УДК 34:004.7:355/359

К. О. Споришев

АНАЛІЗ НОРМАТИВНО-ПРАВОВОЇ БАЗИ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ СИЛ БЕЗПЕКИ УКРАЇНИ: АСПЕКТИ ДЕРЖАВНОГО УПРАВЛІННЯ

Проведено аналіз стану чинної нормативно-правової бази інформаційно-аналітичного забезпечення сил безпеки України, а також закордонного досвіду щодо законодавчих підходів у галузі інформаційно-аналітичного забезпечення правоохоронних органів і спецслужб. Удосконалення нормативно-правової бази інформаційно-аналітичного забезпечення сил безпеки України є ключовим для підвищення ефективності національної оборони й безпеки, тому вимагає комплексного підходу, урахування багатьох чинників, що впливають на безпекову складову. Ідеться про комплексний підхід, який передбачає законодавчі, технічні та організаційні заходи.

Визначено проблемні аспекти нормативно-правової бази інформаційно-аналітичного забезпечення сил безпеки України та шляхи їх подолання.

Ключові слова: *нормативно-правововова база, інформаційно-аналітичне забезпечення, сили безпеки України, органи державного управління, службово-бойова діяльність, державна безпека.*

Постановка проблеми. Удосконалення нормативно-правової бази інформаційно-аналітичного забезпечення сил безпеки України – важливий аспект зміцнення національної безпеки й обороноздатності держави. Інформаційно-аналітичне забезпечення вкрай важливе для оперативного реагування сил безпеки України на внутрішні й зовнішні загрози. Актуальність теми зумовлена щораз численнішими інформаційними операціями проти України і необхідністю адекватно протистояти таким викликам. Розроблення і впровадження законодавчих ініціатив для вдосконалення нормативно-правової бази інформаційно-аналітичного забезпечення (ІАЗ) сил безпеки України є критично важливим кроком у забезпеченні національної безпеки й обороноздатності країни. Розглянемо деякі аспекти впливу нормативно-правової бази ІАЗ на ефективність службово-бойових дій сил безпеки.

Юридична визначеність і прозорість. Сучасне добре структуроване законодавство забезпечує чіткі правила та процедури для діяльності сил безпеки, сприяючи їх прозорості й передбачуваності. Юридична невизначеність може призводити до затримок у реагуванні на загрози, а також до зловживань і порушень прав людини.

Адаптація до сучасних викликів. Ефективність сил безпеки значною мірою залежить від їх здатності швидко адаптуватися до нових загроз: кібератаки, гібридна війна, тероризм тощо. Нормативна база, яка не відображає сучасних реалій, значно обмежує цю здатність.

Міжвідомча координація. Чітке законодавче регулювання сприяє кращій координації між різними силами безпеки і відомствами, уникненню дублювання функцій і зусиль, а також оптимізації розподілу ресурсів.

Міжнародна співпраця. Спроможність України до міжнародної співпраці у сфері безпеки так само залежить від її законодавчої бази. Сумісність національного законодавства з міжнародними стандартами й угодами є визначальною для ефективної міжнародної взаємодії та підтримки.

Інновації і технології. Нормативно-правова база сприяє впровадженню новітніх технологій і методик у діяльність сил безпеки. Брак правових механізмів для інновацій обмежує використання сучасних технологічних рішень.

Гармонізація з міжнародними стандартами. Відповідність національного законодавства міжнародним нормам і стандартам підвищує ефективність міжнародної співпраці.

Посилення міжвідомчої координації. Важливо розробляти і впроваджувати механізми зміцнення взаємодії між різними органами сил безпеки.

Для аналізу поточного стану нормативно-правової бази інформаційно-аналітичного забезпечення сил безпеки України визначимо основні проблеми й виклики.

Наразі в Україні діє низка законів і нормативних актів, які регулюють діяльність сил безпеки, зокрема закони «Про національну безпеку України», «Про державну таємницю», «Про боротьбу з тероризмом» та ін. Однак динаміка сучасних загроз вимагає постійного оновлення і доповнення існуючої нормативної бази. Багато чинних нормативних актів розроблено і прийнято ще до масового розвитку цифрових технологій, що робить їх не цілком адаптованими до викликів сучасної інформаційної безпеки. Це стосується захисту інформаційної інфраструктури, кібербезпеки та обігу

інформації в цифровому середовищі. У деяких випадках чинне законодавство містить прогалини або невизначеності, які ускладнюють ефективне застосування законів на практиці: питання юрисдикції, відповідальності, а також координації між різними відомствами. Україна активно співпрацює з міжнародними організаціями та інтегрується в міжнародні стандарти у сфері безпеки, однак необхідна додаткові зусилля щодо гармонізації внутрішнього законодавства із міжнародними нормами, особливо в контексті кібербезпеки й захисту інформаційного простору.

Основні проблеми нормативно-правової бази полягають у її застарілості, невідповідності сучасним вимогам інформаційної безпеки, бракує також інтегрованого підходу до збирання, оброблення та аналізу даних. Закордонний досвід показує, що ефективне інформаційно-аналітичне забезпечення досягається завдяки впровадженню передових технологій оброблення даних, законодавчій підтримці діяльності спецслужб і посиленню міжвідомчої взаємодії. Потребують запровадження сучасні ІТ-рішення для збирання, оброблення й аналізу даних, так само існує необхідність постійного підвищення кваліфікації фахівців інформаційно-аналітичних підрозділів.

Аналіз останніх досліджень і публікацій. Значний внесок у дослідження проблемних питань інформаційно-аналітичного забезпечення сил безпеки й оборони України зробили такі науковці: О. Й. Мацько, С. А. Микусь, В. Г. Солонніков, Г. А. Дробаха, М. О. Єрмошин, Є. Б. Смірнов, В. В. Шемчук, О. А. Олещенко, О. Ю. Іохов, В. Е. Лісіцин, С. А. Горєлишев та ін. Досліджували питання державного управління силами безпеки С. В. Бєлай, О. Г. Бондаренко, В. В. Єманов та ін.

Однак комплексного дослідження нормативно-правової бази інформаційно-аналітичного забезпечення сил безпеки й оборони України не здійснювалося.

Метою статті є аналіз стану чинної нормативно-правової бази інформаційно-аналітичного забезпечення сил безпеки України, а також закордонного досвіду щодо законодавчих підходів у галузі інформаційно-аналітичного забезпечення правоохоронних органів і спецслужб.

Виклад основного матеріалу. Розглянемо основні нормативно-правові акти щодо інформаційно-аналітичного забезпечення сил безпеки України.

1. Законом України «Про основні засади забезпечення кібербезпеки України» [1] створено комплексне юридичне підґрунтя для захисту кіберпростору України, зокрема захисту критичної інфраструктури, персональних даних громадян, а також державних інформаційних систем. Установлено вимоги до кібербезпеки для операторів критичної інфраструктури. Розроблено механізми реагування на кіберінциденти. Створена національна інфраструктура для виявлення кіберзагроз і запобігання їм. Законом про кібербезпеку регулюється взаємодія між державними органами, приватним сектором і міжнародними організаціями у сфері кібербезпеки.

Україна приділяє значну увагу зміцненню своїх кібербезпекових можливостей у контексті щодалі більших глобальних кіберзагроз. Закон України про кібербезпеку являє собою ключовий документ, що визначає правові й організаційні засади забезпечення кібербезпеки в державі, зокрема й аспекти стосовно інформаційно-аналітичного забезпечення сил безпеки.

Законом визначено органи державної влади, відповідальні за кібербезпеку, включно й ті, що забезпечують інформаційно-аналітичну підтримку сил безпеки, як-от Служба безпеки України, Державна спеціальна служба зв'язку та інформації, Міністерство оборони тощо.

Закон установлює загальні заходи щодо забезпечення кібербезпеки: розроблення і впровадження правил кібербезпеки, захист інформаційних систем, а також ідентифікація та реагування на кіберзагрози. Окреслено також механізми збирання, оброблення та аналізу даних про кіберзагрози, а також розроблення стратегічних та оперативних аналітичних матеріалів для підтримання рішень у сфері національної безпеки й оборони. Визнано важливість міжнародної співпраці в галузі кібербезпеки, зокрема обмін інформацією про кіберзагрози, спільні навчання та розроблення міжнародних стандартів кібербезпеки. Установлено правові норми, що регулюють відповідальність за порушення у сфері кібербезпеки, з метою захисту національних інтересів і забезпечення безпеки інформаційного простору.

2. Забезпечення захисту інформаційного простору України від дезінформації, пропаганди та інших інформаційних операцій, які можуть загрожувати національній безпеці, становить мету Закону України «Про засади інформаційної безпеки України» [2]. Визначаються основні загрози інформаційній безпеці та механізми протидії їм. Створена система моніторингу та аналізу інформаційного простору. Розроблені стандарти для ЗМІ та інших інформаційних ресурсів щодо публікації та поширення інформації. Установлена відповідальність за поширення недостовірної інформації.

Закон про засади інформаційної безпеки, охоплюючи інформаційно-аналітичне забезпечення сил безпеки, створює юридичне підґрунтя для комплексного підходу до захисту інформаційного простору України. Ідеться не лише про технічні та організаційні заходи, а й важливі аспекти міжвідомчої координації, міжнародної співпраці, освіти і правового регулювання.

3. Закон України «Про розвідку» [3] нормативно врегульовує розвідувальну діяльність в Україні задля підвищення ефективності збирання, оброблення та аналізу розвідувальної інформації. Визначаються правові засади розвідувальної діяльності, зокрема збирання, аналіз і поширення розвідданих. Регулюється взаємодія розвідувальних служб з іншими органами державної влади і міжнародними партнерами, встановлюються механізми контролю й нагляду за діяльністю розвідувальних служб.

Законом про розвідку визначено чіткі правові засади для проведення розвідувальної діяльності, основні завдання, принципи й методи розвідки, а також органи, вповноважені здійснювати розвідувальні операції. Регулюються й питання класифікації, зберігання, захисту та розголошення інформації, отриманої в ході розвідувальної діяльності, з метою захисту державної таємниці та інших конфіденційних даних. Визначено механізми парламентського і громадського контролю за діяльністю розвідувальних служб, а також внутрішніх процедур контролю та оцінювання ефективності розвідувальної роботи.

Закон України «Про розвідку» становить ключовий елемент національної безпекової архітектури, який забезпечує правові та організаційні рамки для ефективної роботи розвідки. Роль, яку розвідувальні служби відіграють у збиранні, аналізі й використанні розвідданих, робить їх невід'ємною частиною інформаційно-аналітичного забезпечення сил безпеки, сприяє таким чином своєчасному виявленню та нейтралізації загроз національній безпеці.

4. Закон «Про державну таємницю» [4] визначає нормативи щодо захисту державної таємниці з метою адаптації до сучасних викликів у сфері інформаційної безпеки. Він регламентує взаємовідносини, пов'язані із захистом інформації, яка становить державну таємницю, і встановлює юридичні, організаційні й технічні засади її збереження. У рамках інформаційно-аналітичного забезпечення сил безпеки України визначено критерії, за якими інформація може визнаватися державною таємницею, в тому числі інформація, що стосується обороноздатності й безпеки держави: військові, технічні, наукові розвідувальні дані, котрі мають значення для забезпечення національної безпеки. Закон установлює вимоги до захисту інформації, що належить до державної таємниці, зокрема забезпечення її конфіденційності, інтеграції та доступності. Це має вирішальне значення для ефективного управління і використання інформаційних ресурсів силовими структурами. Закон передбачає відповідальність за незаконне отримання, передачу, розголошення або втрату інформації, котра становить державну таємницю, що створює правове підґрунтя для притягнення до відповідальності осіб, які порушили режим таємниці, тим самим забезпечується додатковий захист інформації. Окреслено повноваження й обов'язки органів державної влади, установ та організацій щодо забезпечення режиму державної таємниці, включаючи органи сил безпеки. Ідеться про розроблення і впровадження заходів безпеки, атестацію робочих місць, навчання персоналу тощо. Закон регламентує порядок надання доступу до державної таємниці, визначає процедури перевірки осіб, їх допуску до роботи з таємними матеріалами, що є ключовим для інформаційно-аналітичної діяльності військових і спецслужб.

Хоча Закон про державну таємницю безпосередньо не зосереджується на інформаційно-аналітичному забезпеченні сил безпеки, він створює правове підґрунтя для захисту й використання інформації, що має важливе значення для національної безпеки й оборони.

5. Закон України «Про національну безпеку України» встановлює правові та організаційні засади забезпечення національної безпеки й оборони країни, а також задає головні принципи діяльності держави в цих сферах [5]. Інформаційно-аналітичне забезпечення сил безпеки України в контексті цього Закону охоплює такі аспекти.

Закон визначає інформаційну безпеку як важливий складник національної безпеки, наголошуючи на необхідності захисту інформаційного простору країни від зовнішніх і внутрішніх загроз. Окремі положення стосуються розвідувальної діяльності, що є частиною інформаційно-аналітичного забезпечення. Зазначається про необхідність забезпечення дієвої розвідки для виявлення та протидії потенційним загрозам національній безпеці. Закон акцентує увагу на забезпеченні кібербезпеки як елементі захисту критичної інформаційної інфраструктури держави та сил безпеки, встановлюючи засади для протидії кіберзагрозам. Положення Закону передбачають координацію діяльності різних

сил безпеки й оборони України, зокрема через обмін інформацією та аналітичними даними для підвищення ефективності виконання завдань національної безпеки. Закон визначає повноваження Президента, Верховної Ради, Кабінету Міністрів, Міністерства оборони, Служби безпеки України та інших органів у сфері забезпечення національної безпеки, у тому числі й інформаційно-аналітичного забезпечення.

Процеси інформатизації сил безпеки істотно відрізняються від ринкових і вимагають жорсткішого керування. Тому стосовно них має бути розроблена нормативно-правова база, а інформатизацію доцільно розглядати як організований процес створення оптимальних умов для задоволення інформаційних потреб особового складу, посадових осіб органів управління силами на основі формування і раціонального використання інформаційних ресурсів у новому технологічному середовищі [6].

Сили безпеки України у своїй службово-бойовій діяльності щодо питань інформатизації використовують нормативно-правову базу Збройних Сил України. Ці питання визначаються низкою документів, серед яких слід виділити такі.

1. Концепція інформатизації Міністерства оборони України – важлива частина стратегічного розвитку військової інфраструктури країни, спрямована на підвищення її обороноздатності та ефективності за допомогою сучасних інформаційних технологій [7]. Вона передбачає комплексний підхід до розвитку, інтеграції та використання інформаційних систем і технологій у всіх аспектах діяльності Збройних Сил. Концепція інформатизації охоплює такі основні аспекти.

Інтеграція інформаційних систем: створення єдиної інформаційної мережі, що дає змогу ефективно управляти ресурсами, координувати дії підрозділів і швидко обмінюватися даними між різними рівнями командування. *Автоматизація процесів управління*: впровадження сучасних інформаційно-керуючих систем для автоматизації процесів планування, управління бойовими діями, логістики та інших важливих аспектів діяльності Збройних Сил. *Забезпечення кібербезпеки*: розроблення і впровадження заходів для захисту військових інформаційних систем від кібератак, шпигунських програм та інших загроз. *Розвиток системи зв'язку*: модернізація та розширення систем зв'язку для забезпечення стабільного, безперебійного й безпечного обміну інформацією в умовах бойових дій. *Підготовка кадрів*: організація навчання та підвищення кваліфікації військовослужбовців у сфері використання сучасних інформаційних технологій.

Реалізація Концепції інформатизації потребує ефективної нормативно-правової бази, зокрема законів і нормативних актів, які регулювали б використання інформаційних технологій у Збройних Силах, забезпечення кібербезпеки, захисту інформації та персональних даних, а також стандартів і регламентів, які визначають технічні вимоги до інформаційних систем, засобів зв'язку, програмного забезпечення та обладнання. Необхідні директиви та інструкції для регулювання порядку розроблення, впровадження та експлуатації інформаційних систем у військовій сфері. Важливі міжнародні угоди та співпраця, що передбачають участь України в міжнародних проєктах і програмах з розвитку військових інформаційних технологій, обмін досвідом і знаннями з країнами-партнерами.

Концепція інформатизації Міністерства оборони України являє собою ключовий елемент стратегії національної безпеки й оборони, спрямованої на підвищення ефективності та готовності військових сил до дій у сучасних умовах. Її реалізація вимагає комплексного підходу, зокрема вдосконалення нормативно-правової бази, інтеграції сучасних інформаційних технологій, забезпечення кібербезпеки, розвитку систем зв'язку та підготовки кадрів.

2. Концепція створення єдиної автоматизованої системи управління (ЄАСУ) Збройних Сил України орієнтована на інтеграцію всіх рівнів управління та видів сил безпеки й оборони в єдину інформаційну структуру [6]. Це має забезпечити ефективне управління, оперативне реагування на змінні умови та злагоджену взаємодію між різними підрозділами й відомствами. Реалізація такої системи передбачає комплексний підхід до автоматизації управління військовими діями, логістики, розвідувальної інформації та інших ключових аспектів діяльності Збройних Сил.

Концепція складається з таких елементів: ЄАСУ має інтегрувати в собі різноманітні інформаційні системи і бази даних, що використовуються у Збройних Силах, забезпечуючи їх взаємосумісність та єдиний формат обміну даними. Головна мета ЄАСУ – максимальна автоматизація процесів прийняття рішень, планування, управління військами та контролю за виконанням завдань. Для надійної роботи ЄАСУ критично важливий високий рівень захисту від зовнішніх і внутрішніх кіберзагроз. Система має бути гнучкою до модифікацій і розширення, аби адаптуватися до змін у структурі Збройних Сил і вимог сучасного бою. Важливим складником вбачається створення єдиної захищеної системи зв'язку, що

уможливлювала б передачу даних між усіма рівнями управління. ЄАСУ повинна забезпечувати взаємодію не тільки в межах Збройних Сил, але й з іншими відомствами, силами безпеки й оборони України, а також міжнародними партнерами.

Створення єдиної автоматизованої системи управління Збройних Сил України становить стратегічно важливе завдання, втілення якого сприятиме підвищенню обороноздатності країни, оперативності управління й ефективності виконання поставлених завдань. Успішна реалізація цієї концепції потребує не тільки технічного забезпечення, а й розроблення програмного забезпечення.

3. Положення про науково-інформаційну діяльність у Збройних Силах України визначає правові, організаційні та методологічні засади проведення наукових досліджень, розроблення, впровадження і використання наукових знань та інформаційних технологій із метою підвищення обороноздатності й безпеки держави [8]. До його головних аспектів належать: підвищення ефективності управління Збройними Силами через упровадження сучасних наукових досягнень та інформаційних технологій; розвиток наукової бази для забезпечення потреб оборони та безпеки; оптимізація процесів збирання, оброблення, зберігання і передачі інформації військового призначення; забезпечення інформаційної безпеки в умовах сучасних викликів і загроз.

4. Доктрина «Зв'язок та інформаційні системи» розроблена з урахуванням вимог союзної об'єднаної публікації НАТО AJP-06 "Allied Joint Doctrine for Communication and Information Systems (Edition A Version 1)" [9]. Вона забезпечує загальне стратегічне керівництво із застосування зв'язку та інформаційних систем у Збройних Силах України та інших складових сил оборони під час їх застосування й підготовки, у тому числі під час проведення спільних навчань (тренувань) тощо. Доктрина запроваджує термінологію в галузі зв'язку та інформаційних систем, сумісну із термінологією, прийнятою в НАТО, описує характеристики зв'язку та інформаційних систем, поняття інформаційного менеджменту, архітектури побудови зв'язку та інформаційних систем, захисту інформації та кіберзахисту в інформаційно-телекомунікаційних системах, функції та завдання щодо зв'язку й інформаційних систем, визначає загальні положення з планування і застосування зв'язку й інформаційних систем, а також визначає аспекти взаємосумісності систем зв'язку й інформаційних систем.

У Національній гвардії як суб'єкті сил безпеки з питань ІАЗ діють Концепція державної цільової програми розвитку Національної гвардії України на період до 2020 р. і Концепція розвитку сектору безпеки і оборони України, затверджена Указом Президента України від 14.03.2016 р. № 92/2016 [6, 10]. Концепція розвитку Національної гвардії України втратила актуальність, термін дії програми закінчилися, її реалізація була не повною.

Концепція розвитку сектору безпеки і оборони України являє собою стратегічний документ, що визначає основні напрямки та пріоритети у формуванні й розвитку здатностей сектору безпеки і оборони країни, зокрема інформаційно-аналітичного забезпечення сил безпеки.

До нормативно-правової бази ІАЗ сил безпеки можна віднести також низку стандартів і нормативних документів, які встановлюють вимоги до захисту інформації в різних сферах: державне управління, банківська сфера, телекомунікації та ін.

1. Державний стандарт України DSTU 4145-2002 «Інформація. Захист інформації. Основні терміни та визначення» встановлює основні терміни й визначення, що використовуються у сфері захисту інформації.

2. Державний стандарт України DSTU ISO/IEC 27001:2015 «Інформаційна технологія. Безпека інформації. Системи управління інформаційною безпекою. Вимоги» встановлює вимоги до систем управління інформаційною безпекою та надає рекомендації щодо їх упровадження.

3. Державний стандарт України DSTU 3731:2001 «Інформаційна технологія. Захист інформації. Загальні положення» визначає загальні положення щодо захисту інформації, зокрема принципи захисту інформації та основні вимоги до нього.

4. Стандарт Payment Card Industry Data Security Standard (PCI DSS) установлює вимоги щодо захисту конфіденційної інформації про платіжні картки та інших даних, які зберігаються та обробляються у платіжних системах.

5. ISO/IEC 27001 – міжнародний стандарт, що встановлює вимоги до системи управління інформаційною безпекою (СУІБ). Незважаючи на те, що це міжнародний стандарт, його принципи та практики можуть бути адаптовані на національному рівні для забезпечення захисту інформації в силових структурах.

6. NIST Cybersecurity Framework розроблено Національним інститутом стандартів і технологій США. Цей фреймворк пропонує структуру для управління і зниження кібербезпекових ризиків. В

Україні може бути розроблено подібний національний стандарт або адаптовано існуючий для потреб сектору безпеки.

Наведені стандарти й нормативні документи визначають базові вимоги й методи захисту інформації в різних сферах діяльності в Україні. Державні установи повинні дотримуватися цих вимог для забезпечення безпеки інформації та відповідності законодавству.

Дослідження закордонного досвіду у сфері нормативно-правової бази інформаційно-аналітичного забезпечення сил безпеки дає змогу визначити передові практики та інноваційні підходи, які можуть бути адаптовані та впроваджені в Україні [11]. Наведемо декілька прикладів.

Patriot Act – закон США, прийнятий після терактів 11 вересня 2001 р., значно розширив повноваження американських правоохоронних органів і спецслужб у сфері нагляду та збирання інформації для боротьби з тероризмом. Він включає положення, які дозволяють владі за певних умов вести нагляд без судового ордера. Це поліпшило інформаційно-аналітичне забезпечення.

Cybersecurity Information Sharing Act (CISA) 2015 – закон, що спрощує обмін інформацією про кіберзагрози між урядом США і приватним сектором. Цей акт сприяє кращій координації та ефективності виявлення кібератак і відповіді на них.

Ізраїль розробив комплексний підхід до кібербезпеки, який включає різні законодавчі та регуляторні ініціативи. Вони зосереджені на захисті критичної інфраструктури і зміцненні національної кібербезпеки шляхом співпраці між державним і приватним секторами. Це забезпечує ефективний обмін інформацією та ресурсами задля протидії кіберзагрозам.

Естонія є світовим лідером у сфері е-урядування та кібербезпеки. У країні розроблена низка законів, що регулюють захист даних, кібербезпеку й електронні послуги, таким чином забезпечується високий рівень захисту інформації та інфраструктури. Передбачено комплексні заходи щодо захисту персональних даних, кіберзахисту державних служб і впровадження цифрових ідентифікаторів.

Закон, який установлює юридичну рамку для кібербезпеки в Сінгапурі, зокрема захист критичної інфраструктури від кібератак, – Cybersecurity Act 2018. Він передбачає створення національної агенції з кібербезпеки, яка координує зусилля з кібербезпеки на національному рівні, а також сприяє міжнародній співпраці.

Bundesamt für Sicherheit in der Informationstechnik (BSI) – закон Німеччини, що регулює діяльність Федерального відомства з безпеки в інформаційних технологіях. Він установлює рамки для захисту федеральних інформаційних систем і сприяє підвищенню кібербезпеки у приватному секторі.

Наведені приклади підтверджують, що ефективне інформаційно-аналітичне забезпечення сил безпеки в сучасному світі потребує комплексного підходу, зокрема оновлення законодавства, співпраці між державним і приватним секторами, а також міжнародної координації.

Висновки

Удосконалення нормативно-правової бази інформаційно-аналітичного забезпечення сил безпеки України є ключовим для підвищення ефективності національної оборони й безпеки і потребує комплексного підходу, урахування багатьох чинників, що впливають на безпекову складову. Такий комплексний підхід передбачає законодавчі, технічні та організаційні заходи.

Виклики сучасності, які постали перед нашою державою, вимагають ширшого запровадження інформатизації та цифровізації державних органів управління. Останніми роками в Україні зроблено значні кроки щодо цифровізації, але темпи цього процесу для сил безпеки заповільні, а в умовах широкомасштабної агресії РФ це є одним із критичних безпекових чинників.

Насичення військ програмно-апаратними засобами вже відбувається, але в існуючих умовах процес інформатизаціїї слабо керований, що й зумовлює його низьку ефективність. Роботи з інформатизації пов’язані з великими витратами сил і засобів, тому не можуть вестися на рівні місцевих ініціатив і громадських засад, а потребують єдиного керівництва, єдиних концептуальних підходів, узгодження зусиль у рамках відомчих і загальнодержавних програм, створення штатних структур, відповідальних за розроблення й застосування програмно-апаратних засобів, узгодження з реформами й розвитком військ, що відбуваються. Цілеспрямовану інформатизацію сил безпеки варто розпочинати з процесу навчання, тим самим вирішити важливі завдання: закласти методологічне ядро майбутньої відомчої інформаційної системи і створити базу підготовки кадрів, які мали б досвід упровадження інформаційних технологій у службово-бойову діяльність.

Напрямками подальших досліджень є адаптація нормативно-правової бази країн ЄС і НАТО до реалій службово-бойових дій сил безпеки України.

Перелік джерел посилання

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. URL: http://surl.li/ajfjh (дата звернення: 10.02.2024).
2. Про засади інформаційної безпеки України : Закон України від 28.05.2014 р. № 4949. URL: http://surl.li/rngwy (дата звернення: 11.02.2024).
3. Про розвідку : Закон України від 17.09.2020 р. № 912-IX. URL: http://surl.li/bvgjz (дата звернення: 11.02.2024).
4. Про державну таємницю : Закон України від 21.01.1994 р. № 3855-XII. URL: http://surl.li/axmgl (дата звернення: 11.02.2024).
5. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII. URL: http://surl.li/tcsi (дата звернення: 12.02.2024).
6. Основи інформатизації Національної гвардії України: навч. посіб. / Г. А. Дробаха та ін. Харків : НАНГУ, КП «Міська друкарня», 2016. 366 с.
7. Про затвердження Концепції інформатизації Міністерства оборони України : наказ Міністерства оборони України від 17.09.2014 р. № 650. URL: http://surl.li/rngzr (дата звернення: 12.02.2024).
8. Положення про науково-інформаційну діяльність у Збройних Силах України : наказ Міністерства оборони України від 27.07.2016 р. № 385. URL: http://surl.li/baayc (дата звернення: 12.02.2024).
9. Доктрина «Зв'язок та інформаційні системи» : затв. Головнокомандувачем Збройних Сил України 02.07.2020 р. № 15841/С. *Центральне управління зв'язку та інформаційних систем Генерального штабу Збройних Сил України*. 78 с.
10. Концепція розвитку сектору безпеки і оборони України : Указ Президента України від 14.03.2016 р. № 92/2016. URL: http://surl.li/rnhbh (дата звернення: 13.02.2024).
11. Єманов В. В., Споришев К. О. Досвід функціонування системи інформаційно-аналітичного забезпечення силових структур провідних країн світу. *Наукові перспективи. Державне управління.* 2024. № 1 (43). С. 132–142.

Стаття надійшла до редакції 10.03.2024 р.

UDC 34:004.7:355/359

K. Sporyshev

ANALYSIS OF THE REGULATORY AND LEGAL BASE OF THE INFORMATION AND ANALYTICAL SUPPLY OF THE SECURITY FORCES OF UKRAINE

An analysis of the current state of the regulatory and legal framework for the information and analytical provision of the security forces of Ukraine, an analysis of foreign experience regarding legislative approaches in the field of information and analytical provision of law enforcement agencies and special services was carried out. Improving the legal framework for the information and analytical support of the security forces of Ukraine is key to improving the effectiveness of national defense and security. This involves a comprehensive approach that includes legislative, technical, and organizational measures. The improvement of the legal framework of the information and analytical support of the security forces of Ukraine requires a comprehensive approach, taking into account many factors affecting the security component.

Problematic aspects of the regulatory and legal framework of information and analytical support of the security forces of Ukraine and ways to overcome them have been identified.

Keywords: *regulatory and legal framework, information and analytical support, security forces of Ukraine, state administration bodies, service and combat activity, state security.*

Споришев Костянтин Олександрович – кандидат технічних наук, доцент, докторант ад'юнктури та докторантури, Національна академія Національної гвардії України

https://orcid.org/0000-0003-4737-9698