НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

ЗАТВЕРДЖЕНО
рішенням Вченої ради Національної академії Служби безпеки України від 29 вересня 2022 року, протокол № 12.

Ректор Національної академії СБ України
«28» жовтня 2022 року

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «КІБЕРЗАХИСТ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА КІБЕРПРОСТОРІ»

ДРУГОГО (МАГІСТЕРСЬКОГО) РІВНЯ ВИЩОЇ ОСВІТИ

галузь 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-2022

П Е Р Е Д М О В А

Оновлено у зв'язку із введенням у дію стандарту вищої освіти України зі спеціальності 256 Національна безпека (за окремими сферами забезпечення і видами діяльності), затвердженого наказом Міністерства освіти і науки України від 23.12.2021 року № 1423 «Про затвердження стандарту вищої освіти зі спеціальності 256 Національна безпека (за окремими сферами забезпечення і видами діяльності для другого (магістерського) рівня вищої світи».

Освітньо-професійна програма «Кіберзахист у сфері інформаційних технологій та кіберпросторі» вводиться у дію з 2022/2023 навчального року

Рецензії-відгуки зовнішніх стейкхолдерів:

Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони України.

Державна служба спеціального зв'язку та захисту інформації України.

Оновлено на підставі рішення, прийнятого на засіданні проєктної групи та групи забезпечення зі спеціальності 256 Національна безпека (за окремими сферами забезпечення і видами діяльності), спеціалізації 256.04 Національна безпека (кіберзахист, забезпечення державної безпеки в інформаційній сфері) 23 червня 2022 року.

Керівник проєктної групи

1. **Профіль освітньо-професійної програми** «Кіберзахист у сфері інформаційних технологій та кіберпросторі» за спеціальністю 256 Національна безпека (за окремими сферами забезпечення і видами діяльності), спеціалізацією 256.04 Національна безпека (кіберзахист, забезпечення державної безпеки в інформаційній сфері) для другого (магістерського) рівня вищої освіти

1 – Загальна інформація	
Повна назва закладу вищої освіти	Національна академія Служби безпеки України, Київ
Структурний підрозділ, відповідальний за реалізацію освітньо-професійної програми	Навчально-науковий інститут інформаційної безпеки та стратегічних комунікацій
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 освітньо-професійної програми	Кіберзахист у сфері інформаційних технологій та кіберпросторі
Тип диплому та обсяг освітньо-професійної програми	Диплом магістра, одиничний ступінь, 120 кредитів ЄКТС, 2 роки (денна форма навчання). 75% обсягу освітньо-професійної програми спрямовано на забезпечення загальних та спеціальних (фахових, предметних) компетентностей за спеціальністю, визначених Стандартом вищої освіти.
Наявність акредитації	Освітньо-професійна програма впроваджена з 2021 року, не акредитована.
Цикл / рівень	НРК України – 7 рівень, FQ-EHEA – другий цикл, QF-LLL – 7 рівень
Передумови	Наявність ступеня бакалавра або магістра (освітньо-кваліфікаційного рівня спеціаліста). Для вступників, які здобули рівень вищої освіти бакалавра за іншою спеціальністю, проводиться фахове вступне випробування, що передбачає перевірку набуття особою компетентностей та здатності продемонструвати результати навчання, визначені стандартом вищої освіти за спеціальністю 256 Національна безпека (за окремими сферами забезпечення і видами діяльності) для першого (бакалаврського) рівня вищої освіти.
Мова (и) викладання	Українська
Термін дії освітньо-професійної програми	5 років; оновлення освітньо-професійної програми (за потреби) на підставі змін

	законодавства у сфері освіти, пропозицій стекхолдерів, здобувачів вищої освіти, інших учасників освітнього процесу. Перегляд освітньо-професійної програми здійснюється щорічно відповідно до планових позицій НА СБ України
Інтернет-адреса постійного розміщення опису освітньо-професійної програми	www.academy.ssu.gov.ua (відповідно до умов і порядку, що визначаються нормативно-правовими актами Служби безпеки України).
2 – Мета освітньо-професійної програми	
Формування та розвиток у здобувачів вищої освіти професійних компетентностей до розв'язування задач дослідницького та інноваційного характеру у галузі національної безпеки (кіберзахист, забезпечення державної безпеки в інформаційній сфері) та організації і забезпечення кібербезпеки у сфері інформаційних технологій та кіберпросторі.	
3 – Характеристика освітньо-професійної програми	
Опис предметної області	Галузь 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). Міжнародна стандартна класифікація освіти: 1031 Military and defence. *Об'єкт вивчення* – національна безпека України в цілому та її сфери і види діяльності, реальні та потенційні загрози національній безпеці України; керівництво сектором безпеки і оборони України та його складовими; національні інтереси України у сфері кібербезпеки, заходи і засоби своєчасного виявлення, запобігання та нейтралізації загроз державній та кібербезпеці у сфері інформаційних технологій та кіберпросторі. *Цілі навчання* – підготовка професіонала, здатного розв'язувати задачі дослідницького та/або інноваційного характеру у сфері національної безпеки, виявляти та протидіяти загрозам національній безпеці України (кіберзахист, забезпечення державної безпеки в інформаційній сфері), здійснювати кіберзахист і забезпечення державної безпеки, провадити діяльність, пов'язану

	із кіберзахистом у сфері інформаційних технологій та кіберпросторі. *Теоретичний зміст предметної області* – основні закони, закономірності, категорії, поняття, принципи, методи і методики, які використовуються для забезпечення національної безпеки відповідно до компетенцій складових сектору безпеки і оборони України. *Методи, методики та технології* – сучасні цифрові технології, методи збирання, аналізу та захисту інформації, методи і технології забезпечення національної безпеки (кіберзахист, забезпечення державної безпеки в інформаційній сфері), методи організації кіберзахисту і забезпечення державної безпеки та кібербезпеки у сфері інформаційних технологій та кіберпросторі. *Інструменти та обладнання* – спеціалізоване програмне забезпечення, електронні бази даних; інтернет-ресурси; інструменти забезпечення національної безпеки (кіберзахист, забезпечення державної безпеки в інформаційній сфері) та організації кіберзахисту і забезпечення державної безпеки та кібербезпеки у сфері інформаційних технологій та кіберпросторі.
Орієнтація освітньо-професійної програми	Програма пропонує комплексний підхід до організації та застосування засобів кібербезпеки, як однієї з складових для здійснення кіберзахисту у сфері інформаційних технологій та кіберпросторі. Орієнтується на сучасні наукові дослідження в галузі кібербезпеки, враховує специфіку роботи підприємств різних форм власності у цьому напрямі; базується на апробованих практичних результатах із врахуванням сучасного стану та перспектив розвитку сфери кіберзахисту, орієнтує на подальшу професійну та наукову кар'єру.
Основний фокус освітньо-професійної програми та спеціалізації	Організаційно-технічні засоби та методи підтримки комплексу заходів для забезпечення державної безпеки в інформаційній сфері та впровадження діяльності, пов’язаної з кіберзахистом у сфері інформаційних технологій та

	кіберпростору.
Особливості освітньо-професійної програми	Програма розвиває перспективи професійної підготовки професіоналів з урахуванням специфічних особливостей забезпечення державної безпеки шляхом організації кіберзахисту у сфері інформаційних технологій та кіберпросторі.
4 – Придатність випускників до працевлаштування та подальшого навчання	
Придатність до працевлаштування	Випускники можуть бути працевлаштовані на керівних посадах структурних підрозділів центральних органів виконавчої влади, в органах управління стратегічного рівня сил оборони, органах управління сил безпеки. Професіонал підготовлений до діяльності відповідно до Міжнародної стандартної класифікації (ЮНЕСКО) за кодами: 103 Служби безпеки, спеціалізації 1031 Військова справа та оборона, а також відповідно до національного класифікатора ДК 003:2010 за кодом 2149.2 Професіонал з організації інформаційної безпеки.
Подальше навчання	Здобуття освітньо-наукового ступеня доктора філософії, здобуття додаткових кваліфікацій в системі освіти дорослих.
5 – Викладання та оцінювання	
Викладання та навчання	Студентоцентроване, проблемно-орієнтоване навчання, самонавчання, навчання через практику з використанням ситуаційних завдань та сучасних програмних засобів.
Оцінювання	Накопичувальна кредитно-модульна рейтингова система, що передбачає оцінювання студентів за усіма видами аудиторної та позааудиторної (самостійної, індивідуальної) навчальної діяльності, спрямовані на опанування навчального матеріалу з освітньо-професійної програми: поточний контроль, модульний, підсумковий контроль, письмові та усні диференційовані заліки й екзамени, тестування, реферати, презентації, проходження науково-дослідної практики, написання курсових робіт, підготовка та захист випускної кваліфікаційної (магістерської) роботи. Рівень досягнутих результатів навчання

	вимірюється у трьох системах оцінювання: 100-бальній, національній та за шкалою ЄКТС. Критерії та методи оцінювання розробляються кафедрами й визначаються в робочих програмах навчальних дисциплін.
6 – Програмні компетентності	
Інтегральна компетентність	Здатність розв'язувати задачі дослідницького та/або інноваційного характеру у галузі національної безпеки (кіберзахист, забезпечення державної безпеки в інформаційній сфері), провадити діяльність, пов'язану із кіберзахистом у сфері інформаційних технологій та кіберпросторі.
Загальні компетентності (ЗК)	ЗК 1. Здатність до абстрактного мислення, аналізу та синтезу. ЗК 2. Здатність приймати обґрунтовані рішення. ЗК 3. Здатність спілкуватися іноземною мовою. ЗК 4. Здатність проводити дослідження на відповідному рівні. ЗК 5. Усвідомлення рівних можливостей та гендерних проблем. ЗК 6. Здатність вчитися і оволодівати сучасними знаннями.
Спеціальні (фахові, предметні) компетентності (СК)	
Визначені Стандартом	СК 1. Здатність здійснювати професійну діяльність у відповідних сферах національної безпеки (кіберзахист, забезпечення державної безпеки в інформаційній сфері). СК 2. Здатність аналізувати та оцінювати сучасний стан і тенденції розвитку міжнародних відносин та проблеми міжнародної безпеки, їх вплив на національну безпеку в контексті набуття Україною членства в НАТО. СК 3. Здатність використовувати понятійно-категоріальний апарат теорії національної безпеки, аналізувати та розвивати структуру системи забезпечення національної безпеки та принципи її функціонування.

Керівник проєктної групи

	СК 4. Здатність аналізувати та прогнозувати розвиток безпекового середовища (глобальний, регіональний та національний аспекти) за окремими сферами забезпечення та видами діяльності (кіберзахист, забезпечення державної безпеки в інформаційній сфері). СК 5. Здатність організовувати цілеспрямовану діяльність щодо формування і реалізації державної політики у сферах національної безпеки та оборони. СК 6. Здатність організовувати заходи територіальної оборони, мобілізаційної підготовки та мобілізації у межах посадових обов'язків. СК 7. Здатність інтегрувати знання та розв'язувати складні задачі національної безпеки (кіберзахист, забезпечення державної безпеки в інформаційній сфері) у широких та/або мультидисциплінарних контекстах за наявності неповної або обмеженої інформації з урахуванням аспектів соціальної та етичної відповідальності.
Визначені НА СБУ	СК 8. Здатність використовувати відповідне програмне забезпечення (мови програмування, пакети) для реалізації загальних завдань протиборства в інформаційній сфері та спеціальних задач (операцій) у кіберпросторі. СК 9. Здатність вирішувати складні завдання і проблеми побудови інформаційно-комунікаційних систем та забезпечення їх безпеки в інформаційній сфері та кіберпросторі.
7 – Програмні результати навчання (ПРН)	
ПРН, визначені Стандартом вищої освіти спеціальності	ПРН 1. Застосовувати системний аналіз та синтез для вирішення завдань забезпечення національної безпеки. ПРН 2. Застосовувати вітчизняний та зарубіжний досвід забезпечення національної безпеки з урахуванням теорії національної безпеки під час здійснення професійної діяльності. ПРН 3. Приймати обґрунтовані рішення з питань забезпечення національної безпеки держави (кіберзахист,

	забезпечення державної безпеки в інформаційній сфері), у тому числі в умовах багатокритеріальності, неповних чи суперечливих інформації та вимог. ПРН 4. Організовувати роботу колективу, забезпечувати професійний розвиток його членів та досягнення поставлених цілей. ПРН 5. Розробляти та реалізовувати інноваційні проєкти у сфері національної безпеки з урахуванням правових, соціальних, економічних та етичних аспектів. ПРН 6. Вільно спілкуватися державною та іноземною мовами усно і письмово для обговорення професійної діяльності, результатів досліджень та інновацій, пошуку та аналізу відповідної інформації. ПРН 7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища. ПРН 8. Забезпечувати дотримання принципу гендерної рівності під час здійснення професійної діяльності. ПРН 9. Синтезувати спектр заходів та підходів, що можуть використовуватись для вирішення проблем, пов’язаних з викликами глобальній, європейській та регіональній безпеці. ПРН 10. Формувати елементи (складові) стратегії національної безпеки держави (за сферами забезпечення та видами діяльності) (кіберзахист, забезпечення державної безпеки в інформаційній сфері). ПРН 11. Застосовувати загальну методологію, спеціальні методи і технології для розв’язання професійних задач у визначених законодавством сферах та за напрямами майбутньої діяльності. ПРН 12. Застосовувати спеціалізовані концептуальні знання, що включають сучасні наукові здобутки і є основою для прийняття ефективних рішень, проведення досліджень та критичного осмислення проблем у галузі національної безпеки. ПРН 13. Організовувати та здійснювати

Керівник проєктної групи

	керівництво територіальною обороною, мобілізаційною підготовкою та мобілізацією у межах професійної компетентності. ПРН 14. Зрозуміло і недвозначно доносити власні знання, висновки та аргументацію з питань національної безпеки до фахівців і нефахівців, зокрема до осіб, які навчаються. ПРН 15. Управляти проведенням заходів у процесі забезпечення національної безпеки в різних умовах обстановки з використанням нових стратегічних підходів.
ПРН, визначені НА СБУ	ПРН 16. Організовувати та спрямовувати діяльність фахівців з кіберзахисту у сфері інформаційних технологій та кіберпросторі; розробляти та впроваджувати заходи із кіберзахисту у сфері інформаційних технологій та кіберпросторі, самостійно та у взаємодії з контролюючими органами. ПРН 17. Створювати та документально оформлювати організаційно-технічні та організаційно-правові моделі кіберзахисту, а також моделі захисту конфіденційності, організовувати та розробляти системи кіберзахисту у сфері інформаційних технологій та кіберпростору, здійснювати моніторинг та аудит інформаційної безпеки та кібербезпеки на підприємствах, установах та організаціях різних форм власності. ПРН 18. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення. ПРН 19. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного

	забезпечення. ПРН 20. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. ПРН 21. Досліджувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури ПРН 22. Оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації ПРН 23. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. ПРН 24. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. ПРН 25. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому. ПРН 26. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
8 – Ресурсне забезпечення реалізації 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 освітньо-професійної програми, підвищують свою кваліфікацію шляхом навчання за програмою підвищення кваліфікації та/або стажування у кількості не менше 180 годин протягом п’яти років.
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.
Інформаційне та навчально-методичне забезпечення	Використання традиційних та електронних інформаційних ресурсів загальної бібліотеки, авторських розробок 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 року №579
Навчання іноземних здобувачів вищої освіти	Відповідно до Правил прийому до НА СБУ на всі рівні вищої освіти приймаються виключно громадяни України

Керівник проєктної групи

2. Перелік компонентів освітньо-професійної програми та їх логічна послідовність

2.1. Загальна характеристика освітньо-професійної програми

№ з/п	Назва показника	Значення показника
1. Показники освітньо-професійної програми (*у кредитах ЄКТС/годинах*)		
1.1.	Загальний обсяг за весь термін навчання	120/3600
1.2.	Обсяг нормативної (обов'язкової) складової	90/2700
1.3.	Обсяг вибіркової складової для вільного вибору здобувачів вищої освіти	30/900
1.4.	Обсяг циклу загальної підготовки	17/510
1.5.	Обсяг циклу професійної підготовки	73/2190
2. Показники навчального навантаження здобувачів вищої освіти (*у кредитах ЄКТС/годинах*)		
2.1.	Обсяг по рокам навчання	
2.1.1.	1 рік навчання	60/1800
2.1.2.	2 рік навчання	60/1800
2.2.	Тижневе навантаження	
2.2.1.	максимальне	1 кр / 30
2.2.2.	мінімальне	0,56 кр / 17
3. Показник співвідношення між навчальними заняттями і годинами самостійної роботи здобувачів вищої освіти (*у кредитах ЄКТС/годинах*)		
3.1.	Обсяг навчальних занять	39,8/1196
3.2.	Обсяг самостійної роботи	80,1/2404
4. Загальні показники компонент освітньо-професійної програми		
4.1.	Мінімальний обсяг навчальної дисципліни (спецкурсу), (*у кредитах ЄКТС/годинах*)	2/60
4.2.	Максимальний обсяг навчальної дисципліни (спецкурсу), (*у кредитах ЄКТС/годинах*)	6/180
4.3.	Кількість обов'язкових освітніх компонентів	20
4.4.	Орієнтовна кількість навчальних дисциплін за вільним вибором здобувачів вищої освіти	7
4.5.	Вид (и) практичної підготовки *(тривалість у тижнях)*	
4.5.1.	Науково-дослідна практика	6
4.6.	Назва, форма атестації *(тривалість підготовки до неї в днях)*	
4.6.1.	Атестаційний іспит	5
4.6.2.	Випускна кваліфікаційна (магістерська) робота	5

5. Перелік компонентів освітньо-професійної програми

Код н/д	Компоненти освітньо-професійної програми (навчальні дисципліни, спецкурси, курсові роботи, практики, кваліфікаційна робота)	Кількість кредитів ЄКТС	Форма підсумкового контролю	Номер додатка до освітньо-професійної програми
Обов'язкові компоненти освітньо-професійної програми				
Цикл загальної підготовки				
ОК-1	Методологія наукових досліджень	4	диф. залік	додаток 1
ОК-2	Теорія прийняття рішень	4	диф. залік	додаток 2
ОК-3	Іноземна мова професійного спрямування	6	диф. залік, екзамен	додаток 3
ОК-4	Гендерна політика в системі національної безпеки та оборони України	3	диф. залік	додаток 4

Керівник проєктної групи

Цикл професійної підготовки				
ОК-5	Теорія кіберпростору, кібербезпеки та кіберзахисту	6	екзамен	додаток 5
ОК-6	Інформаційне протиборство	5	екзамен	додаток 6
ОК-7	Прикладні системи штучного інтелекту в кібербезпеці	2	диф. залік	додаток 7
ОК-8	Організаційно-правове забезпечення кіберзахисту	5	екзамен	додаток 8
ОК-9	Актуальні питання національної безпеки України	5	екзамен	додаток 9
ОК-10	Системи прийняття рішень та експертні системи протидії кіберзагрозам	2	диф. залік	додаток 10
ОК-11	Безпека інформаційно-комунікаційних систем	3	диф. залік	додаток 11
ОК-12	Безпека розподілених інформаційних ресурсів та хмарні обчислення	2	диф. залік	додаток 12
ОК-13	Організаційно-технічне моделювання кіберзахисту	6	екзамен	додаток 13
ОК-14	Телекомунікаційні системи передачі на об’єктах критичної інфраструктури	3	екзамен	додаток 14
ОК-15	Напрямні структури в телекомунікаційних мережах об’єктів критичної інфраструктури	3	диф. залік	додаток 15
ОК-16	Системи кіберзахисту у сфері інформаційних технологій та кіберпросторі	6	екзамен	додаток 16
ОК-17	Аудит інформаційної безпеки та кібербезпеки	6	екзамен, курсова робота	додаток 17
ОК-18	Територіальна оборона, мобілізаційна підготовка та мобілізація	4	екзамен	додаток 18
ОК-19	Науково-дослідна практика	9	диф. залік	додаток 19
ОК-20	Випускна кваліфікаційна (магістерська) робота	6	публічний захист	додаток 20
	Всього обов’язкові компоненти	90		
Вибіркові компоненти освітньо-професійної програми				
Дисципліни вільного вибору (формуються відповідно до переліку)		30		
Всього		120		

Керівник проєктної групи

2.2. Структурно-логічна схема освітньо-професійної програми

Складові освітньо-професійної програми	Цикли підготовки	1 курс		2 курс	
		1 семестр	2 семестр	3 семестр	4 семестр
Нормативна (обов'язкова) складова (у кредитах ЄКТС)	Загальної підготовки	Методологія наукових досліджень			Гендерна політика в системі національної безпеки та оборони України
		4 Екзамен			3 Диф. залік
			Іноземна мова професійного спрямування		
		2 Диф. залік	2 Диф. залік	2 Екзамен	
		Теорія прийняття рішень			
		4 Диф. залік			
	17	**10**	**2**	**2**	**3**
	Професійної (фахової) підготовки	Теорія кіберпростору, кібербезпеки та кіберзахисту	Актуальні питання національної безпеки України	Напрямні структури в телекомунікаційних мережах об'єктів критичної інфраструктури	Територіальна оборона, мобілізаційна підготовка та мобілізація
		6 Екзамен	5 Екзамен	3 Диф. залік	4 Екзамен
		Інформаційне протиборство	Системи прийняття рішень та експертні системи протидії кіберзагрозам	Системи кіберзахисту у сфері інформаційних технологій та кіберпросторі	Науково-дослідна практика
		5 Екзамен	2 Диф. залік	6 Екзамен	9 Диф. залік
		Прикладні системи штучного інтелекту в кібербезпеці	Безпека інформаційно-комунікаційних систем	Аудит інформаційної безпеки та кібербезпеки	Випускна кваліфікаційна (магістерська) робота
		2 Диф. залік	3 Диф. залік	6 Екзамен, курсова робота	6 Публічний захист
		Організаційно-провове забезпечення кіберзахисту	Безпека розподілених інформаційних ресурсів та хмарні обчислення		
		5 Екзамен	2 Диф. залік		
			Організаційно-технічне моделювання кіберзахисту		
			6 Екзамен		
			Телекомунікаційні системи передачі на об'єктах критичної інфрасруктури		
			3 Екзамен		
	73	**18**	**21**	**15**	**19**
Разом:	**90**	**28**	**23**	**17**	**22**
		Дисципліни вільного вибору			
	30		**9**	**13**	**8**
Разом	**120**	**28**	**32**	**30**	**30**

3. Форма атестації здобувачів вищої освіти

Форми атестації здобувачів вищої освіти	Атестація здобувачів вищої освіти здійснюється у формі атестаційного іспиту та публічного захисту випускної кваліфікаційної (магістерської) роботи
Вимоги до випускної кваліфікаційної (магістерської) роботи	Випускна кваліфікаційна (магістерська) робота повинна містити розв'язання актуальної наукової, технічної, службової або науково-методичної складної задачі, пов'язаної з аналізом (синтезом), моделюванням, дослідженням процесів (явищ), об'єктів, систем у галузі національної безпеки (кіберзахист, забезпечення державної безпеки в інформаційній сфері). Випускна кваліфікаційна (магістерська) робота не повинна містити академічного плагіату, фабрикації, фальсифікації. Роботи, які виконані не за спеціальними темами та не містять інформації з обмеженим доступом, оприлюднюються на офіційному сайті або в репозитарії закладу вищої освіти. Рішення щодо оприлюднення таких робіт приймається екзаменаційною комісією закладу вищої освіти із залученням представників режимно-секретного органу з дотриманням вимог законодавства України у сфері охорони державної таємниці.
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)
Вимоги до публічного захисту (демонстрації) (за наявності)	Визначаються Положенням про кваліфікаційні роботи здобувачів вищої освіти в Національній академії СБ України, затвердженим наказом НА СБУ від 01.11.2016 № 313

4. Матриця відповідності програмних компетентностей компонентам освітньо-професійної програми

Компоненти освітньо-професійної програми (ОК)	**Компетентності**															
	Інтегральна компетентність. Здатність розв'язувати задачі дослідницького та/або інноваційного характеру у галузі національної безпеки (кіберзахист, забезпечення державної безпеки в інформаційній сфері), провадити діяльність, пов'язану із кіберзахистом у сфері інформаційних технологій та кіберпросторі.															
	Шифр	**Загальні компетентності**						**Спеціальні (фахові, предметні) компетентності**								
		ЗК1	**ЗК2**	**ЗК3**	**ЗК4**	**ЗК5**	**ЗК6**	**СК1**	**СК2**	**СК3**	**СК4**	**СК5**	**СК6**	**СК7**	**СК8**	**СК9**
Методологія наукових досліджень	ОК-1	+	+		+		+									
Теорія прийняття рішень	ОК-2	+	+		+		+				+					+
Іноземна мова професійного спрямування	ОК-3			+	+		+		+							
Гендерна політика в системі національної безпеки та оборони України	ОК-4					+			+	+		+				
Теорія кіберпростору, кібербезпеки та кіберзахисту	ОК-5						+				+			+		
Інформаційне протиборство	ОК-6		+				+		+	+		+	+			
Прикладні системи штучного інтелекту в кібербезпеці	ОК-7		+		+			+			+				+	+
Організаційно-правове забезпечення кіберзахисту	ОК-8				+			+	+					+		+
Актуальні питання національної безпеки України	ОК-9						+	+	+	+		+		+		
Системи прийняття рішень та експертні системи протидії кіберзагрозам	ОК-10		+		+			+			+			+	+	+
Безпека інформаційно-комунікаційних систем	ОК-11							+			+			+	+	+
Безпека розподілених інформаційних ресурсів та хмарні обчислення	ОК-12							+			+			+	+	+
Організаційно-технічне моделювання кіберзахисту	ОК-13	+	+		+		+	+			+			+	+	+
Телекомунікаційні системи передачі на об'єктах критичної інфраструктури	ОК-14						+	+							+	+
Напрямні структури в телекомунікаційних мережах об'єктів критичної інфраструктури	ОК-15						+	+							+	+
Системи кіберзахисту у сфері інформаційних технологій та кіберпросторі	ОК-16				+			+	+			+		+	+	+
Аудит інформаційної безпеки та кібербезпеки	ОК-17				+			+	+		+			+	+	+
Територіальна оборона, мобілізаційна підготовка та мобілізація	ОК-18		+				+			+	+	+	+			

Компоненти освітньо-професійної програми (ОК)	**Компетентності**														
	Інтегральна компетентність. Здатність розв'язувати задачі дослідницького та/або інноваційного характеру у галузі національної безпеки (кіберзахист, забезпечення державної безпеки в інформаційній сфері), провадити діяльність, пов'язану із кіберзахистом у сфері інформаційних технологій та кіберпросторі.														
	Шифр	**Загальні компетентності**						**Спеціальні (фахові, предметні) компетентності**								
		ЗК1	**ЗК2**	**ЗК3**	**ЗК4**	**ЗК5**	**ЗК6**	**СК1**	**СК2**	**СК3**	**СК4**	**СК5**	**СК6**	**СК7**	**СК8**	**СК9**
Науково-дослідна практика	ОК-19	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Випускна кваліфікаційна (магістерська) робота	ОК-20	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

Керівник проєктної групи

Матриця відповідності визначених Стандартом та освітньо-професійною програмою компетентностей дескрипторам Національної рамки кваліфікацій

Класифікація компетентностей (результатів навчання) за НРК	**Знання 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, критичне осмислення проблем у галузі та на межі галузей знань	**Уміння/навички** **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.	**Комунікація К1** Зрозуміле і недвозначне донесення власних знань, висновків та аргументації до фахівців і нефахівців, зокрема, до осіб, які навчаються	**Відповідальність та автономія** **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.
Інтегральна компетентність. Здатність розв'язувати задачі дослідницького та/або інноваційного характеру у галузі національної безпеки (кіберзахист, забезпечення державної безпеки в інформаційній сфері), провадити діяльність, пов'язану із кіберзахистом у сфері інформаційних технологій та кіберпросторі.				
Загальні компетентності				
ЗК1	Зн1	Ум3	К1	
ЗК2	Зн1	Ум2		АВ2
ЗК3				АВ3
ЗК4	Зн1	Ум1	К1	АВ1
ЗК5			К1	
ЗК6	Зн1	Ум2	К1	
Спеціальні (фахові, предметні) компетентності				
СК1	Зн1	Ум2	К1	АВ2
СК2	Зн1	Ум2	К1	АВ2

Керівник проєктної групи

СК3	Зн1	Ум3	К1	АВ1
СК4	Зн1	Ум3	К1	АВ1
СК5	Зн1		К1	АВ1
СК6	Зн1	Ум1	К1	АВ3
СК7	Зн1	Ум2	К1	АВ1
СК8	Зн1	Ум2	К1	АВ1
СК9	Зн1	Ум3	К1	АВ1

Керівник проєктної групи

Матриця відповідності визначених Стандартом та ОПП результатів навчання та компетентностей

Результати навчання	Компетентності															
	Інтегральна компетентність	Загальні компетентності						Спеціальні (фахові, предметні) компетентності								
		ЗК1	ЗК2	ЗК3	ЗК4	ЗК5	ЗК6	СК1	СК2	СК3	СК4	СК5	СК6	СК7	СК8	СК9
ПРН1	Здатність розв'язувати задачі дослідницького та/або інноваційного характеру у галузі національної безпеки (кіберзахист, забезпечення державної безпеки в інформаційній сфері), провадити діяльність, пов'язану із кіберзахистом у сфері інформаційних технологій та кіберпросторі	+			+						+			+	+	+
ПРН2			+						+			+		+	+	+
ПРН3			+			+		+		+						
ПРН4						+	+					+			+	+
ПРН5					+									+		
ПРН6				+												
ПРН7					+						+			+		
ПРН8		+				+	+	+	+						+	+
ПРН9						+									+	+
ПРН10											+				+	+
ПРН11			+							+					+	
ПРН12					+			+						+		+
ПРН13													+			
ПРН14		+	+		+		+							+	+	+
ПРН15			+							+				+		
ПРН16			+					+						+	+	+
ПРН17					+		+							+	+	+
ПРН18											+			+	+	+
ПРН19										+				+	+	+
ПРН20								+						+	+	+
ПРН21									+					+	+	+
ПРН22														+	+	+
ПРН23										+				+	+	+
ПРН24								+						+	+	+
ПРН25										+				+	+	+
ПРН26									+					+	+	+

Керівник проєктної групи

5. Матриця забезпечення програмних результатів навчання відповідними компонентами освітньо-професійної програми

Шифри результатів навчання			ПРН 1	ПРН 2	ПРН 3	ПРН 4	ПРН 5	ПРН 6	ПРН 7	ПРН 8	ПРН 9	ПРН 10	ПРН 11	ПРН 12	ПРН 13	ПРН 14	ПРН 15	ПРН 16	ПРН 17	ПРН 18	ПРН 19	ПРН 20	ПРН 21	ПРН 22	ПРН 23	ПРН 24	ПРН 25	ПРН 26
№ з/п	Повна назва освітнього компонента	Шифр																										
Освітні компоненти (далі – ОК)																												
1.	Методологія наукових досліджень	ОК-1	+				+		+				+			+			+									
2.	Теорія прийняття рішень	ОК-2	+		+	+			+				+				+	+		+								
3.	Іноземна мова професійного спрямування	ОК-3					+	+								+												
4.	Гендерна політика в системі національної безпеки та оборони України	ОК-4				+				+							+											
5.	Теорія кіберпростору, кібербезпеки та кіберзахисту	ОК-5	+						+			+						+	+								+	
6.	Інформаційне протиборство	ОК-6		+	+		+			+			+		+		+	+				+				+		
7.	Прикладні системи штучного інтелекту в кібербезпеці	ОК-7	+									+		+			+				+	+						+
8.	Організаційно-правове забезпечення кіберзахисту	ОК-8	+	+			+		+		+	+	+				+		+			+					+	+
9.	Актуальні питання національної безпеки України	ОК-9		+	+		+		+							+		+				+			+			
10.	Системи прийняття рішень та експертні системи протидії кіберзагрозам	ОК-10	+		+	+			+		+	+	+	+			+			+	+			+		+		
11.	Безпека інформаційно-комунікаційних систем	ОК-11	+						+		+									+			+		+	+		
12.	Безпека розподілених інформаційних ресурсів та хмарні обчислення	ОК-12	+						+		+									+			+		+	+		
13.	Організаційно-технічне моделювання кіберзахисту	ОК-13	+				+				+	+	+	+			+		+	+	+	+						+
14.	Телекомунікаційні системи передачі на об’єктах критичної інфраструктури	ОК-14												+			+				+		+					

Керівник проєктної групи

Шифри результатів навчання			ПРН 1	ПРН 2	ПРН 3	ПРН 4	ПРН 5	ПРН 6	ПРН 7	ПРН 8	ПРН 9	ПРН 10	ПРН 11	ПРН 12	ПРН 13	ПРН 14	ПРН 15	ПРН 16	ПРН 17	ПРН 18	ПРН 19	ПРН 20	ПРН 21	ПРН 22	ПРН 23	ПРН 24	ПРН 25	ПРН 26
№ з/п	Повна назва освітнього компонента	Шифр																										
15.	Напрямні структури в телекомунікаційних мережах об’єктів критичної інфраструктури	ОК-15												+			+				+		+					
16.	Системи кіберзахисту у сфері інформаційних технологій та кіберпросторі	ОК-16	+		+		+		+					+									+		+			
17.	Аудит інформаційної безпеки та кібербезпеки	ОК-17	+	+		+			+								+				+		+				+	
18.	Територіальна оборона, мобілізаційна підготовка та мобілізація	ОК-18			+							+			+	+				+								
19.	Науково-дослідна практика	ОК-19	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
20.	Випускна кваліфікаційна (магістерська) робота	ОК-20	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

Керівник проєктної групи

6. Система забезпечення якості вищої освіти за освітньо-професійною програмою передбачає:

– 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 відповідних складових освітньої діяльності;

– забезпечення аналізу виконання здобувачами освіти навчального (індивідуальних навчальних) планів освітньої програми, контролю за якістю викладання навчальних дисциплін у порядку та строки, визначені розпорядчими документами Національної академії СБ України;

– здійснення моніторингу та періодичного перегляду освітньої програми;

– 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 підвищення кваліфікації науково-педагогічних співробітників (працівників) Національної академії СБ України;

– забезпечення наявності необхідних ресурсів для організації освітнього процесу, у тому числі самостійної роботи здобувачів освіти, за освітньою програмою;

– забезпечення наявності інформаційних систем для ефективного управління освітнім процесом;

– забезпечення публічності інформації про освітню програму з урахуванням вимог нормативно-правових актів СБ України, ступінь вищої освіти та кваліфікації (освітню, професійну, у документі про освіту);

– забезпечення ефективної системи запобігання та виявлення академічного плагіату у наукових працях співробітників (працівників) Національної академії СБ України і здобувачів освіти;

– здійснення інших процедур і заходів.

7. 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.

Довідник типових професійно-кваліфікаційних характеристик основних посад керівників та інших працівників режимно-секретних органів органів державної влади, органів місцевого самоврядування, підприємств, установ і організацій.

8. Додаткові вимоги до організації освітнього процесу для освітніх програм з підготовки фахівців для професій, для яких запроваджене додаткове регулювання (за необхідності)

Відсутні

9. Перелік нормативних, розпорядчих, інструктивних документів, на яких базується освітньо-професійна програма:

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

– Постанова Кабінету Міністрів України від 23.11.2011 № 1341 «Про затвердження Національної рамки кваліфікацій»;

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

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

– Наказ Президента України №392/2020 Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»;

– Наказ Президента України №447/2021 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»;

– Національний класифікатор України «Класифікатор професій», ДК003:2010 затверджений наказом Держспоживстандарту України від 28.07.2010 № 237 (із змінами);

– Наказ Центрального управління Служби безпеки України від 04.07.2017 № 410 «Про затвердження виду діяльності (спеціалізації) спеціальності 256 «Національна безпека (за окремими сферами забезпечення і видами діяльності)»;

– Наказ Центрального управління Служби безпеки України від 19.05.2021 № 169 «Про внесення змін до наказу Центрального управління Служби безпеки України від 04.07.2017 № 410»;

– Наказ Міністерства освіти і науки України від 01.06.2016 № 600 «Про затвердження та введення в дію Методичних рекомендацій щодо розроблення стандартів вищої освіти» (у редакції наказу Міністерства освіти і науки України від 30.04.2020 р. № 584);

– 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;

– Положення про організацію освітнього процесу в Національній академії Служби безпеки України, затверджено наказом НА СБУ від 31.08.2015 № 234 (зі змінами);

– Європейська кредитна трансферно-накопичувальна система: довідник користувача / пер. з англ.; за ред. д.т.н., проф. Ю.М. Рашкевича та д. пед.н., доц. Ж.В. Таланової. – Львів: Видавництво Львівської політехніки, 2015. – 106 с.;

Керівник проєктної групи

– 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.;

– Національний освітній глосарій: вища освіта 2014;

– Проект Європейської Комісії «Гармонізація освітніх структур в Європі» (Tuning Educational Structures in Europe, TUNING);

– TUNING (для ознайомлення зі спеціальними (фаховими) компетентностями та прикладами стандартів);

– Рашкевич Ю.М. Болонський процес та нова парадигма вищої освіти;

– Розвиток системи забезпечення якості вищої освіти в Україні: інформаційно-аналітичний огляд, 2015;

– Стандарти і рекомендації щодо забезпечення якості в Європейському просторі вищої освіти (ESG), 2015.

– EQF 2017 (Європейська рамка кваліфікацій) // URL: https://ec.europa.eu/ploteus/sites/eac-eqf/files/en.pdf; https://ec.europa.eu/ploteus/content/descriptors-page

– QF EHEA 2018 (Рамка кваліфікацій ЄПВО) // URL: http://www.ehea.info/Upload/document/ministerial_declarations/EHEAParis2018_Com munique_AppendixIII_952778.pdf

– ISCED (Міжнародна стандартна класифікація освіти, МСКО) 2011 // URL: http://uis.unesco.org/sites/default/files/documents/international-standardclassificatio-of-education-isced-2011-en.pdf.

– ISCED-F (Міжнародна стандартна класифікація освіти – Галузі, МСКОГ) 2013 // URL: http://uis.unesco.org/sites/default/files/documents/internationalstandard-classification-of-education-fields-of-education-and-training-2013-detailedfield-descriptions-2015-en.pdf

Керівник проєктної групи