УДК 351.86:004.9(477)

К. О. Споришев, В. М. Клішин, В. Л. Белоусов

РОЛЬ ІНФОРМАЦІЙНО- АНАЛІТИЧНОГО СКЛАДНИКА У СФЕРІ ДЕРЖАВНОЇ БЕЗПЕКИ

Досліджено роль і значення інформаційно-аналітичних систем у забезпеченні державної безпеки України в умовах гібридних загроз, кібернетичного протистояння та динамічного розвитку інформаційних технологій, розкрито сутність і тенденції розвитку аналітичного забезпечення в Україні, окреслено ключові напрями цифрової трансформації сектору безпеки. Проведено порівняльний аналіз практичного застосування інформаційно-аналітичних систем у сфері державної безпеки України, Сполучених Штатів Америки та країн Європейського Союзу.

Запропоновано комплекс заходів із удосконалення інформаційно-аналітичного механізму державного управління у сфері безпеки, зокрема створення єдиного національного аналітичного центру, уніфікацію форматів обміну даними, впровадження інтелектуальних алгоритмів оброблення інформації та формування системи підготовки фахівців нового покоління.

Ключові слова: *державна безпека, інформаційно-аналітична діяльність, системи підтримки прийняття рішень, сили безпеки.*

Постановка проблеми. У сучасних умовах гібридних загроз, інформаційних війн та збройної агресії проти України особливої ваги набуває питання формування ефективної системи державної безпеки, заснованої на оперативному аналізі, оцінюванні та прогнозуванні ситуацій. Водночас, незважаючи на наявність значного масиву даних, інформаційно-аналітичний складник у діяльності сил безпеки та органів державного управління залишається недостатньо інтегрованим, фрагментарним та технологічно нерівномірним [1, 2, 3]. Основна проблема полягає у відсутності цілісного механізму використання інформаційно-аналітичних систем для підтримки процесів прийняття управлінських рішень у сфері державної безпеки, що призводить до зниження оперативності реагування на кризові ситуації і зменшення ефективності взаємодії між суб'єктами сектору безпеки та оборони [3–6]. Інформація стала стратегічним ресурсом XXI століття, який визначає рівень національної безпеки, економічної стабільності та політичної стійкості держави. В умовах інтенсивного розвитку інформаційних технологій, штучного інтелекту, кіберзагроз і дезінформаційних кампаній держава потребує нового підходу до управління безпековими процесами – на основі сучасних інформаційно-аналітичних систем [6]. Посилення ролі інформаційно-аналітичного складника дасть змогу створити єдиний ситуаційний простір для прогнозування, моніторингу й управління загрозами, що є критично важливим для підвищення ефективності рішень органів державної влади, сил безпеки та оборони. Отже, розвиток цього складника виступає необхідною умовою забезпечення стійкості держави до внутрішніх і зовнішніх викликів.

Аналіз останніх досліджень і публікацій. Проблемні питання державного управління системою інформаційно-аналітичного забезпечення сил безпеки України розглянуто в працях таких учених, як Г. П. Ситник, С. В. Бєлай, К. О. Споришев, В. В. Єманов, Г. А. Дробаха, О. А. Олещенко, І. О. Кириченко, С. А. Горєлишев, А. А. Побережний, О. Ю. Іохов, В. Е. Лісіцин та ін.

Метою статті є обґрунтування ролі та значення інформаційно-аналітичного складника у сфері державної безпеки, визначення основних проблем і викликів у його реалізації, а також окреслення напрямів удосконалення інформаційно-аналітичних механізмів підтримки прийняття управлінських рішень у діяльності сил безпеки України.

Виклад основного матеріалу. Незважаючи на значний прогрес у впровадженні інформаційно-аналітичних технологій у діяльність органів державної безпеки, залишається низка системних проблем і викликів, що стримують ефективне функціонування аналітичних систем. Їх можна класифікувати за технологічними, організаційними, кадровими, правовими та безпековими аспектами.

1. Кіберзагрози та вразливість інформаційних систем. Одним із найсерйозніших викликів сучасності є зростання масштабів і складності кібератак. Державні та військові інформаційні ресурси постійно піддаються спробам несанкціонованого доступу, знищення або модифікації даних [1, 3].

До основних проявів кіберзагроз слід віднести:

1) проникнення у критичні інформаційні інфраструктури;

2) створення шкідливих програм для збирання або спотворення інформації;
3) атаки типу DoS і ransomware на аналітичні сервери;
4) використання штучного інтелекту для автоматизації кібератак.

Особливо небезпечними є комбіновані інформаційно-психологічні операції, які поєднують технічні злами з маніпулюванням громадською думкою. Це вимагає посилення кіберзахисту, розвитку національної системи кіберстійкості та регулярного аудиту інформаційних платформ безпеки.

2. Недостатня інтеграція даних і несумісність інформаційних систем. Незважаючи на активний розвиток аналітичних технологій, єдиної міжвідомчої системи обміну даними в Україні поки що бракує [2, 4]. Інформаційні ресурси належать різним відомствам [Міністерству внутрішніх справ (МВС), Службі безпеки України (СБУ), Міністерству оборони (Міноборони), Національній гвардії України (НГУ), Державній службі з надзвичайних ситуацій (ДСНС)], які використовують власні стандарти, формати та бази даних. Це призводить до таких проблем:

– дублювання або фрагментарність інформації;

– складнощі в об'єднанні відомчих баз у єдине аналітичне середовище;

– брак централізованих протоколів взаємодії.

Без створення інтероперабельної аналітичної інфраструктури з уніфікованими форматами обміну даними неможливо забезпечити повноцінне функціонування національної системи інформаційно-аналітичної підтримки безпеки.

3. Кадровий дефіцит та нерівномірний рівень кваліфікації фахівців. Одним із ключових обмежень залишається брак кваліфікованих аналітиків, ІТ-спеціалістів та фахівців із кібербезпеки. Більшість наявних програм підготовки не відповідають сучасним вимогам до аналітичної діяльності, зокрема у частині роботи з великими даними, штучним інтелектом, автоматизованими системами підтримки рішень. Проблема посилюється кадровою плинністю, обмеженими можливостями підвищення кваліфікації у сфері безпеки та недостатнім рівнем міжвідомчої підготовки [7].

Для подолання цього виклику необхідно створювати єдину систему професійного розвитку аналітичних кадрів, включно з навчальними центрами, симуляційними платформами та інтегрованими освітніми програмами у вищих навчальних закладах сектору безпеки.

4. Етичні та правові аспекти використання даних. Активне впровадження аналітичних систем супроводжується ризиками порушення прав людини на конфіденційність і приватність. Оброблення великих масивів персональних даних (зокрема біометричних, комунікаційних і поведінкових) потребує чіткого правового регулювання. Основними проблемами у цій сфері є:

– відсутність уніфікованої законодавчої бази для аналітичних систем безпеки;

– недостатня прозорість алгоритмів оброблення інформації;

– потенційна можливість зловживання аналітичними інструментами для політичних або комерційних цілей.

Потребує удосконалення національне законодавство у частині регулювання штучного інтелекту, кіберрозвідки, захисту персональних даних і міжнародного обміну аналітичною інформацією.

5. Технологічна фрагментованість та відставання від світових стандартів. Багато наявних інформаційних систем органів безпеки України створювалися автономно, без єдиної архітектурної моделі. У результаті мають місце різнорідність технічних платформ, застарілі бази даних, низька швидкодія серверів і обмежена масштабованість. Спостерігається також відставання від міжнародних стандартів, зокрема у сфері штучного інтелекту, оброблення великих даних, блокчейн-технологій та геоінформаційного аналізу [3].

Для подолання цих бар'єрів потрібна державна стратегія модернізації аналітичних систем, заснована на уніфікованих технічних вимогах і стандартах обміну даними (ISO, NATO STANAG, EU INSPIRE тощо).

6. Брак єдиного центру аналітичної координації. Інформаційно-аналітична діяльність у секторі безпеки часто розподілена між різними відомствами, які не мають спільного координаційного механізму. Це призводить до розривів у ланцюгах прийняття рішень, дублювання функцій і втрати актуальності даних. Проблема посилюється відсутністю постійного аналітичного моніторингу на національному рівні, який міг би забезпечувати системне прогнозування ризиків.

Вирішенням може стати створення Національного центру аналітичного забезпечення безпеки, що акумулюватиме дані з усіх державних органів, формуватиме єдину картину загроз і координуватиме інформаційні потоки між міністерствами та силовими структурами.

7. Фінансові та інфраструктурні обмеження. Більшість інформаційно-аналітичних проєктів у сфері безпеки потребують значних інвестицій у технічне обладнання, ліцензійне програмне забезпечення, засоби шифрування та системи резервування даних. Проте обмежене фінансування та непостійність бюджетного забезпечення часто знижують темпи цифровізації безпекових процесів. Недостатній рівень технічного оснащення окремих підрозділів спричиняє нерівномірний доступ до аналітичних ресурсів, що знижує оперативність реагування на загрози.

Вирішення цієї проблеми потребує створення державних і державно-приватних програм підтримки, які дадуть можливість залучати технологічних партнерів, грантові ресурси Європейського Союзу (ЄС) і міжнародні проєкти кіберстійкості.

8. Проблема «довіри» та міжвідомчої взаємодії. Ще однією суттєвою перепоною є низький рівень довіри між окремими державними інституціями у питанні обміну чутливою інформацією. Наявність відомчих обмежень, бюрократичних процедур і страху витоку даних ускладнює аналітичну інтеграцію. Для її подолання необхідно запровадити:

а) єдині стандарти безпеки обміну інформацією;

б) механізми контролю та аудиту доступу;

в) інституційні угоди про обмін даними на основі довіри.

Розвиток культури міжвідомчої співпраці є передумовою створення цілісної системи аналітичного управління державною безпекою.

Розглянемо досвід використання інформаційно-аналітичних систем у світі.

І. Система національної безпеки Сполучених Штатів Америки (США) є однією з найскладніших та найтехнологічніших у світі. Вона базується на розгалуженій мережі аналітичних центрів, баз даних, інформаційно-комунікаційних платформ і систем підтримки прийняття рішень, які охоплюють усі рівні – від федерального до місцевого. Сполучені штати Америки стали піонером у застосуванні інформаційно-аналітичних технологій у сфері оборони, протидії тероризму, кібербезпеки та управління кризами [8].

1. Агентство національної безпеки (NSA) та система SIGINT. Один із найвідоміших прикладів аналітичної діяльності у США – робота **Агентства національної безпеки**, яке здійснює збирання, оброблення та аналіз сигналів розвідки (SIGINT – Signals Intelligence). Інформаційно-аналітичні комплекси NSA обробляють мільярди одиниць даних, отриманих із супутників, інтернет-каналів, телефонних мереж і відкритих джерел. Основою цих процесів є **аналітичні системи великих даних (Big Data Analytics)**, які дають змогу виявляти закономірності, взаємозв'язки та потенційні загрози. Для автоматизованого аналізу інформації NSA використовує спеціалізовані алгоритми машинного навчання, здатні розпізнавати підозрілі комунікації, визначати джерела кібератак або ідентифікувати нові типи шкідливих впливів. Крім цього, функціонує програма **XKeyscore**, що забезпечує глобальний пошук і фільтрацію інформації у режимі реального часу, інтегруючи розвідувальні потоки з десятків джерел.

2. Федеральне бюро розслідувань (FBI) та система IAFIS [8]**.** У сфері внутрішньої безпеки одним із ключових інструментів є **Інтегрована автоматизована система ідентифікації відбитків пальців (IAFIS)**, якою користується **FBI**. Це одна з наймасштабніших біометричних баз даних у світі, що містить понад 70 млн записів. Система дає можливість здійснювати швидкий пошук і автоматичне зіставлення біометричних даних підозрюваних, осіб без громадянства або загиблих. Пізніше вона була розширена до **NGI (Next Generation Identification System)**, яка об'єднала не лише відбитки пальців, але й зображення облич, райдужної оболонки очей, а також інші біометричні ідентифікатори. Система NGI використовує аналітичні алгоритми штучного інтелекту для розпізнавання осіб у потоках відеоспостереження, виявлення аномальної поведінки та побудови зв'язків між учасниками злочинних мереж.

Такі системи значно підвищують ефективність роботи правоохоронних органів і дозволяють забезпечити комплексну інформаційно-аналітичну підтримку у сфері кримінальної безпеки.

3. Агентство з кібер- та інфраструктурної безпеки (CISA). У 2018 р. при Міністерстві внутрішньої безпеки (DHS) створено **CISA (Cybersecurity and Infrastructure Security Agency)**, яке відповідає за моніторинг, аналіз і захист критичної інфраструктури США від кіберзагроз. Центральною частиною його діяльності є **Національний центр кібербезпеки та комунікацій**, який

використовує аналітичні платформи **Einstein 3 Accelerated** та **Continuous Diagnostics and Mitigation (CDM)**. Einstein 3 A**ccelerated** – це система глибокого аналізу мережевого трафіку, яка автоматично виявляє шкідливу активність, порушення безпеки та несанкціоновані дії у державних інформаційних мережах. Система CDM, зі свого боку, забезпечує **постійну оцінку кіберризиків**, збирання метрик із сотень федеральних систем і формування аналітичних звітів для керівництва DHS. Завдяки цим системам США мають змогу здійснювати **проактивний аналіз кіберзагроз** і координувати дії між державними та приватними структурами у режимі реального часу.

4. Центральне розвідувальне управління (CIA) та система DCGS. Центральне розвідувальне управління США активно використовує інформаційно-аналітичні платформи для стратегічного прогнозування, аналізу ризиків і підтримки оперативних рішень. Один із ключових інструментів – **Distributed Common Ground System (DCGS)**, який використовується також збройними силами США. Це розподілена аналітична система, що інтегрує дані з різних джерел: супутникових сенсорів, радарів, безпілотників, радіорозвідки, агентурних повідомлень і відкритих джерел. За допомогою DCGS аналітики можуть створювати **оперативні ситуаційні картини**, проводити глибокий аналіз об'єктів і тенденцій, а також прогнозувати можливі сценарії дій противника. Система підтримує спільну роботу аналітиків у різних часових зонах, забезпечуючи доступ до актуальних даних у режимі реального часу [8].

5. Система Homeland Security Information Network (HSIN). **Система** HSIN є ключовим інформаційно-аналітичним середовищем Міністерства внутрішньої безпеки США, що забезпечує взаємодію між федеральними, регіональними та місцевими структурами. Це **захищена платформа обміну аналітичною інформацією**, через яку щоденно проходять тисячі оперативних повідомлень, аналітичних довідок і ситуаційних звітів. Зазначена система дає змогу користувачам створювати **віртуальні ситуаційні центри**, вести спільні обговорення у кризових ситуаціях, координувати дії між поліцією, службами екстреного реагування, прикордонниками й іншими структурами. У кризових подіях (наприклад, під час стихійних лих або терористичних загроз) HSIN інтегрується із системами геоінформаційного аналізу (GIS) для відображення карт ризику, маршрутів евакуації та ресурсів рятувальних служб [8].

6. Національний центр боротьби з тероризмом (NCTC). Після терактів 11 вересня 2001 р. США створили **Національний центр боротьби з тероризмом**, який об'єднав аналітичні ресурси розвідки, армії, дипломатичних і правоохоронних структур. Цей центр функціонує як **єдина аналітична платформа з протидії тероризму**, що агрегує дані з понад 20 джерел, зокрема з NSA, CIA, FBI, Пентагону та Державного департаменту. Система використовує інструменти штучного інтелекту для побудови **соціальних графів** зв'язків між підозрюваними, аналізу фінансових транзакцій і прогнозування можливих терористичних актів. Завдяки аналітичним алгоритмам NCTC може автоматично визначати «аномальні поведінкові патерни» у великих потоках даних, що дає змогу запобігати злочинам на ранніх стадіях [8].

7. Системи кризового управління FEMA. **Агентство з надзвичайних ситуацій (FEMA)** використовує потужну інформаційно-аналітичну платформу для прогнозування, реагування та відновлення після стихійних лих. Аналітична система **HURREVAC** дає можливість оцінювати траєкторії ураганів, масштаби можливих руйнувань і необхідність евакуації населення. Платформа **EMMA (Emergency Management Mission Area)** інтегрує дані з місцевих департаментів, метеорологічних служб, супутникових систем і безпілотників, формуючи **оперативну ситуаційну картину** у режимі реального часу. Ці аналітичні рішення дають змогу ефективно координувати роботу рятувальників, прогнозувати потреби у ресурсах і мінімізувати людські втрати під час катастроф.

Ⅱ. Європейський Союз є одним із найбільш технологічно розвинених регіонів світу у сфері безпеки, аналітики та обміну інформацією між державами-членами. Основою європейської безпекової архітектури є інтегровані інформаційно-аналітичні системи, що забезпечують моніторинг загроз, координацію оперативних дій, аналіз ризиків і стратегічне прогнозування у сфері внутрішньої та зовнішньої безпеки.

Європейський Союз активно формує єдиний інформаційно-аналітичний простір безпеки, який поєднує діяльність агентств, національних спецслужб, поліційних структур і дипломатичних інституцій. Цей простір створено на засадах міжвідомчої співпраці, кіберстійкості та поваги до принципів захисту персональних даних.

1. Європол – Європейський поліцейський офіс. Одним із ключових аналітичних центрів ЄС є **Європол**, штаб-квартира якого розташована в Гаазі (Нідерланди). Основна його функція полягає у **збиранні, аналізі та поширенні оперативної інформації** між національними поліціями країн-членів. В основі роботи Європолу лежить **Єдина інформаційно-аналітична платформа (EIS – Europol Information System)**, яка забезпечує централізоване зберігання та оброблення даних про злочинні угруповання, фінансові потоки, кіберзлочини, незаконну міграцію та терористичну діяльність [9, 10].

Ця платформа дозволяє країнам ЄС здійснювати спільний аналіз загроз і координувати дії у реальному часі. Аналітики Європолу використовують алгоритми інтелектуального аналізу даних (data mining, link analysis) для виявлення зв'язків між подіями, персоналіями та транскордонними злочинними мережами. Важливим складником є також аналітична платформа AP (Analysis Project), у межах якої створюються тематичні модулі (наприклад, AP Terrorism, AP Cybercrime, AP Fraud, AP Drugs). Кожен модуль дає можливість вести окремі аналітичні дослідження, формувати ризикові профілі та підтримувати оперативні рішення на рівні національних поліцій.

2. Система Schengen Information System (SIS II). **Schengen Information System** є найбільшою загальноєвропейською базою даних, яка забезпечує контроль за безпекою у межах Шенгенської зони. Система містить понад 100 млн записів про розшукуваних осіб, транспортні засоби, зброю, документи, міграційні порушення тощо. Вона використовується поліцією, прикордонниками, митними та судовими органами усіх країн-членів ЄС. Система SIS II функціонує у режимі реального часу, забезпечуючи **автоматичну взаємодію** між національними інформаційними центрами (N.SIS) і центральною системою (C.SIS), що розташована у Страсбурзі [9, 10].

Система доповнена аналітичними модулями, які дають змогу здійснювати ризик-аналіз переміщення осіб, визначати можливі маршрути нелегальної міграції, відстежувати переміщення транспортних засобів, що можуть бути пов'язані з кримінальною діяльністю. На практиці SIS II стала ключовим інструментом попередження терористичних актів, розслідування транскордонних злочинів і зміцнення контролю над зовнішніми кордонами ЄС.

3. Європейська прикордонна та берегова охорона (Frontex). Агентство **Frontex**, створене у 2004 р., використовує високотехнологічну систему ситуаційного моніторингу **EUROSUR (European Border Surveillance System)**. EUROSUR є платформою, яка об'єднує дані з супутників, радарів, сенсорів, безпілотних літальних апаратів, морських і наземних спостережних пунктів. Мета системи **– забезпечити цілісне бачення ситуації на зовнішніх кордонах ЄС** і сприяти запобіганню нелегальній міграції, контрабанді та морським катастрофам.

EUROSUR має багаторівневу структуру [9, 10]:

1) національні координаційні центри збирають дані на рівні держав;
2) регіональні хаби здійснюють порівняльний аналіз і прогнозування;
3) центральний рівень Frontex формує аналітичну картину загальноєвропейського масштабу.

Аналітичні модулі EUROSUR дозволяють моделювати можливі сценарії міграційних криз, розраховувати ризики і планувати розподіл сил реагування. У кризових ситуаціях система інтегрується із SIS II та EIS Європолу, що забезпечує єдиний інформаційний простір реагування.

4. Європейський центр боротьби з кіберзлочинністю. У структурі Європолу функціонує **Європейський центр боротьби з кіберзлочинністю**, який є головним аналітичним вузлом у сфері кібербезпеки. Цей центр здійснює моніторинг кіберінцидентів у країнах-членах ЄС, проводить криміналістичний аналіз шкідливого програмного забезпечення, координує операції з виявлення кіберзлочинців і хакерських угруповань. Система використовує **інформаційно-аналітичну платформу Threat Intelligence Platform**, що забезпечує обмін даними між поліцейськими структурами, CERT-центрами, фінансовими установами й IT-компаніями.

Особливу роль відіграє аналіз великих даних (Big Data) та автоматизоване кореляційне виявлення, наприклад, визначення зв'язків між кіберінцидентами, доменами, IP-адресами та цифровими артефактами. Це дає можливість не лише розслідувати злочини, а й запобігати масовим кібератакам на критичну інфраструктуру [9, 10].

5. Інтегровані аналітичні центри у сфері тероризму (CTG, INTCEN). Після терактів у Лондоні (2005 р.) та Брюсселі (2016 р.) ЄС активізував створення міждержавних аналітичних структур, як-от **Counter Terrorism Group (CTG)** та **EU Intelligence and Situation Centre (INTCEN)**. Ці установи здійснюють **обмін розвідувальною інформацією** між спецслужбами держав-членів і проводять **спільний аналітичний аналіз загроз тероризму**.

Структура INTCEN, яка діє при Європейській службі зовнішніх дій (EEAS), функціонує як стратегічний аналітичний центр, що опрацьовує дані з дипломатичних місій, військових структур, відкритих джерел і спеціальних служб. Його фахівці створюють аналітичні звіти, оцінки ризиків, попередження та прогнози для керівництва ЄС. Установа CTG зосереджується на оперативному аналізі терористичних загроз, обміні даними між національними агентствами та координації спільних операцій.

Разом ці структури створюють інформаційно-аналітичний каркас антитерористичної політики ЄС, заснований на принципах спільної відповідальності та взаємного обміну інформацією.

6. Інформаційно-аналітична система Європейської служби зовнішніх дій. Європейська служба зовнішніх дій використовує систему **EU Open Source Intelligence (EU OSINT)** – інструмент збирання та аналізу відкритих даних для моніторингу геополітичних процесів. Система інтегрує аналітику із соціальних мереж, медіа, геолокаційних сервісів і супутникових спостережень. На її основі формується **Європейський аналітичний бюлетень безпеки**, який містить оцінки кризових регіонів, імовірних конфліктів і ризиків для енергетичної чи економічної стабільності ЄС [9, 10].

Ⅲ. В Україні інформаційно-аналітичні системи активно використовуються у діяльності органів безпеки та оборони. Наприклад, у межах боротьби з кіберзагрозами застосовуються сучасні системи моніторингу та аналізу мережевого трафіку, що дозволяє виявляти та нейтралізувати кібератаки в реальному часі. Сучасна система державної безпеки України перебуває на етапі активної цифрової трансформації, коли інформаційно-аналітичні технології стають не лише допоміжним, а й визначальним чинником ефективності діяльності органів безпеки, оборони, внутрішніх справ і цивільного захисту. Нижче наведено низку прикладів практичного використання таких систем, які демонструють різноманітність їхніх функцій, рівнів інтеграції та сфер застосування [2, 6].

1. Національна гвардія України. В останні роки у структурі НГУ активно впроваджуються елементи інформаційно-аналітичного забезпечення службово-бойової діяльності. Зокрема, функціонують оперативно-аналітичні центри, які здійснюють моніторинг поточної обстановки у районах відповідальності, збирання даних із підрозділів, безпілотних літальних апаратів, систем відеоспостереження та відкритих джерел (OSINT).

На основі цих даних формується ситуаційна картина, що дозволяє командирам оперативно оцінювати ризики, планувати дії підрозділів і прогнозувати можливі сценарії розвитку подій.

Такі аналітичні центри інтегровані із системами управління бойовими підрозділами та зв’язку, що значно скорочує час між отриманням інформації і прийняттям рішення. Розробляються програмні модулі для автоматизації аналізу даних із використанням елементів штучного інтелекту, наприклад, для виявлення підозрілих об’єктів у відеопотоці або визначення імовірних напрямів переміщення диверсійних груп.

2. Система «АрміяІнформ» та Центр стратегічних комунікацій. Інформаційно-аналітичні інструменти застосовуються не лише у військовому управлінні, але й у сфері інформаційної протидії.

Важливу роль відіграє Центр стратегічних комунікацій та інформаційної безпеки при Міністерстві культури та інформаційної політики України. Центр забезпечує моніторинг інформаційного простору, виявлення кампаній дезінформації, формування аналітичних звітів і прогнозів щодо інформаційних впливів з боку держав-агресорів [2, 6].

Система «АрміяІнформ», зі свого боку, використовує алгоритми контент-аналізу та семантичного оброблення даних для виявлення тенденцій у публічному дискурсі про Збройні Сили України. Це дає змогу вчасно реагувати на інформаційні атаки, координувати комунікаційну політику оборонного сектору та формувати позитивний імідж сил безпеки.

3. Єдина державна система кіберзахисту (Держспецзв’язок). Важливим прикладом є створення та розвиток Національного координаційного центру кібербезпеки (НКЦК) при Раді національної безпеки і оборони України.

Цей центр здійснює збирання, аналіз та узагальнення інформації про кіберінциденти, а також координацію взаємодії між державними установами, військовими формуваннями та приватним сектором.

Інформаційно-аналітичні системи НКЦК містять модулі моніторингу мережевого трафіку, автоматичного виявлення шкідливих впливів, прогнозування потенційних атак і оцінки рівня кіберстійкості критичної інфраструктури.

У межах ініціативи «Cyber Rapid Response Teams» спільно з партнерами з ЄС створено платформу обміну аналітичними даними (Threat Intelligence Sharing), що дають можливість у реальному часі виявляти та нейтралізувати загрози.

4. Аналітична система «Ситуаційний центр МВС». У системі Міністерства внутрішніх справ України функціонує Єдина аналітична платформа МВС, яка об'єднує бази даних Національної поліції, Державної прикордонної служби, Національної гвардії, Державної служби України з надзвичайних ситуацій та інших структур.

Система дозволяє здійснювати інтегрований аналіз оперативної обстановки, прогнозувати виникнення кризових ситуацій, визначати «гарячі точки» злочинності, координувати міжвідомчі дії.

Особливістю цієї платформи є використання геоінформаційних технологій, що забезпечують просторове відображення подій, маршрути патрулів, зони контролю та ризикові території. На практиці це дає змогу швидше реагувати на правопорушення та раціональніше розподіляти сили й засоби безпеки.

Крім того, система підтримує алгоритми машинного навчання для виявлення закономірностей у кримінальних подіях і побудови моделей прогнозування.

5. Аналітичні системи розвідки та оборонного аналізу. Сили оборони України активно використовують інформаційно-аналітичні системи типу «Delta», розроблену Центром інновацій та розвитку оборонних технологій Міноборони [2, 6].

Зазначена система є інтегрованою геоінформаційною платформою, що дає можливість об'єднувати дані з безпілотних літальних апаратів, супутникових знімків, радіолокаційних засобів, соціальних мереж і відкритих джерел.

Вона забезпечує командирів актуальною оперативною інформацією про обстановку на полі бою, дозволяє відслідковувати пересування противника в реальному часі, здійснювати аналіз і прогнозування бойової ситуації.

Система має високий рівень сумісності з платформами партнерів НАТО, що підвищує ефективність міжнародної взаємодії та обміну даними.

Фактично «Delta» стала прикладом успішного поєднання національних аналітичних рішень і міжнародних технологічних стандартів.

6. Використання інформаційно-аналітичних систем у сфері цивільного захисту. Державна служба України з надзвичайних ситуацій активно застосовує системи моніторингу надзвичайних подій, які інтегрують дані з метеорологічних станцій, геоданих, сенсорних мереж і мобільних додатків громадян.

Такі системи, як «Rescuer» та «Ситуаційний центр ДСНС», забезпечують оперативну візуалізацію місць подій, координацію дій рятувальних підрозділів, оцінку масштабів загроз і прогнозування розвитку надзвичайних ситуацій.

Особлива увага приділяється створенню інтелектуальних аналітичних моделей, які на основі історичних даних дають змогу оцінювати ризики природних катастроф або техногенних аварій [2, 6].

7. Інтеграція аналітичних рішень у систему державного управління. На рівні уряду створено Єдину інформаційно-аналітичну систему «Безпечна країна», що об'єднує інформаційні ресурси різних міністерств і служб. Ця система дає можливість здійснювати комплексну оцінку стану національної безпеки, моделювати вплив економічних, соціальних та військових чинників, формувати аналітичні довідки для урядових структур і Ради національної безпеки та оборони.

У межах цифрової трансформації запроваджуються аналітичні модулі у платформах «Дія» та «Трембіта», які створюють передумови для формування єдиного інформаційного середовища безпеки держави.

Практичне впровадження інформаційно-аналітичних систем в Україні демонструє поступовий перехід від розрізнених інформаційних ресурсів до інтегрованих аналітичних платформ, які забезпечують не лише оброблення даних, а й підтримку стратегічного управління у сфері безпеки.

Водночас зберігаються проблеми сумісності міжвідомчих систем, брак кваліфікованих аналітиків і потреба у створенні єдиних стандартів обміну даними. Подальший розвиток цих систем має відбуватися на основі принципів міжвідомчої інтеграції, кіберстійкості, використання штучного інтелекту та міжнародної кооперації.

Інформаційно-аналітична діяльність у сфері безпеки охоплює сукупність процесів збирання, оброблення, аналізу та поширення інформації, необхідної для прийняття управлінських рішень. Вона містить:

1) збирання інформації з різних джерел: відкритих, закритих, технічних, розвідувальних;
2) оброблення та систематизацію даних для подальшого аналізу;
3) аналіз інформації з використанням сучасних методів та технологій;
4) прогнозування можливих загроз та сценаріїв розвитку подій;
5) розроблення рекомендацій для органів управління та безпеки.

Інформаційно-аналітичний складник у системі безпеки виконує такі основні функції [2, 6]:

1) моніторинг ситуації: постійне спостереження за внутрішніми та зовнішніми чинниками, що можуть впливати на безпеку;
2) прогнозування загроз: оцінка ймовірності виникнення кризових ситуацій та їхніх можливих наслідків;
3) підтримка прийняття рішень: надання аналітичних матеріалів для обґрунтованих управлінських рішень;
4) оцінювання ефективності заходів безпеки: аналіз результатів упроваджених заходів та корегування стратегії безпеки.

Сучасні технології значно поліпшили ефективність інформаційно-аналітичної діяльності. До основних методів та технологій належать:

– великі дані: оброблення великих обсягів інформації для виявлення закономірностей та трендів;
– штучний інтелект: використання алгоритмів машинного навчання для автоматизації аналізу даних;
– геоінформаційні системи: візуалізація та аналіз просторової інформації для оцінювання ситуації;
– системи підтримки прийняття рішень: інструменти для моделювання різних сценаріїв та оцінювання їхніх наслідків.

Напрямами подальшого розвитку інформаційно-аналітичного складника системи безпеки держави можна вважати:

1) інтеграцію новітніх технологій: використання блокчейн-технологій для забезпечення цілісності даних, розвиток квантових обчислень для підвищення швидкості оброблення інформації;
2) міжнародну співпрацю: розширення обміну даними та координації дій між країнами й міжнародними організаціями;
3) освітні програми: підготовка кадрів через спеціалізовані навчальні програми та підвищення кваліфікації наявних фахівців.

Висновки

Інформаційно-аналітичний складник є невід'ємною частиною сучасної системи безпеки. Він забезпечує своєчасне виявлення загроз, обґрунтоване прийняття рішень та ефективну координацію дій між різними структурами. Успішний розвиток цього складника вимагає інтеграції новітніх технологій, підготовки кваліфікованих кадрів та міжнародної співпраці.

Досвід США свідчить, що інформаційно-аналітичні системи є стрижнем національної безпеки і ключовим чинником швидкого реагування на загрози будь-якого характеру – військові, кібернетичні, терористичні чи природні. Вони об’єднують технології великих даних, штучного інтелекту, біометрії, супутникового моніторингу й мережевої аналітики в єдину систему управління безпекою. Україна, адаптуючи цей досвід, може створити інтегровану багаторівневу систему аналітичної підтримки рішень у секторі безпеки, орієнтовану на міжвідомчу взаємодію, кіберзахист і оперативну координацію.

Досвід Європейського Союзу показує, що ефективна система безпеки базується на мережевій взаємодії та спільному аналітичному середовищі. Європейський Союз досяг значних результатів у створенні інтероперабельних інформаційно-аналітичних систем, що охоплюють правоохоронну, прикордонну, кібернетичну та зовнішньополітичну сфери. Ключовими принципами є інтеграція, прогнозування, аналітика та додержання правових норм щодо захисту даних.

Отже, ефективне функціонування інформаційно-аналітичного складника у сфері державної безпеки потребує комплексного вирішення низки проблем – від технологічних і кадрових до правових і координаційних. Подолання цих викликів можливе лише за умови інституційної інтеграції, інноваційного оновлення, розвитку аналітичної культури та міжвідомчої взаємодії.

Перспективи подальших досліджень вбачаємо в аналізі та розвитку міжвідомчої взаємодії суб'єктів сил безпеки та оборони України, дослідженні можливостей з інституційної інтеграції інформаційно-аналітичного складника у сфері державної безпеки.

Перелік джерел посилання

1. Ситник Г. П. Державне управління у сфері національної безпеки (концептуальні та організаційно-правові засади) : підручник. Київ : НАДУ, 2011. 730 с.
2. Споришев К. О. Інформаційно-аналітичні технології сил безпеки у парадигмі державного управління. *Наукові інновації та передові технології. Управління та адміністрування.* 2024. № 1 (29). С. 128–136.
3. Основи інформатизації Національної гвардії України : навч. посіб. / Г. А. Дробаха та ін. Харків : НА НГУ, 2016. 366 с.
4. Бєлай С. В., Споришев К. О. Вплив стану системи інформаційно-аналітичного забезпечення сил безпеки України на державну безпеку. *Наукові інновації та передові технології. Управління та адміністрування.* 2024. № 2 (30). С. 29–37.
5. Кириченко І. О., Горєлишев С. А., Побережний А. А. Технологічні основи інформаційно-аналітичного забезпечення службово-бойової діяльності сил охорони правопорядку : монографія. Харків : Акад. ВВ МВС України, 2013. 292 с.
6. Бєлай С. В., Споришев К. О. Системи підтримки прийняття рішень у державному управлінні силами безпеки України. *Актуальні питання у сучасній науці. Державне управління.* 2024. № 2 (20). С. 320–329.
7. Споришев К. О. Розвиток менеджменту кадрових ресурсів в системі інформаційно-аналітичного забезпечення сил безпеки України. *Актуальні питання у сучасній науці. Державне управління.* 2024. № 3 (21). С. 410–421.
8. U.S. Department of Homeland Security (CISA). Cybersecurity Strategic Plan 2023–2027. Washington, D.C. : DHS, 2023.
9. European Union Agency for Cybersecurity (ENISA). Threat Landscape 2024 Report. Brussels : ENISA Publications, 2024.
10. Europol. European Union Serious and Organised Crime Threat Assessment (SOCTA 2024). The Hague : Europol Press, 2024.

Стаття надійшла до редакції 24.10.2025 р.

UDC 351.86:004.9(477)

K. Sporyshev, V. Klishyn, V. Belousov

THE ROLE OF THE INFORMATION AND ANALYTICAL COMPONENT IN THE FIELD OF STATE SECURITY

The article explores the role and significance of information and analytical systems in ensuring Ukraine's national security under conditions of hybrid threats, cyber confrontation, and rapid technological advancement. It emphasizes that modern security processes are impossible without systematic data collection, analysis, forecasting, and interpretation, which together form the basis for informed managerial decision-making in crisis situations. The main problem is identified as the absence of a unified mechanism for utilizing information-analytical systems in the activities of security forces, which results in data fragmentation and reduces the effectiveness of responses to emerging threats.

The study reveals the essence and current trends in the development of analytical support in Ukraine and outlines key directions of digital transformation in the security sector. A comparative analysis is conducted of the practical use of information-analytical systems in Ukraine, the United States, and the European Union. Particular attention is devoted to analyzing major problems and challenges – cyber threats, personnel shortages, technological fragmentation, legal limitations, and insufficient integration of

interagency data resources. The importance of developing cyber resilience, interagency cooperation, and an analytical decision-making culture is emphasized.

The article proposes a set of measures to improve the information-analytical mechanism of state management in the field of security, including the creation of a unified national analytical center, the unification of data exchange formats, the implementation of intelligent data-processing algorithms, and the establishment of an advanced system for training next-generation specialists. The obtained results have practical value for optimizing management processes in the security sector and enhancing the effectiveness of state responses to contemporary threats.

Keywords: *state security, information and analytical activities, decision support sestems, security forces.*

Споришев Костянтин Олександрович – доктор наук з державного управління, доцент, заступник начальника навчально-наукового інституту підготовки керівних кадрів з наукової роботи – начальник науково-дослідної лабораторії будівництва та оперативного застосування НГУ, Національна академія Національної гвардії України
https://orcid.org/0000-0003-4737-9698

Клішин Віктор Миколайович – кандидат військових наук, доцент, начальник навчально-наукового інституту підготовки керівних кадрів, Національна академія Національної гвардії України
https://orcid.org/0000-0002-5291-5160

Белоусов Володимир Леонідович – ад'юнкт, Національна академія Національної гвардії України
https://orcid.org/0009-0009-8550-2694