

Державна політика України у сфері забезпечення інформаційної безпеки людини, суспільства, держави

identity, statehood, and guaranteeing security as the foundation of quality life for individuals, society, and the state.

Based on the results of the study, using content analysis, descriptive, and axiological methods, it has been concluded that Ukrainian language law can serve as a tool for regulating the language sphere and providing mechanisms for achieving national security.

Key words: *English language, security discourse, official language, language policy, language law, language planning, national security, legal discourse.*

DOI: 10.51369/2707-7276-2025-1(38)-2

УДК 355.233.2:355.45:007

ДОРОШЕНКО Тетяна Володимирівна

ORCID ID: 0000-0003-4873-7119

РЕАЛІЇ ТА ПЕРСПЕКТИВИ ПІДГОТОВКИ ФАХІВЦІВ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ ДЛЯ ПІДРОЗДІЛІВ ЗА НАПРЯМОМ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ ДІЯЛЬНОСТІ

У статті досліджуються особливості підготовки фахівців підрозділів Служби безпеки України, які працюють за напрямом інформаційно-аналітичної діяльності. В умовах сучасного світу, де інформаційна безпека набуває критичного значення, зростає роль інформаційної протидії, психологічних та інформаційних операцій як інструментів забезпечення національної безпеки. З урахуванням цих аспектів аналізуються сучасні підходи до професійної підготовки кадрів СБ України, освітні програми й тренінги, а також вимоги до фахівців СБУ, які працюють в інформаційно-аналітичній сфері.

Виявлено ключові проблеми, зокрема недостатність уваги до практичного навчання, розвитку етичних і психологічних аспектів підготовки фахівців для інформаційно-аналітичної сфери, використання сучасних технологій аналізу даних, застарілість технічного оснащення.

Проведено порівняльний аналіз систем підготовки кадрів у різних країнах, який демонструє можливості використання передового міжнародного досвіду в Україні в контексті забезпечення ефективності інформаційно-аналітичної діяльності.

Результати дослідження, проведеного з використанням комплексного методологічного підходу, свідчать про необхідність удосконалення освітніх програм, ураховуючи останні тенденції у сфері інформаційних технологій та аналітики й сучасні виклики інформаційній безпеці. Вказується на важливість зміцнення кадрового потенціалу СБ України. Рекомендації включають посилення координації між різними відомствами, розвиток міжнародної співпраці та впровадження нових методів навчання з урахуванням сучасних технологій і методик.

© Дорошенко Т. В., 2025

State policy of Ukraine in the field of ensuring information security of person, society and the state

Ключові слова: інформаційна протидія, інформаційні та психологічні операції, інформаційно-аналітична діяльність СБУ, компетенції співробітників.

Постановка проблеми. На сучасному етапі, коли перед державою постають нові виклики та загрози, особливо важливого значення набуває інформаційно-аналітична діяльність як складова національної безпеки. Служба безпеки України відіграє ключову роль у забезпеченні захисту державних інтересів, зокрема в інформаційній сфері. Однак в умовах розвитку технологій, поширення кіберзагроз та ускладнення геополітичної ситуації виникає потреба у підвищенні кваліфікації та спеціалізації фахівців СБ України, відповідальних за інформаційно-аналітичну діяльність.

Сучасна інформаційно-аналітична діяльність потребує від фахівців не тільки глибоких знань у сфері інформаційних технологій та аналізу даних, але й високого рівня професійної підготовки в питаннях забезпечення інформаційної безпеки. У цьому контексті особливо актуальною є підготовка спеціалістів, здатних оперативно реагувати на нові загрози, ефективно використовувати аналітичні методи й інструменти, а також працювати конфіденційно та з високою відповідальністю.

Основною проблемою є недостатня адаптація освітніх програм до сучасних вимог і викликів, що виникають у сфері інформаційної безпеки. Крім того, наявна обмежена кількість досліджень і науково-методичних розробок, присвячених саме підготовці фахівців для інформаційно-аналітичних підрозділів СБ України. Важливо врахувати особливості діяльності цих

підрозділів і специфіку роботи з конфіденційною інформацією.

Отже, об'єктом дослідження є підготовка фахівців СБ України у сфері інформаційно-аналітичної діяльності, а предметом – особливості освітніх програм, методів навчання та професійної підготовки.

Аналіз останніх досліджень і публікацій. Підготовка фахівців для інформаційно-аналітичної діяльності в правоохоронних органах, зокрема в Службі безпеки України, є важливою темою дослідження.

У роботі [1] акцентується на важливості адаптації навчальних програм для підготовки фахівців у сфері кібербезпеки, ураховуючи швидкий розвиток технологій і збільшення кіберзагроз. На думку автора, необхідно постійно оновлювати навчальні матеріали та практичні завдання, щоби забезпечити відповідність сучасним викликам.

У статті [2] А. Мовчан розглядає роль інформаційного аналізу в контексті національної безпеки та важливість відповідної підготовки фахівців. Автор зазначає, що ефективний аналіз інформації потребує не тільки технічних знань, але й розвинених аналітичних навичок. Висновки дослідження підтверджують необхідність створення спеціалізованих курсів і тренінгів для підвищення кваліфікації кадрів.

У дослідженні [3] Ю. Саричев порівнює освітні програми з інформаційної безпеки в різних країнах і доходить висновку, що успішні програми включають не лише технічні аспекти,

Державна політика України у сфері забезпечення інформаційної безпеки людини, суспільства, держави

але й навчання з питань етики та правового регулювання. Аналіз міжнародного досвіду виявив, що інтеграція міждисциплінарного підходу є ключовою для ефективної підготовки фахівців.

У роботі [4] розглянуто психологічні виклики, з якими стикаються фахівці, які працюють із конфіденційною інформацією. Автори наголошують на важливості розвитку стресостійкості й емоційної стабільності, необхідності включення психологічної підготовки в освітні програми для спеціалістів СБ України.

У дослідженні [5] О. Манжай аналізує освітні програми з підготовки фахівців у сфері інформаційної безпеки та їхню відповідність сучасним потребам. Автор вважає, що через недостатню гнучкість програм неможливо вчасно реагувати на нові виклики. У висновках рекомендується впровадження адаптивних навчальних програм, що швидко оновлюються відповідно до змін у сфері безпеки.

Аналіз літератури показує, що хоча багато аспектів підготовки фахівців з інформаційно-аналітичної діяльності вже досліджено, залишаються кілька ключових проблем. Зокрема це:

– відсутність стандартизованих освітніх програм, які б ураховували специфіку роботи з конфіденційною інформацією та кіберзагрозами;

– недостатня увага до практичного аспекту навчання, що включає симуляції та тренування в реальних умовах;

– необхідність упровадження інтерактивних методів навчання та но-

вітніх технологій, які дають можливість адаптуватися до швидко змінюваного інформаційного середовища;

– потреба в більшій кількості досліджень щодо психологічних аспектів роботи фахівців у сфері інформаційної безпеки, зокрема стресостійкості та морально-етичних питань.

Ця стаття має на меті заповнити деякі з цих прогалин, пропонуючи нові підходи та рекомендації щодо вдосконалення підготовки фахівців СБ України для інформаційно-аналітичної діяльності.

Метою статті є дослідження та аналіз сучасних підходів до професійної підготовки кадрів Служби безпеки України, які спеціалізуються на інформаційно-аналітичній діяльності, виявлення актуальних викликів у цій сфері, визначення ключових компетенцій, потрібних для ефективної роботи, та розроблення рекомендацій щодо вдосконалення освітніх програм і тренінгів для підвищення кваліфікації співробітників з урахуванням сучасних тенденцій у сфері національної безпеки й інформаційного аналізу, а також необхідності адаптації міжнародного досвіду до українських реалій.

Виклад основного матеріалу. Інформаційно-аналітична діяльність є ключовим елементом у системі національної безпеки, зокрема в роботі таких органів як Служба безпеки України. Вона полягає у збиранні, обробленні, аналізі й інтерпретації даних для прийняття обґрунтованих рішень на різних рівнях управління. Ця діяльність охоплює широкий спектр завдань – від моніторингу й оцінювання

State policy of Ukraine in the field of ensuring information security of person, society and the state

поточних загроз до прогнозування майбутніх викликів.

Інформаційно-аналітична діяльність (ІАД) базується на використанні спеціалізованих методів та інструментів, що дають можливість ефективно обробляти великі обсяги даних, виділяючи з них критично важливу інформацію. ІАД здійснюється як на стратегічному, так і тактичному рівнях, забезпечуючи керівництво актуальною та достовірною інформацією.

Значення ІАД у сучасних умовах важко переоцінити. Коли відбувається глобалізація, зростають швидкість передачі інформації та обсяги даних, здатність точно й швидко аналізувати інформацію стає критично важливою. У контексті національної безпеки, інформаційно-аналітична діяльність сприяє [1–7]:

- виявленню загроз – постійний моніторинг та аналіз інформації дають змогу ідентифікувати потенційні загрози, включаючи терористичні акти, кіберзагрози, економічну нестабільність тощо;

- прогнозуванню розвитку ситуації – аналітичні методи дають можливість моделювати сценарії розвитку подій, що сприяє ефективному плануванню та підготовці до різних ситуацій;

- підтримці прийняття рішень – надання керівництву чіткої та обґрунтованої інформації забезпечує прийняття своєчасних та ефективних рішень, що є критично важливим в умовах кризових ситуацій;

- оцінюванню ефективності заходів – аналіз даних дає змогу оцінювати ефективність уже вжитих заходів і коригувати стратегії у відповідності до нових даних.

У Службі безпеки України ІАД займає центральне місце, забезпечуючи оперативне реагування на загрози державній безпеці. Фахівці з інформаційно-аналітичної діяльності СБ України використовують широкий спектр методів, включаючи кіберрозвідку, аналіз відкритих джерел, соціально-політичний моніторинг та інші. Особлива увага приділяється розвитку навичок аналітичного мислення та використанню сучасних інформаційних технологій, що забезпечують високу якість та оперативність аналізу.

Отже, інформаційно-аналітична діяльність є невід’ємною частиною забезпечення національної безпеки й ефективного управління державою. Вона дає можливість адаптуватися до швидко змінюваних умов і забезпечує інформаційний супровід усіх ключових процесів, що стосуються безпеки держави та суспільства.

Підготовка фахівців Служби безпеки України в інформаційно-аналітичній сфері є складним і багатоступеневим процесом, який включає базову освіту, спеціалізоване навчання та постійне підвищення кваліфікації. Цей процес покликаний забезпечити підготовку висококваліфікованих аналітиків, здатних ефективно виконувати завдання в умовах зростаючих викликів у сфері національної безпеки. Можна виділити такі етапи цього процесу:

1. Базова освіта для фахівців інформаційно-аналітичної діяльності СБУ – здебільшого надається у профільних вищих навчальних закладах, таких як Національна академія Служби безпеки України. Навчальні програми включають вивчення основ ін-

Державна політика України у сфері забезпечення інформаційної безпеки людини, суспільства, держави

формаційної безпеки, аналітичних методів, кібербезпеки, управління ризиками, а також правових аспектів діяльності СБ України.

Програми базової освіти націлені на формування базових знань і навичок, необхідних для роботи в аналітичних підрозділах. Студенти отримують ґрунтовну теоретичну підготовку, а також практичні навички з використання сучасних інформаційних технологій і методів аналізу даних.

2. Спеціалізоване навчання фахівців – здійснюється через участь у програмах підвищення кваліфікації, курсах і тренінгах, організованих як у межах СБ України, так і у співпраці з іншими державними та міжнародними організаціями. Ці програми охоплюють такі аспекти, як:

– аналітичні методи та технології – фокус на сучасні підходи до збирання, оброблення й аналізу великих обсягів даних, включаючи використання штучного інтелекту та машинного навчання;

– інформаційна та кібербезпека – поглиблене вивчення захисту інформації та кіберпростору, що включає аспекти захисту даних, мережевої безпеки та протидії кіберзагрозам;

– соціально-політичний аналіз – навчання методам аналізу соціально-політичної обстановки, включаючи аналіз відкритих джерел, соціальних медіа та інших ресурсів для прогнозування та оцінювання ризиків.

3. Постійне підвищення кваліфікації. Фахівці СБ України постійно залучаються до програм підвищення

кваліфікації, що спрямовані на підтримання високого рівня професійної компетентності. Це включає участь у семінарах, конференціях, а також проходження онлайн-курсів і тренінгів. Такі заходи дають можливість фахівцям бути в курсі останніх тенденцій у сфері інформаційної безпеки й аналітики, а також удосконалювати свої навички.

4. Співпраця з міжнародними організаціями. Служба безпеки України активно співпрацює з міжнародними партнерами, такими як Європейський Союз, НАТО, а також національними органами безпеки інших країн. Це дає змогу переймати кращі практики та методики, отримувати доступ до передових технологій і підходів у сфері інформаційно-аналітичної діяльності.

Отже, сучасний стан підготовки фахівців СБ України в інформаційно-аналітичній сфері характеризується комплексністю та системністю. Однак в умовах постійно змінюваних загроз і викликів необхідним є вдосконалення освітніх програм і підвищення кваліфікації фахівців для забезпечення їхньої готовності до ефективної роботи.

В умовах гібридної війни, кібератак, інформаційних операцій та інших асиметричних складних і швидкозмінних загроз вимоги до професійних якостей і компетенцій співробітників СБ України значно зросли. Основні вимоги до фахівців СБ України в цьому контексті наведені в таблиці 1 (складена авторкою на основі [5–8]).

State policy of Ukraine in the field of ensuring information security of person, society and the state

Таблиця 1 – Основні вимоги до фахівців СБ України
в інформаційно-аналітичній сфері

Вимоги	Характеристика
Висока професійна компетентність	Фахівці СБУ повинні мати глибокі знання та практичні навички у своїй галузі діяльності. Це включає знання законодавства, методів інформаційно-аналітичної роботи, кібербезпеки, контррозвідки, протидії тероризму тощо. Особливо важливою є здатність швидко адаптуватися до нових технологій та методів роботи.
Аналіз і критичне мислення	Фахівці мають бути здатні до глибокого аналізу інформації, критичного оцінювання джерел і виявлення загроз. Це включає навички аналітичного мислення, здатність розпізнавати фейкові новини, маніпуляції в інформаційному просторі й інші форми інформаційного впливу.
Кібербезпека і технічна грамотність	З огляду на зростання кількості кіберзагроз фахівці СБУ повинні бути добре обізнані з аспектами кібербезпеки, включаючи захист інформаційних систем, реагування на кіберінциденти й аналіз кіберзагроз. Володіння сучасними інформаційними технологіями є критично важливим.
Етичні та моральні якості	Етична відповідальність та моральна стійкість є ключовими вимогами до фахівців СБУ. У своїй роботі вони повинні дотримуватися законності, поваги до прав людини й етичних норм, зокрема в умовах протидії гібридним загрозам і проведення оперативних заходів.
Комунікаційні навички	Ефективна комунікація, уміння працювати в команді, а також здатність до переконливого донесення інформації є важливими аспектами роботи фахівців СБУ. Це включає не лише внутрішні комунікації, але й роботу з громадськістю, міжнародними партнерами й іншими органами.
Психологічна стійкість	Робота в умовах постійного стресу, високої відповідальності та загроз потребує від фахівців СБУ психологічної стійкості. Важливими є навички управління стресом, уміння зберігати спокій і концентрацію в критичних ситуаціях.
Міжнародний досвід і знання мов	Знання іноземних мов, зокрема англійської, є важливим для співпраці з міжнародними партнерами, участі в міжнародних програмах обміну досвідом і доступу до міжнародних джерел інформації. Фахівці повинні бути обізнані з міжнародними стандартами та практиками у сфері безпеки.
Гнучкість і адаптивність	Фахівці СБУ повинні бути здатні швидко адаптуватися до змін у середовищі безпеки, бути готовими до нових викликів і завдань. Це включає готовність до постійного навчання, саморозвитку та освоєння нових методів роботи.

Державна політика України у сфері забезпечення інформаційної безпеки людини, суспільства, держави

Отже, для протистояння сучасним викликам фахівцям СБ України потрібні: високий рівень професіоналізму, широкий спектр знань і навичок, а також етична відповідальність. Для досягнення цього необхідні: постійне підвищення кваліфікації, запровадження нових освітніх програм і

тренінгів, підтримка високих стандартів професійної діяльності. Особливо важливими є психологічні й етичні аспекти підготовки, які забезпечують готовність співробітників діяти ефективно в умовах стресу та зберігати високі моральні стандарти (див. табл. 2 (складена авторкою на основі [5–9])).

Таблиця 2 – Характеристика психологічних та етичних аспектів підготовки фахівців в інформаційно-аналітичній сфері

Психологічні аспекти підготовки	Етичні аспекти підготовки
<p>1. Розвиток стресостійкості.</p> <p>Співробітники СБУ, зокрема в інформаційно-аналітичній сфері, часто стикаються з високим рівнем стресу, зумовленим роботою з великими обсягами інформації, аналізом загроз, участю в оперативних заходах і конфліктних ситуаціях. Тому одним із важливих напрямів підготовки є розвиток стресостійкості. Це включає тренінги з управління стресом, техніки релаксації, а також навчання методам швидкого прийняття рішень у кризових ситуаціях.</p>	<p>1. Дотримання етичних стандартів.</p> <p>Фахівці СБУ повинні діяти відповідно до високих етичних стандартів, забезпечуючи дотримання законодавства, прав людини й етичних норм у своїй діяльності. Навчання включає розгляд етичних дилем, розуміння моральних принципів, якими керуються в професійній діяльності, та їх застосування на практиці.</p>
<p>2. Підготовка до роботи в умовах невизначеності.</p> <p>Умови гібридної війни, зростання кіберзагроз та інформаційних атак потребують від співробітників здатності працювати в умовах невизначеності та швидко адаптуватися до нових обставин. Психологічна підготовка включає розвиток когнітивної гнучкості, здатності до багатозадачності й опрацювання великої кількості інформації.</p>	<p>2. Повага до конфіденційності й особистих даних.</p> <p>У роботі з інформацією особливо важливим є дотримання норм конфіденційності та захисту особистих даних. Це включає навчання правильному поведженню з чутливою інформацією, розумінню правових аспектів обробки даних і дотримання норм інформаційної безпеки.</p>
<p>3. Психологічна підтримка.</p> <p>Важливою частиною підготовки є забезпечення постійної психологічної підтримки співробітників. Це включає доступ до консультацій психологів, програми емоційного благополуччя, а також створення підтримуючого робочого середовища, яке сприяє зниженню емоційного вигорання.</p>	<p>3. Запобігання конфлікту інтересів.</p> <p>Співробітники СБУ повинні вміти розпізнавати й уникати конфлікту інтересів у своїй діяльності. Це забезпечує неупередженість та об'єктивність у прийнятті рішень, а також запобігає можливості зловживання службовим становищем.</p>

State policy of Ukraine in the field of ensuring information security of person, society and the state

Різні країни розробили свої підходи до підготовки кадрів для інформаційно-аналітичних підрозділів. Розглянемо деякі з них детальніше (див. табл. 3 (складена авторкою на основі [4–10])).

Таблиця 3 – Підходи до підготовки кадрів для інформаційно-аналітичних підрозділів у різних країнах світу

Країна	Основні установи	Навчальні програми	Базові особливості
США	Військова академія США, АНБ, приватні компанії (Google, IBM)	Інформаційна безпека, кібербезпека, стратегічний аналіз	Розвинена система навчання, включаючи військові академії та приватний сектор; акцент на кібербезпеці та стратегічному аналізі
Велика Британія	Національна академія кібербезпеки (NCSC), університети	Кіберрозвідка, аналіз загроз, кіберзахист	Інтеграція між державними установами й університетами, акцент на кібербезпеці
Німеччина	Федеральне відомство з інформаційної безпеки (BSI), технічні університети	Кібербезпека, захист критичної інфраструктури	Технічна орієнтація, сильна база в кібербезпеці та технічній освіті
Ізраїль	Армійські підрозділи, Техніон	Кібербезпека, розвідка, інформаційний аналіз	Унікальний підхід через військову службу, висока концентрація на кібербезпеці та розвідці
Україна	СБУ, Національна академія СБУ	Інформаційна безпека, аналітична робота	Основний акцент на аналітичній роботі та кібербезпеці; потреба в розширенні спеціалізованих програм та інтеграції сучасних методів навчання

США відзначаються глибокою інтеграцією військової та цивільної підготовки в галузі інформаційної безпеки, зокрема через великі ІТ-компанії, що надають додаткові можливості для навчання.

Велика Британія акцентує увагу на кібербезпеці через національні й університетські програми, що охоплюють широкий спектр тем від кіберзахисту до розвідки.

Державна політика України у сфері забезпечення інформаційної безпеки людини, суспільства, держави

У Німеччині віддають перевагу технічним аспектам інформаційної безпеки, підготовка реалізується через державні установи й технічні університети.

Ізраїль застосовує підхід, орієнтований на військову службу, що дає можливість отримати високий рівень практичних навичок у кібербезпеці та розвідці.

В Україні підготовка фахівців у галузі інформаційно-аналітичної діяльності проводиться переважно за спеціалізованими програмами в Службі безпеки України та Національній академії СБ України. Основні аспекти підготовки включають навчання з аналітичної роботи, кібербезпеки й інформаційної безпеки. Проте порівняно з міжнародними практиками є потреба в розширенні спеціалізованих прог-

рам, інтеграції сучасних методів навчання та посиленій співпраці з приватним сектором.

Міжнародний досвід показує, що підготовка фахівців для інформаційно-аналітичних підрозділів потребує інтеграції академічних знань, практичних навичок і безперервної освіти. Для України важливо адаптувати передові світові практики, зокрема розвиток програм співпраці з міжнародними партнерами, упровадження новітніх технологій навчання та посилення акценту на кібербезпеку й аналітичну роботу. Це дасть змогу забезпечити високий рівень підготовки фахівців, здатних ефективно реагувати на сучасні виклики та загрози. Основні шляхи вдосконалення за цим напрямом наведено в таблиці 4 (складена авторкою на основі [5–10]).

Таблиця 4 – Основні шляхи вдосконалення підготовки фахівців СБ України за напрямом інформаційно-аналітичної діяльності

Напрямок	Характеристика
Модернізація навчальних програм	Включення новітніх тем, таких як кібербезпека, аналіз великих даних, штучний інтелект та машинне навчання. Важливо, щоб навчальні програми відповідали сучасним викликам і загрозам.
	Збільшення частки практичних занять, лабораторних робіт і симуляцій реальних ситуацій. Це допоможе студентам отримати практичні навички, необхідні для роботи в умовах реальних загроз.
Впровадження сучасних технологій	Оновлення обладнання та програмного забезпечення, що використовуються в навчальному процесі. Важливо, щоб студенти мали доступ до сучасних інструментів для аналізу даних та інформаційної безпеки.
	Створення віртуальних середовищ для тренування навичок у кіберпросторі, включаючи симуляцію атак і захист.
Підвищення кваліфікації викладачів	Забезпечення постійного навчання та підвищення кваліфікації викладацького складу. Включення курсів і стажувань у провідних міжнародних центрах, що спеціалізуються на інформаційно-аналітичній діяльності.

State policy of Ukraine in the field of ensuring information security of person, society and the state

	Залучення до викладання спеціалістів із досвідом роботи в інформаційній безпеці й аналітиці, які можуть поділитися реальними кейсами та практичними знаннями.
Розвиток міжнародної співпраці	Участь у міжнародних програмах обміну, що дають змогу студентам і викладачам отримати досвід у закордонних установах, ознайомитися з найкращими практиками та методиками.
	Ініціація спільних дослідницьких проєктів із міжнародними партнерами, що дасть можливість адаптувати найкращі світові практики до українських умов.
Інтеграція етичних та психологічних аспектів	Включення курсів з етики та професійної відповідальності, що стосуються роботи з конфіденційною інформацією та дотримання прав людини.
	Забезпечення психологічної підготовки, включаючи стрес-менеджмент і розвиток емоційної стійкості, що є критично важливим для роботи у стресових умовах і при прийнятті складних рішень.

Пропоновані заходи допоможуть підвищити ефективність інформаційно-аналітичної діяльності фахівців Служби безпеки України, а також забезпечити безпеку та захист державних інтересів.

Висновки. Дослідження підтвердило, що в сучасному інформаційному суспільстві підготовка кваліфікованих кадрів для інформаційно-аналітичних підрозділів СБ України є ключовим елементом забезпечення національної безпеки. Загрози інформаційно-аналітичній діяльності займають центральне місце у структурі сучасних загроз, включаючи й сферу кібербезпеки.

Встановлено, що чинні освітні програми та тренінги переважно відповідають базовим вимогам, але потребують суттєвого оновлення для відображення останніх тенденцій у сфері інформаційних технологій та аналітики. Недостатньо уваги приділяється практичному навчанню та

використанню сучасних технологій аналізу даних.

З'ясовано, що сучасні виклики зумовлюють підвищення рівня етичних стандартів, технічної підготовки та психологічної стійкості фахівців СБ України. Ці аспекти важливі для роботи в умовах постійного стресу та за необхідності прийняття швидких рішень.

Виявлено, що в багатьох країнах акцентується увага на практичній підготовці, використанні симуляцій і віртуальних лабораторій, а також на тісній співпраці з приватним сектором. Цей досвід може бути успішно інтегрований в українські програми підготовки.

Основними проблемами, які потребують вирішення, є застарілість технічного оснащення, відсутність інтеграції сучасних методів аналізу даних у навчальні програми, а також недостатня увага до розвитку етичних

Державна політика України у сфері забезпечення інформаційної безпеки людини, суспільства, держави

і психологічних аспектів підготовки фахівців.

Рекомендується оновити зміст навчальних програм, включивши новітні досягнення у сфері інформаційно-аналітичної діяльності, а також посилити практичну складову.

Необхідно забезпечити постійне підвищення кваліфікації викладачів, включаючи міжнародні стажування й обмін досвідом.

Важливо оновити технічне оснащення навчальних закладів і забезпечити доступ до сучасного програмного забезпечення для аналізу даних.

Необхідне подальше вивчення питання інтеграції сучасних технологій у навчальний процес, а також розроблення методик для оцінювання ефективності підготовки фахівців. Особливу увагу слід приділити вивченню міжнародного досвіду та можливості його адаптації до українських реалій.

Вирішення зазначених проблем сприятиме забезпеченню ефективної підготовки фахівців Служби безпеки України в контексті протидії сучасним викликам.

Список використаних джерел

1. Кочеров М. Особливості інформаційно-аналітичного забезпечення реформ в органах національної поліції. *Knowledge, Education, Law, Management*. 2020. № 3 (31). С. 244–246.

2. Мовчан А. В. Інформаційно-аналітична робота в оперативно-розшуковій діяльності Національної поліції : навчальний посібник. Львів : ЛьвДУВС, 2017. 244 с.

3. Саричев Ю. Інформаційно-аналітичне забезпечення як вид інформаційного забезпечення в системі державного управління. *Вісник Національної академії державного управління при Президентові України*. Серія: Державне управління. 2017. № 3. С. 120–126.

4. Манжай О. В., Галауз В. Є. Шляхи підготовки фахівців у сфері протидії кіберзлочинності. *Актуальні питання протидії кіберзлочинності та торгівлі людьми* : збірник матеріалів Всеукраїнської науково-практичної конференції, (Харків, 23 листоп. 2018 р.) / МВС України, Харківський національний університет внутрішніх справ ; Координатор проектів ОБСЄ

в Україні. Харків : Харків. нац. ун-т внутр. справ, 2018. С. 350–352.

5. Манжай О. В. Особливості аналітичної та технічної складової підготовки фахівців для національної поліції України. Підготовка поліцейських в умовах реформування системи МВС України. Харків, 2019. С. 295–298.

6. Соколов В. А. Класифікація, функції та завдання аналітичної діяльності в системі забезпечення національної безпеки. *Інвестиції: практика та досвід*. 2016. № 16. С. 89–94.

7. Шевченко М. М., Зозуля О. С. Системи забезпечення національної безпеки адаптивного та креативного типів: порівняльний аналіз. *Інвестиції: практика та досвід*. 2015. № 16. С. 125–129.

8. Ганцюк Т. Д. Інформаційно-аналітичне забезпечення діяльності органів публічної влади в Україні: джерелознавчий аналіз дискурсного поля. *Державне управління: удосконалення та розвиток*. 2018. № 8. URL: <http://www.dy.nayka.com.ua/?op=1&z=1287> (дата звернення: 31.07.2024).

State policy of Ukraine in the field of ensuring information security of person, society and the state

9. Запорожець Т., Савченко Н. Інформаційно-аналітичне забезпечення державних механізмів запобігання та врегулювання міжнародних конфліктів. *Аспекти публічного управління*. 2022. № 10 (6). С. 24–29.

10. Сніцаренко П. М., Саричев Ю. О. Роль та місце інформаційного забезпечення в системі державного управління. *Державне управління: теорія та практика*. 2016. № 1. С. 46–56.

Стаття надійшла до редакції 02.12.2024

UDC 355.233.2:355.45:007

Doroshenko T. V.

REALITIES AND PROSPECTS OF TRAINING SPECIALISTS FOR THE SECURITY SERVICE OF UKRAINE IN THE FIELD OF INFORMATION AND ANALYTICAL ACTIVITIES

The article examines the peculiarities of training specialists for the units of the Security Service of Ukraine (SBU) working in the field of information and analytical activities. In the modern world, where information security has become critically important, the role of information countermeasures, psychological and informational operations as tools for ensuring national security is growing. In light of these aspects, the article analyses contemporary approaches to professional training within the SBU, educational programs and training sessions, as well as the requirements for SBU specialists working in the information and analytical sphere.

Key problems are identified, including insufficient attention to practical training, the development of ethical and psychological aspects of preparing specialists for the information and analytical field, the use of modern data analysis technologies, and the outdated technical equipment.

A comparative analysis of personnel training systems in different countries is conducted, demonstrating the potential for utilizing international best practices in Ukraine to enhance the effectiveness of information and analytical activities.

The results of the study, conducted using a comprehensive methodological approach, indicate the need to improve educational programs, considering the latest trends in information technologies, analytics, and the contemporary challenges of information security. The importance of strengthening the human resources potential of the SSU is highlighted. Recommendations include enhancing coordination between various agencies, developing international cooperation, and implementing new training methods that incorporate modern technologies and methodologies.

Key words: *security and defense sector, information countermeasures, information and psychological operations, information and analytical activities of the SBU, strategic communications.*