(за наявності)*	
Вимоги до атестаційного екзамену (екзаменів)	Організація і проведення атестації здобувачів 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).

Атестація випускника освітньої програми завершується видачею документа про вищу освіту встановленого зразка про присудження йому ступеня магістра із присвоєнням кваліфікації «Магістр з національної безпеки (кіберзахист, забезпечення державної безпеки в інформаційній сфері). Професіонал з організації інформаційної безпеки».

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

Компетентності, визначені освітньою програмою (програмні компетентності)	**Знання**	**Уміння/навички**	**Комунікація**	**Відповідальність та автономія**
	Інтегральна компетентність. Здатність розв'язувати задачі дослідницького та/або інноваційного характеру та практичні проблеми забезпечення національної безпеки в інформаційній сфері та кіберпросторі та/або у процесі навчання.			
	Зн1. Спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері професійної діяльності або галузі знань і є основою для оригінального мислення та проведення досліджень. **Зн2.** Критичне осмислення проблем у галузі та на межі галузей знань.	**Ум1.** Спеціалізовані уміння/навички розв'язання проблем, необхідні для проведення досліджень та/або провадження інноваційної діяльності з метою розвитку нових знань та процедур. **Ум2.** Здатність інтегрувати знання та розв'язувати складні задачі у широких або мультидисциплінарних контекстах. **Ум3.** Здатність розв'язувати проблеми у нових або незнайомих середовищах за наявності неповної або обмеженої інформації з урахуванням аспектів соціальної та етичної відповідальності.	**К1.** Зрозуміле і недвозначне донесення власних знань, висновків та аргументації до фахівців і не фахівців, зокрема до осіб, які навчаються.	**АВ1.** Управління робочими або навчальними процесами, які є складними, непередбачуваними та потребують нових стратегічних підходів. **АВ2.** Відповідальність за внесок до професійних знань і практики та/або оцінювання результатів діяльності команд та колективів. **АВ3.** Здатність продовжувати навчання з високим ступенем автономії.
Загальні компетентності				
ЗК-01. Здатність формулювати задачу, для її вирішення та досягнення обґрунтованого висновку використовувати потрібну інформацію та методологію.	**Зн2**	**Ум2**	**К1**	**АВ2**
ЗК-02. Знання стандартів, необхідних для наукового дослідження і публікування, включаючи критичну обізнаність та інтелектуальну чесність.	**Зн1**	**Ум1**	**К1**	**АВ2**
ЗК-03. Здатність працювати в команді, виконуючи провідну роль, у міжнародній та мультикультурній групі.	**Зн2**	**Ум3**	**К1**	**АВ1**
ЗК-04. Здатність спілкуватися державною та іноземною мовами згідно з різними комунікаційними стилями (неофіційним, офіційним, науковим).	**Зн1**	**Ум1**	**К1**	**АВ3**
ЗК-05. Здатність скеровувати зусилля, поєднуючи результати різних досліджень та аналізу, вчасно подавати результат.	**Зн2**	**Ум1**	**К1**	**АВ1**
Спеціальні (фахові) компетентності				
СК-01. Здатність до аналізу об'єктів національної безпеки та оборони держави як сукупності елементів, що утворюють систему, здійснювати оцінку поведінки об'єкта за факторами, що впливають на його функціонування, визначати умови сприйняття та засвоєння деструктивних впливів на об'єкти національної безпеки та оборони.	**Зн2**	**Ум1, Ум2**	**К1**	**АВ1**

Компетентності, визначені освітньою програмою (програмні компетентності)	Знання	Уміння/навички	Комунікація	Відповідальність та автономія
СК-02. Здатність робити оцінки у сфері національної безпеки і оборони та знаходити відповідні рішення із чітким визначенням припущень та використанням спеціальних і граничних випадків.	**Зн2**	**Ум3**	**К1**	**АВ1**
СК-03. Здатність розуміти та використовувати математичні та числові методи, які часто використовуються в інформаційних, соціальних та психологічних технологіях у сфері національної безпеки і оборони.	**Зн1**	**Ум2**	**К1**	**АВ3**
СК-04. Здатність до аналізу об'єктів інформаційного та кіберпростору, здійснювати оцінку поведінки об'єкта як системи з усіма факторами, що впливають на його функціонування, визначати умови сприйняття та засвоєння деструктивних впливів інформаційною сферою з метою забезпечення національної безпеки в цілому.	**Зн1**	**Ум1**	**К1**	**АВ3**
СК-05. Здатність вирішувати широке коло загальних проблем і задач (завдань) протиборства в інформаційній сфері та кіберпросторі шляхом розуміння їх фундаментальних основ та використання як теоретичних, так експериментальних методів.	**Зн2**	**Ум2**	**К1**	**АВ1**
СК-06. Здатність використовувати відповідне програмне забезпечення (мови програмування, пакети) для реалізації загальних завдань протиборства в інформаційній сфері та спеціальних задач (операцій) у кіберпросторі.	**Зн1**	**Ум1**	**К1**	**АВ1**
СК-07. Здатність описати широке коло методологічних, наукових та технічних основ побудови інформаційної сфери та кіберпростору, процеси протиборства в інформаційній сфері та кіберпросторі, організацію протиборства в інформаційній сфері та кіберпросторі провідних країн світу, інформаційно-психологічні операції у кібернетичному просторі, методи та засоби забезпечення інформаційної безпеки, інформаційно-психологічної безпеки, кібербезпеки особистості, суспільства та держави в інформаційній сфері та кіберпросторі.	**Зн2**	**Ум2**	**К1**	**АВ2**
СК-08. Здатність шляхом самостійної роботи розробляти та впроваджувати новітні заходи, методи та засоби щодо аналізу та організації заходів забезпечення національної безпеки в інформаційній сфері та кіберпросторі.	**Зн2**	**Ум2**	**К1**	**АВ3**

Компетентності, визначені освітньою програмою (програмні компетентності)	Знання	Уміння/навички	Комунікація	Відповідальність та автономія
СК-09. Здатність вирішувати широке коло проблем організаційно-технічного моделювання, створення та випробування систем забезпечення інформаційної та кібербезпеки.	**Зн1**	**Ум3**	**К1**	**АВ1**
СК-10. Здатність вирішувати широке коло проблем, пов'язаних з організацією та реалізацією аудиторської діяльності у сфері інформаційної безпеки та кібербезпеки.	**Зн1**	**Ум1**	**К1**	**АВ1**
СК-11. Здатність обґрунтовувати та впроваджувати заходи, методи та засоби щодо аналізу та організації протидії спеціальним операціям в інформаційній сфері та кіберпросторі.	**Зн2**	**Ум3**	**К1**	**АВ2**
СК-12. Здатність обґрунтовувати та впроваджувати заходи, методи та засоби щодо організації антитерористичної діяльності в інформаційній сфері та кіберпросторі з метою забезпечення національної безпеки в цілому.	**Зн2**	**Ум2**	**К1**	**АВ3**
СК-13. Здатність обґрунтовувати та впроваджувати заходи, методи та засоби щодо організації системи кіберзахисту об'єктів критичної інфраструктури.	**Зн1**	**Ум1**	**К1**	**АВ2**
СК-14. Здатність обґрунтовувати та впроваджувати методи та моделі щодо організації науково-практичної діяльності у галузі кібербезпеки та національної безпеки в цілому.	**Зн1**	**Ум3**	**К1**	**АВ3**

5. Матриця відповідності визначених освітньою програмою результатів навчання (програмні результати) та програмних компетентностей

	Інтегральна компетентність. Здатність розв'язувати задачі дослідницького та/або інноваційного характеру та практичні проблеми забезпечення національної безпеки в інформаційній сфері та кіберпросторі та/або у процесі навчання.																	
	Загальні компетентності					**Спеціальні (фахові) компетентності**												
	ЗК-01	**ЗК-02**	**ЗК-03**	**ЗК-04**	**ЗК-05**	**СК-01**	**СК-02**	**СК-03**	**СК-04**	**СК-05**	**СК-06**	**СК-07**	**СК-08**	**СК-09**	**СК-10**	**СК-11**	**СК-12**	**СК-13**	**СК-14**
РН-01. Володіти системним знанням і здатністю відтворювати методологічні та теоретичні основи сучасних проблем забезпечення національної безпеки у державі.	+	+				+													
РН-02. Аналізувати об'єкти національної безпеки з метою оцінки поведінки об'єкта за факторами, що впливають на його функціонування, визначати умови сприйняття та засвоєння деструктивних впливів на об'єкти національної безпеки та оборони.	+	+			+		+												
РН-03. Робити оцінки у сфері національної безпеки і оборони та знаходити відповідні рішення із чітким визначенням припущень та використанням спеціальних і граничних випадків.	+	+					+	+											
РН-04. Застосовувати математичні та числові методи, які часто використовуються в інформаційних, соціальних та психологічних технологіях у сфері національної безпеки і оборони.	+	+						+											
РН-05. Проводити дослідження об'єктів інформаційної сфери та кіберпростору, здійснювати оцінку поведінки об'єкта як системи з усіма факторами, що впливають на його функціонування, визначати умови сприйняття та засвоєння деструктивних впливів інформаційною сферою та кіберпростором.	+	+	+	+	+				+										
РН-06. Вирішувати загальні проблеми і конкретні задачі (завдання) протиборства в інформаційній сфері та кіберпросторі шляхом розуміння їх фундаментальних основ та використання як теоретичних, так і експериментальних методів.	+	+	+	+	+					+	+								

	ЗК-01	ЗК-02	ЗК-03	ЗК-04	ЗК-05	СК-01	СК-02	СК-03	СК-04	СК-05	СК-06	СК-07	СК-08	СК-09	СК-10	СК-11	СК-12	СК-13	СК-14
РН-07. Характеризувати широке коло методологічних, наукових та технічних основ побудови інформаційної сфери та кіберпростору, а також процеси протиборства в інформаційній сфері та кіберпросторі.	+	+										+							
РН-08. Оцінювати організацію протиборства в інформаційній сфері та кіберпросторі провідних країн світу.	+	+		+								+							
РН-09. Характеризувати інформаційні, інформаційно-психологічні операції та кібероперації в інформаційній сфері та кіберпросторі.	+	+		+	+							+							
РН-10. Брати участь в розробленні та реалізації методів та засобів забезпечення інформаційної безпеки, інформаційно-психологічної безпеки та кібербезпеки особистості суспільства та держави в інформаційні сфері та кіберпросторі.	+	+		+	+							+					+		
РН-11. Використовувати відповідне програмне забезпечення (мови програмування, пакети) для реалізації загальних завдань протиборства в інформаційній сфері та спеціальних задач (операцій) у кіберпросторі.	+	+		+	+						+								
РН-12. Розробляти та впроваджувати методи та заходи забезпечення інформаційної безпеки та безпеки електронних інформаційних ресурсів.	+	+		+	+							+							
РН-13. Розробляти та впроваджувати методи та заходи фізичної безпеки та кібербезпеки об’єктів критичної інформаційної інфраструктури.	+	+		+	+							+						+	
РН-14. Розробляти та впроваджувати інноваційні заходи, методи та засоби щодо аналізу та організації заходів забезпечення національної безпеки в інформаційній сфері та кіберпросторі.	+	+	+	+	+								+						
РН-15. Вирішувати широке коло проблем організаційно-технічного моделювання, створення та випробування систем забезпечення інформаційної та кібербезпеки.							+		+	+			+				+		+

	ЗК-01	ЗК-02	ЗК-03	ЗК-04	ЗК-05	СК-01	СК-02	СК-03	СК-04	СК-05	СК-06	СК-07	СК-08	СК-09	СК-10	СК-11	СК-12	СК-13	СК-14
РН-16. Вирішувати широке коло проблем, пов'язаних з організацією та реалізацією аудиторської діяльності у сфері інформаційної безпеки та кібербезпеки.			+												+				
РН-17. Володіти достатніми науковими знаннями щодо сфери правових, соціальних та політичних відносин в інформаційній сфері та кіберпросторі як середовища для проведення спеціальних операцій.	+	+				+													
РН-18. Визначати об'єкти протиборства і спеціальних операцій в інформаційній сфері та кіберпросторі, знати основні принципи, процеси та методи вивчення цих об'єктів.	+	+			+		+												
РН-19. Планувати, організовувати та реалізовувати протидію спеціальним операціям в кіберпросторі.	+	+					+	+					+						
РН-20. Розробляти загальні підходи до створення державної політики забезпечення протидії спеціальним операціям в інформаційній сфері та кіберпросторі.	+	+						+						+					
РН-21. Демонструвати достатні знання щодо класифікації та основних характеристик напрямів та видів розвідки кіберпростору, зокрема розвідки систем комунікацій, мережної розвідки та кіберрозвідки (розвідки застосунків), з метою виявлення об'єктів контррозвідувального захисту.	+	+	+	+	+				+										
РН-22. Обґрунтовувати та використовувати методи та засоби розвідки та контррозвідувального захисту в інформаційній сфері та кіберпросторі з метою планування та реалізації розвідувальних та контррозвідувальних операцій в кіберпросторі.	+	+	+	+	+					+	+								
РН-23. Обґрунтовувати та впроваджувати заходи, методи та засоби щодо організації антитерористичної діяльності в інформаційній сфері та кіберпросторі.								+				+			+		+		

	ЗК-01	ЗК-02	ЗК-03	ЗК-04	ЗК-05	СК-01	СК-02	СК-03	СК-04	СК-05	СК-06	СК-07	СК-08	СК-09	СК-10	СК-11	СК-12	СК-13	СК-14
РН-24. Здатність обґрунтовувати та впроваджувати заходи, методи та засоби щодо організації оперативно-розшукової діяльності в інформаційній сфері та кіберпросторі і розкриття кіберзлочинів спрямованих проти національної безпеки.				+			+							+		+			
РН-25. Обґрунтовувати та впроваджувати заходи, методи та засоби щодо організації контролю кіберзахисту електронних інформаційних ресурсів.	+	+							+						+		+		
РН-26. Обґрунтовувати та впроваджувати заходи, методи та засоби щодо організації контроля кіберзахисту об’єктів критичної інфраструктури.				+									+					+	+

6. Матриця відповідності програмних компетентностей 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
Загальні компетентності																
ЗК-01. Здатність формулювати задачу, для її вирішення та досягнення обґрунтованого висновку використовувати потрібну інформацію та методологію.	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК-02. Знання стандартів, необхідних для наукового дослідження і публікування, включаючи критичну обізнаність та інтелектуальну чесність.	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК-03. Здатність працювати в команді, виконуючи провідну роль, у міжнародній та мультикультурній групі.	+	+	+	+	+		+	+	+	+	+		+	+		
ЗК-04. Здатність спілкуватися державною та іноземною мовами згідно з різними комунікаційними стилями (неофіційним, офіційним, науковим).		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ЗК-05. Здатність скеровувати зусилля, поєднуючи результати різних досліджень та аналізу, вчасно подавати результат.		+	+	+	+		+	+	+	+	+	+	+	+	+	+
Спеціальні (фахові) компетентності																
СК-01. Здатність до аналізу об’єктів національної безпеки та оборони держави як сукупності елементів, що утворюють систему, здійснювати оцінку поведінки об’єкта за факторами, що впливають на його функціонування, визначати умови сприйняття та засвоєння деструктивних впливів на об’єкти національної безпеки та оборони.	+	+									+					
СК-02. Здатність робити оцінки у сфері національної безпеки і оборони та знаходити відповідні рішення із чітким визначенням припущень та використанням спеціальних і граничних випадків.	+	+	+	+		+	+	+		+		+	+	+	+	+
СК-03. Здатність розуміти та використовувати математичні та числові методи, які часто використовуються в інформаційних, соціальних та психологічних технологіях у сфері національної безпеки і оборони.	+			+	+	+	+	+				+		+	+	+
СК-04. Здатність до аналізу об’єктів інформаційного та кіберпростору, здійснювати оцінку поведінки об’єкта як системи з усіма факторами, що впливають на його функціонування, визначати умови сприйняття та засвоєння деструктивних впливів інформаційною сферою з метою забезпечення національної безпеки в цілому.			+			+		+		+	+		+			+
СК-05. Здатність вирішувати широке коло загальних проблем і задач (завдань) протиборства в інформаційній сфері та кіберпросторі шляхом розуміння їх фундаментальних основ та використання як теоретичних, так експериментальних методів.		+		+		+	+	+			+		+			

	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
СК-06. Здатність використовувати відповідне програмне забезпечення (мови програмування, пакети) для реалізації загальних завдань протиборства в інформаційній сфері та спеціальних задач (операцій) у кіберпросторі.		+		+			+	+			+					
СК-07. Здатність описати широке коло методологічних, наукових та технічних основ побудовиінформаційної сфери та кіберпростору, процеси протиборства в інформаційній сфері та кіберпросторі, організацію протиборства в інформаційній сфері та кіберпросторі провідних країн світу, інформаційно-психологічні операції у кібернетичному просторі, методи та засоби забезпечення інформаційної безпеки, інформаційно-психологічної безпеки, кібербезпеки особистості, суспільства та держави в інформаційній сфері та кіберпросторі.		+	+		+			+	+	+	+	+	+	+	+	+
СК-08. Здатність шляхом самостійної роботи розробляти та впроваджувати новітні заходи, методи та засоби щодо аналізу та організації заходів забезпечення національної безпеки в інформаційній сфері та кіберпросторі.		+		+	+	+			+			+	+	+		
СК-09. Здатність вирішувати широке коло проблем організаційно-технічного моделювання, створення та випробування систем забезпечення інформаційної та кібербезпеки.						+		+								+
СК-10. Здатність вирішувати широке коло проблем, пов’язаних з організацією та реалізацією аудиторської діяльності у сфері інформаційної безпеки та кібербезпеки.	+				+			+			+	+		+		+
СК-11. Здатність обґрунтовувати та впроваджувати заходи, методи та засоби щодо аналізу та організації протидії спеціальним операціям в інформаційній сфері та кіберпросторі.						+										+
СК-12. Здатність обґрунтовувати та впроваджувати заходи, методи та засоби щодо організації антитерористичної діяльності в інформаційній сфері та кіберпросторі з метою забезпечення національної безпеки в цілому.			+		+	+		+			+	+	+	+		+
СК-13. Здатність обґрунтовувати та впроваджувати заходи, методи та засоби щодо організації системи кіберзахисту об’єктів критичної інфраструктури.					+											
СК-14. Здатність обґрунтовувати та впроваджувати методи та моделі щодо організації науково-практичної діяльності у галузі кібербезпеки та національної безпеки в цілому.		+				+			+				+			

7. Матриця забезпечення програмних результатів відповідними освітніми компонентами

	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
РН-01. Володіти системним знанням і здатністю відтворювати методологічні та теоретичні основи сучасних проблем забезпечення національної безпеки у державі.	+															
РН-02. Аналізувати об'єкти національної безпеки з метою оцінки поведінки об'єкта за факторами, що впливають на його функціонування, визначати умови сприйняття та засвоєння деструктивних впливів на об'єкти національної безпеки та оборони.		+	+							+						
РН-03. Робити оцінки у сфері національної безпеки і оборони та знаходити відповідні рішення із чітким визначенням припущень та використанням спеціальних і граничних випадків.	+			+			+	+								
РН-04. Застосовувати математичні та числові методи, які часто використовуються в інформаційних, соціальних та психологічних технологіях у сфері національної безпеки і оборони.	+				+										+	
РН-05. Проводити дослідження об'єктів інформаційної сфери та кіберпростору, здійснювати оцінку поведінки об'єкта як системи з усіма факторами, що впливають на його функціонування, визначати умови сприйняття та засвоєння деструктивних впливів інформаційною сферою та кіберпростором.			+							+						
РН-06. Вирішувати загальні проблеми і конкретні задачі (завдання) протиборства в інформаційній сфері та кіберпросторі шляхом розуміння їх фундаментальних основ та використання як теоретичних, так і експериментальних методів.				+			+	+			+					
РН-07. Характеризувати широке коло методологічних, наукових та технічних основ побудови інформаційної сфери та кіберпростору, а також процеси протиборства в інформаційній сфері та кіберпросторі.			+						+					+		
РН-08. Оцінювати організацію протиборства в інформаційній сфері та кіберпросторі провідних країн світу.		+			+							+			+	
РН-09. Характеризувати інформаційні, інформаційно-психологічні операції та кібероперації в інформаційній сфері та кіберпросторі.												+				+
РН-10. Брати участь в розробленні та реалізації методів та засобів забезпечення інформаційної безпеки, інформаційно-психологічної безпеки та кібербезпеки особистості суспільства та держави в інформаційні сфері та кіберпросторі.			+					+			+			+		
РН-11. Використовувати відповідне програмне забезпечення (мови програмування, пакети) для реалізації загальних завдань протиборства в інформаційній сфері та спеціальних задач (операцій) у кіберпросторі.				+			+									
РН-12. Розробляти та впроваджувати методи та заходи забезпечення інформаційної безпеки та безпеки електронних інформаційних ресурсів.										+			+			

	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
РН-13. Розробляти та впроваджувати методи та заходи фізичної безпеки та кібербезпеки об'єктів критичної інформаційної інфраструктури.		+			+										+	
РН-14. Розробляти та впроваджувати інноваційні заходи, методи та засоби щодо аналізу та організації заходів забезпечення національної безпеки в інформаційній сфері та кіберпросторі.					+				+					+		
РН-15. Вирішувати широке коло проблем організаційно-технічного моделювання, створення та випробування систем забезпечення інформаційної та кібербезпеки.						+							+			
РН-16. Вирішувати широке коло проблем, пов'язаних з організацією та реалізацією аудиторської діяльності у сфері інформаційної безпеки та кібербезпеки.	+							+								
РН-17. Володіти достатніми науковими знаннями щодо сфери правових, соціальних та політичних відносин в інформаційній сфері та кіберпросторі як середовища для проведення спеціальних операцій.		+									+					
РН-18. Визначати об'єкти протиборства і спеціальних операцій в інформаційній сфері та кіберпросторі, знати основні принципи, процеси та методи вивчення цих об'єктів.			+												+	
РН-19. Планувати, організовувати та реалізовувати протидію спеціальним операціям в кіберпросторі.				+								+		+		
РН-20. Розробляти загальні підходи до створення державної політики забезпечення протидії спеціальним операціям в інформаційній сфері та кіберпросторі.						+		+								+
РН-21. Демонструвати достатні знання щодо класифікації та основних характеристик напрямів та видів розвідки кіберпростору, зокрема розвідки систем комунікацій, мережної розвідки та кіберрозвідки (розвідки застосунків), з метою виявлення об'єктів контррозвідувального захисту.										+			+			
РН-22. Обґрунтовувати та використовувати методи та засоби розвідки та контррозвідувального захисту в інформаційній сфері та кіберпросторі з метою планування та реалізації розвідувальних та контррозвідувальних операцій в кіберпросторі.		+					+									
РН-23. Обґрунтовувати та впроваджувати заходи, методи та засоби щодо організації антитерористичної діяльності в інформаційній сфері та кіберпросторі.					+							+		+		
РН-24. Здатність обґрунтовувати та впроваджувати заходи, методи та засоби щодо організації оперативно-розшукової діяльності в інформаційній сфері та кіберпросторі і розкриття кіберзлочинів спрямованих проти національної безпеки.						+										+
РН-25. Обґрунтовувати та впроваджувати заходи, методи та засоби щодо організації контролю кіберзахисту електронних інформаційних ресурсів.								+			+					+
РН-26. Обґрунтовувати та впроваджувати заходи, методи та засоби щодо організації контроля кіберзахисту об'єктів критичної інфраструктури.		+			+				+				+			

8. 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 та вироблення на його основі заходів, спрямованих на покращання відповідних складових освітньої діяльності;

– забезпечення аналізу виконання здобувачами вищої освіти навчального (робочих навчальних) планів освітньої програми, контролю якості викладання навчальних дисциплін у порядку та строки, визначені розпорядчими документами НА СБУ;

– моніторинг та періодичний перегляд освітньої програми на підставі змін законодавства у сфері освіти, інформаційної безпеки та кібербезпеки, а також пропозицій стейкхолдерів, здобувачів вищої освіти, інших учасників освітнього процесу;

– щорічне оцінювання здобувачів вищої освіти, науково-педагогічних співробітників (працівників) НА СБУ 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 за освітньою програмою, 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 (магістерських) роботах здобувачів вищої освіти;

– проведення інших процедур і заходів.

9. Вимоги професійних стандартів *(за наявності)*

Довідник кваліфікаційних характеристик професій працівників «Безпека господарської діяльності підприємства, установи, організації», погодженого Міністерством соціальної політики України, затвердженого і введеного в дію наказом Всеукраїнської організації Українського союзу промисловців і підприємців від 03.10.2011 № 99. – К. – 2011.

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

Закон України від 01.07.2014 № 1556-VII «Про вищу освіту»;

Закон України від 21.06.2018 № 2469-VIII «Про національну безпеку України»;

Закон України від 05/10/2017 № 2163- VIII «Про основні засади забезпечення кібербезпеки України»;

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);

постанова Кабінету Міністрів України від 29.04.2015 № 266 «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти»;

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);

Національний класифікатор України ДК 009: 2010 «Класифікація видів економічної діяльності»;

Національний класифікатор України ДК 003:2010 «Класифікатор професій»;

Довідник кваліфікаційних характеристик професій працівників «Безпека господарської діяльності підприємства, установи, організації», погодженого Міністерством соціальної політики України, затвердженого і введеного в дію наказом Всеукраїнської організації Українського союзу промисловців і підприємців від 03.10.2011 № 99. – К. – 2011.

Наказ Міністерства освіти і науки України від 01.06.2016 № 600 «Про затвердження та введення в дію Методичних рекомендацій щодо розроблення стандартів вищої освіти».

лист Міністерства освіти і науки України від 28.04.2017 № 1/9-239 «Щодо примірного зразка освітньо-професійної програми для першого (бакалаврського) та другого (магістерського) рівнів вищої освіти»;

лист Міністерства освіти і науки України від 05.06.2018 № 1/9-377 «Щодо надання роз’яснень стосовно освітніх програм»;

лист Міністерства освіти і науки України від 09.07.2018 № 1/9-434 «Щодо рекомендацій з навчально-методичного забезпечення»;

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»;

наказ Національної академії Служби безпеки України від 16.01.2016 № 20 (зі змінами) «Про затвердження Положення про екзаменаційну комісію Національної академії Служби безпеки України»;

наказ Національної академії Служби безпеки України від 06.12.2019 № 340 «Про затвердження Кодексу академічної доброчесності в Національній академії Служби безпеки України»;

Стандарти і рекомендації щодо забезпечення якості в Європейському просторі вищої освіти (ESG). - К.: ТОВ «ЦС», 2015. - 32 с.

ISO/IEC 27032:2012 Information technology — Security techniques — Guide-lines for cybersecurity, 50 p.

Cybersecurity: A Generic Reference Curriculum (RC). Dear Partners/NATO Members, 4500-1 (OSEM PED), Oct. 2016, 73 p.

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.

Керівник проєктної групи (гарант освітньої програми)