УДК 343.341:323.28(477)
DOI https://doi.org/10.32844/2618-1258.2023.3.21

ГОРБ В. В.

АКТУАЛЬНІ ПИТАННЯ ІНФОРМАЦІЙНОЇ ВЗАЄМОДІЇ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

CURRENT ISSUES OF INFORMATION INTERACTION OF THE SECURITY SERVICE OF UKRAINE

У статті наведено авторське бачення стану автоматизованого обміну інформацією в електронній формі всередині Служби безпеки України та з взаємодіючими силовими структурами. Зазначено на динамічній цифровій трансформації нашої держави в сучасних умовах, високих позиціях у світових рейтингах досліджень електронного уряду та відкритих даних. Проведено огляд нормативно-правових джерел, що регламентують організацію інформаційної взаємодії, визначено регламентований порядок її реалізації, а також розкрито фактичний стан обміну інформацією у сфері службової діяльності. Розглянуто співвідношення центральної підсистеми єдиної інформаційної системи Міністерства внутрішніх справ і системи електронної взаємодії державних електронних інформаційних ресурсів «Трембіта», вказано про єдину систему інформаційного забезпечення оперативно-розшукової, контррозвідувальної, аналітичної, управлінської та іншої діяльності СБУ «Синтез» як про таку, що не відповідає вимогам інтероперабельності і являється застарілою, вузькоспеціалізованою. Проведений огляд інформаційної взаємодії в СБУ через використання паперового документообігу, шифрованого зв'язку, систему електронного документообігу. Визначено недоліки і переваги кожного з видів взаємодії. Акцентовано увагу на високому рівні комунікації силовиків за допомогою мобільних застосунків внаслідок нестачі швидкодоступних програмних і апаратних засобів для передачі службових повідомлень і електронних файлів. Позитивно охарактеризовані процеси перебудови єдиної інформаційної системи МВС України. Зроблено висновок про необхідність проведення інтенсивної інформатизації і цифровізації вітчизняної спецслужби шляхом побудови сучасної інтероперабельної єдиної системи інформаційного забезпечення, інтеграції до неї вже існуючих інформаційно-довідкових банків даних, а також впровадження в оперативно-службову діяльність спеціального службового месенджера з високою надійністю криптографічних протоколів.

Ключові слова: *інформатизація, інформаційна взаємодія, інформаційна система, об'єднана автоматизована інформаційна система у сфері боротьби з тероризмом, Служба безпеки України, Міністерство внутрішніх справ України.*

The article presents the author's vision of the state of automated information exchange in electronic form within the Security Service of Ukraine and with cooperating law enforcement agencies. It is noted for the dynamic digital transformation of our state in modern conditions, high positions in the world rankings of e-government research and open data. A review of regulatory and legal sources regulating the organization of information interaction was carried out, the regulated procedure for its implementation was determined, and the actual state of information exchange in the field of official activity was revealed. The ratio of the central subsystem of the unified information system of the Ministry of Internal Affairs and the system of electronic interaction of state electronic information resources «Trembita» was considered, the unified system of information support for operative-research, counter-intelligence, analytical, management and other activities of the SSU «Sintez» was indicated as such that it does not meets

© ГОРБ В.В. – полковник, співробітник (Служба безпеки України)

the requirements of interoperability and is outdated, highly specialized. An overview of information interaction in the SSU through the use of paper document circulation, encrypted communication, and an electronic document circulation system was conducted. The disadvantages and advantages of each type of interaction are determined. Attention is focused on the high level of communication by law enforcement officers using mobile applications due to the lack of readily available software and hardware for transmitting official messages and electronic files. The processes of reconstruction of the unified information system of the Ministry of Internal Affairs of Ukraine have been positively characterized. A conclusion was made about the need for intensive informatization and digitization of the domestic special service by building a modern interoperable unified information support system, integrating existing information and reference data banks into it, as well as introducing a special service messenger with high reliability of cryptographic protocols into operational and service activities.

Key words: *informatization, information interaction, information system, unified automated information system in the field of combating terrorism, Security Service of Ukraine, Ministry of Internal Affairs of Ukraine.*

Постановка проблеми. До пріоритетних завдань запобігання терористичній діяльності, вирішення яких закріплено у «Концепції боротьби з тероризмом в Україні», віднесено підвищення рівня координації діяльності суб'єктів боротьби з тероризмом, запровадження дієвих механізмів взаємодії та обміну інформацією між суб'єктами боротьби з тероризмом та іншими державними органами, а також удосконалення інформаційно-аналітичного забезпечення заходів боротьби з терористичною діяльністю, насамперед шляхом впровадження сучасних форм, методів і технологій добування, оброблення та використання інформації. Процес антитерористичного забезпечення об'єктів можливих терористичних посягань передбачає функціонування об'єднаної автоматизованої інформаційної системи у сфері боротьби з тероризмом [1].

Попередження терористичної діяльності через застосування новітніх інформаційно-комунікаційних технологій корелюється з загальнодержавним планом інформатизації, Законом України «Про Національну програму інформатизації» [2].

Поряд з визнанням в Концепції Національної програми інформатизації незадовільного стану інформатизації в Україні станом на 1998 рік також декларується, що «обчислювальна та комунікаційна техніка, електронні комунікаційні мережі, бази і банки даних та знань, інформаційні технології (ІТ), система інформаційно-аналітичних центрів різного рівня, виробництво технічних засобів інформатизації, системи науково-дослідних установ та підготовки висококваліфікованих фахівців є складовими національної інформаційної інфраструктури і основними чинниками, що забезпечують економічне піднесення. Як показує досвід інших країн, інформатизація сприяє забезпеченню національних інтересів, поліпшенню керованості економікою, розвитку наукоємних виробництв та високих технологій, зростанню продуктивності праці, вдосконаленню соціально-економічних відносин, збагаченню духовного життя та подальшій демократизації суспільства. Національна інформаційна інфраструктура, створена з урахуванням світових тенденцій і досягнень, сприятиме рівноправній інтеграції України у світове співтовариство» [3].

Констатовані 25 років тому сподівання від інформатизації набувають дедалі більшої актуальності у сьогоденному житті країни. Останні роки цифрова трансформація України є динамічною. Світова спільнота солідарна з таким твердженням. Так, за результатами дослідження електронного уряду ООН (United Nations E-government Survey 2016) рейтинг України у 2022 році становив 46 з 193 держав-членів. У 2018 році цей показник становив 82 місце, у 2020 – 69.

Серед 35 країн-претенденток у 2022 році Україна зайняла 2 місце в рейтингу European Open Data Maturity Report серед країн Євросоюзу. З 2020 року наша держава перебуває у переліку країн, що швидко розвиваються зберігаючи позитивну тенденцію розвитку сфери відкритих даних: у 2021 і 2020 роках ми посідали 6 і 17 місце відповідно.

Високими оцінками удостоєні такі складові рейтингу як державна політика, єдиний державний веб-портал відкритих даних, ряд реалізованих в Україні проєктів на основі відкритих даних під патронатом Міністерства цифрової трансформації та міжнародного проєкту USAID/ UK aid/TAPAS Project.

На фоні здобутих досягнень на шляху побудови e-Government в Україні дисонують негативні прояви залишків бюрократії, анахронічні підходи до організації інформаційної взаємодії в окремих державних структурах, зокрема, сектору безпеки і оборони.

Аналіз останніх досліджень і публікацій. Перспективні погляди щодо напрямів удосконалення процедур взаємодії задіяних у антитерористичній діяльності суб'єктів викладені у наукових працях Крутова В.В. Необхідність оптимізації, формалізації та структурування інформаційних потоків, створення комп'ютерних баз даних і систем управління ними, залучення і адаптації до завдань антитерористичної діяльності штучного інтелекту з метою підвищення оперативності та ефективності збору, попередньої обробки інформації, яка надходить до її споживачів були предметом наукових досліджень згаданого науковця понад двадцять років тому [4].

Про актуальність та нагальну необхідність створення дієвої системи аналізу загроз терористичного характеру та оцінювання їх впливу на найважливіші сфери забезпечення національної безпеки, яка б базувалася на сучасних інформаційних технологіях та забезпечувала протидію цим загрозам у режимі реального часу неодноразово наголошував у своїх працях вчений-дослідник Рижов І.М. [5].

Внесок у науковий доробок у сфері інформаційної діяльності правоохоронних органів зробили українські дослідники Бандурка О.М., Мельнікова О.О., Овчинський В.С. та інші.

Стрімкий розвиток інформаційних технологій та їх активне впровадження в усі сфери нашого життя обумовлює попит на проведення різноспрямованих наукових пошуків в процесі переходу до нового типу інформаційного суспільства.

Мета статті. Охарактеризувати реальний стан інформаційної взаємодії всередині та ззовні Служби безпеки України на підставі чого обґрунтувати необхідність проведення інформатизації сфер оперативно-службової діяльності та її забезпечення, сформувати ключові пропозиції напрямів інформатизації.

Виклад основного матеріалу. Автоматизований обмін інформацією в електронній формі в порядку інформаційної взаємодії між СБУ, МВС, НП, ДПСУ, ДСНС регламентований «Порядком електронної інформаційної взаємодії Служби безпеки України, Міністерства внутрішніх справ України та центральних органів виконавчої влади, діяльність яких спрямовується та координується Кабінетом Міністрів України через Міністра внутрішніх справ України», що затверджений наказом СБУ, МВС України від 13 жовтня 2022 року № 360/657 (далі – Порядок).

Згідно з п. 3 розділу ІІ Порядку, інформаційна взаємодія здійснюється з використанням інформаційних систем суб'єктів інформаційних відносин, зокрема засобами центральної підсистеми єдиної інформаційної системи Міністерства внутрішніх справ (ЦП ЄІС МВС) або системи електронної взаємодії державних електронних інформаційних ресурсів («Трембіта»).

За відсутності технічної можливості передачі даних із використанням ЦП ЄІС МВС і «Трембіти» інформаційна взаємодія суб'єктів інформаційних відносин може здійснюватися з використанням інших інформаційних систем із застосуванням у них відповідних комплексних систем захисту інформації з підтвердженою відповідністю [6].

У разі відсутності можливості забезпечення доступу до інформації в ресурсах суб'єктів інформаційних відносин з використанням інформаційних систем, визначених у пункті 3 розділу ІІ Порядку, доступ може надаватися з урахуванням установлених законодавством вимог та з дотриманням визначених суб'єктами інформаційних відносин процедур доступу до таких систем (п. 4 р. ІІ Порядку).

Тож, Порядком визначено чотири способи інформаційної взаємодії суб'єктів інформаційних відносин, зокрема через:

– ЦП ЄІС МВС;

– систему електронної взаємодії державних електронних інформаційних ресурсів «Трембіта»;

– відомчі інформаційні системи з атестатом відповідності комплексних систем захисту інформації;

– безпосередній доступ визначеного користувача до затребуваних інформаційних ресурсів.

Відповідно до заявлених суб'єктів е-взаємодії ЄІС МВС, за своєю архітектурою вона є міжвідомчою, а в окремих випадках запитів до неї – інтернаціональною (міждержавною) інформаційною системою [7].

Використання ЦП ЄІС МВС передбачає електронну ідентифікацію та автентифікацію користувачів, розмежування прав доступу та надання ним контрольованого доступу до наявних інформаційних ресурсів, ведення системних журналів дій користувачів тощо, а також забезпечення електронної взаємодії автоматизованих систем у режимі «система-система» або в інший спосіб [8].

З цього випливає, що доступ до ЦП ЄІС МВС потребує кваліфікованого електронного підпису, а електронний міжсистемний обмін даними передбачає інтероперабельність та уніфікацію доступу.

Інтероперабельність «Трембіти», побудованій на базі платформи обміну даними X-ROAD і ЄІС МВС очевидна, оскільки остання є підсистемою «Трембіти» [9].

Доступ до інформаційних ресурсів ЄІС МВС в режимі «користувач-система», на думку автора, не є комплексним рішенням і не забезпечує міжвідомчу взаємодію в затребуваному обсязі.

Тому питання побудови інформаційної взаємодії СБУ з взаємодіючими структурами шляхом використання відомчих інформаційних систем потребує детального розгляду і являється предметом даної наукової розвідки. Цілком логічно, що задля забезпечення функціональної сумісності внутрішніх систем СБУ з сучасними периферійними інформаційними системами вони в першу чергу повинні бути створені і використовуватись всередині самої спецслужби. Єдина система інформаційного забезпечення оперативно-розшукової, контррозвідувальної, аналітичної, управлінської та іншої діяльності СБУ «Синтез» (ЄСІЗ «Синтез») за своєю сутністю є закритою системою, яка побудована на застарілих інформаційних технологіях і не має підключення до глобальної інформаційної мережі. В реальності, прикладний функціонал ЄСІЗ «Синтез» зведений до банку даних, який накопичує і видає різнопланову інформацію у відношенні об'єктів оперативної зацікавленості СБУ.

Найбільш характерні способи внутрішньої інформаційної взаємодії в СБУ такі:

1. Шляхом паперового документообігу.
2. З використанням апаратури, яка забезпечує шифрований, шифрований електронний документообіг.
3. Через систему електронного документообігу (СЕДо).

Паперовий документообіг здійснюється через Головне управління урядового фельд'єгерського зв'язку Державної служби спеціального зв'язку та захисту інформації України і його регіональні підрозділи, представництва Державної фельд'єгерської служби України, станції фельд'єгерсько-поштового зв'язку Збройних Сил України. Такому способу приймання і передавання матеріальних носіїв інформації притаманний великий обсяг людських зусиль (людино-годин), обумовлений широким спектром типових операцій: реєстрація документа, внесення необхідних відміток в облікові форми, конвертування та оформлення відправлень, підготовка реєстрів на відправку, пересилання кореспонденції між установами і населеними пунктами. Адресат, що отримав кореспонденцію, виконує практично аналогічний набір операцій у зворотному порядку.

Нинішні умови війни зумовили перебування ряду державних органів поза пунктами постійної дислокації, внаслідок чого до типових транспортних ланцюжків включено додаткові транзитні ланки. Емпіричний досвід засвідчує, що часові показники такого способу інформаційної взаємодії зазвичай закономірні, вимірюються днями, як правило від трьох і більше. На фоні стрімкого розвитку ІТ-технологій, зокрема, інститутів електронного документообігу, цифрового підпису, широкого арсеналу алгоритмів криптозахисту інформації, паперовий обіг документів стає архаїчним. В перспективі він має суттєво втратити сьогоденні обсяги пересилань і зайняти нішу особливо важливих і особисто адресованих відправлень.

Шифрований документообіг дозволяє скоротити часові затрати на пересилання інформації між абонентами мало не на порядок. Окрім зменшення кількості персоналу, задіяного у процесі підготовки та пересилання, пов'язаних з цим типових операцій, сучасні зразки шифрувальної апаратури забезпечують високу криптографічну стійкість, мають інтуїтивно зрозумілий програмний інтерфейс. За рахунок викотехнологічності і модульності побудови досягнута мобільність (як приклад – комплекс «Абак-МЕ»). До недоліків слід віднести дороговартість шифрувального обладнання, що обумовлює її розподіл між окремо дислокованими підрозділами.

Система електронного документообігу (СЕДо) або EDMS (Electronic Document Management Systems) – це програмне забезпечення з можливістю створювати, поширювати і контролювати ланцюжок передачі документів всередині мережі. Доступний функціонал е-документообігу дозволяє автоматизувати і оптимізувати роботу з електронними документами, здійснювати їх обробку в рамках одного програмного інструментарію, одноразову реєстрацію з можливістю подальшої ідентифікації, контроль руху документа з можливістю визначення відповідального за його виконання, архівування, моніторинг дотримання встановлених термінів проходження і виконання документів [10].

Вищенаведені способи інформаційного обміну як в СБУ, так і в МВС, інших силових структурах слід віднести до формальних, загальноприйнятних. Натомість реальний стан речей дещо інший.

В мирний і особливо у воєнний час відсутність оперативної можливості передати інформацію або електронний документ для його реалізації компенсується за рахунок повсюдного

використання мобільних застосунків для смартфонів, планшетів, ноутбуків. Серед широкого вибору таких додатків найбільш поширені в силу належності до країни-розробника софту та особливостей безпекових сервісів – WhatsApp, Signal, Telegram. Рівень комунікації в силових структурах за допомогою т.зв. «месенджерів» нині можна констатувати як тотальний. Окрім обміну повідомленнями, використання можливостей IP-телефонії, функціонал вказаних застосунків дозволяє передавати формати текстових, структурованих, графічних даних, архіви тощо. Нині, отримання інформації визначеними співробітниками СБУ з ЄСІЗ «Синтез», обліків та інформаційних масивів МВС України реалізується через створену в Signal групу «Рубін».

Тож наразі у сфері внутрішнього службового документообігу в СБУ існує певна дилема, що полягає в обумовленій, здебільшого, крайньою необхідністю потребі швидкого інформаційного обміну службовою інформацією (в т.ч. з обмеженим доступом) та водночас відсутності достатньої кількості швидкодоступних програмних і апаратних засобів для її передачі. Особливої актуальності дана проблема набуває у районах ведення бойових дій, в умовах територіальної віддаленості співробітників від своїх організаційних центрів.

Свідченням переосмислення підходів до інформаційного забезпечення в МВС України є реновація її єдиної інформаційної системи. В межах реалізації сучасних галузевих програм – Концепцій програм інформатизації на 2018–2020, 2021–2023 роки [11], у даному відомстві успішно втілені Інформаційний портал Національної поліції України, оновлена Інтегрована інформаційно-пошукова система (раніше – «АРМОР», включає понад 17 підсистем різної тематичної спрямованості), інформаційні системи «Цунамі», «Арсенал», «Оріон», автоматична дактилоскопічна інформаційна система «ДАКТО», продовжується робота над іншими проєктами цифрової трансформації. Існує можливість безпосереднього доступу поліціянтів до інформації та інформаційних ресурсів інших органів державної влади.

На погляд автора, подолання існуючих негараздів в СБУ полягає в проведенні інтенсивної інформатизації (цифровізації) відомства, в першу чергу шляхом побудови сучасної ЄСІЗ з підсистемами інтеграційної взаємодії, мережевої доставки даних, єдиного розподіленого сховища даних (Інтернет-орієнтованого і закритого, реляційного та неструктурованого), технологіями єдиного входу, наскрізного ідентифікатора, електронної ідентифікації та автентифікації користувачів тощо. В межах ЄСІЗ слід реалізувати інтеграцію вже існуючих інформаційних банків, таких як електронний довідник «Піраміда» (ДІАЗ СБУ), ІПС «АРМОР» і Єдиний державний реєстр транспортних засобів (МВС України), «Єдиний державний демографічний реєстр (Державна міграційна служба України), реєстри Міністерства юстиції України та інші.

Об'єднана автоматизована інформаційна система у сфері боротьби з тероризмом, як підсистема ЄСІЗ СБУ, повинна об'єднати такі бази даних, як «Перелік терористів» (Державна служба фінансового моніторингу), «Реєстр осіб, які підозрюються в причетності до терористичної діяльності, незаконних збройних формувань, сепаратизму та колабораціонізму» (ДІАЗ СБУ), списки колаборантів (Штаб АТЦ при СБУ), полонених (об'єднаний центр з пошуку та звільнення полонених), система обробки попередньої інформації про пасажирів (API/PNR), а також спеціальну інформаційну систему щодо загроз і вразливостей критичній інфраструктурі (Держспецзв'язок).

Для задоволення потреб інформаційного обміну безпосередньо між оперативними співробітниками, на погляд автора, доречно розробити і впровадити спеціальний службовий месенджер з високою надійністю криптографічних протоколів та атестатом відповідності комплексних систем захисту інформації.

Окрім інформатизації пріоритетних напрямів службової діяльності, які прямо впливають на ефективність контррозвідувального пошуку, режиму, перевірки і розробки, впровадження електронної взаємодії потребують підрозділи забезпечення агентурно-оперативного процесу (інформаційно-аналітичні, кадрові, фінансові, господарські, режимно-секретні). Основна мета – зменшення негативних проявів бюрократизму: великих термінів проходження документів в інстанціях, їх погодження і візування, викорінення ведення анахронічних облікових форм, накопичення великих обсягів справ і архівів.

Підсумовуючи вищевикладене, можна констатувати, що для автоматизованого обміну інформацією в електронній формі, передбаченого вимогами Порядку, в СБУ нині відсутня інтероперабельна інформаційна система. Її побудова дозволить оптимізувати процеси внутрішньої та зовнішньої інформаційної взаємодії. Інтенсифікація електронної взаємодії через інформаційні системи, всеохоплюючу мережу електронного документообігу, криптографічного захисту інформації призведе до мінімізації паперового документообігу.

Список використаних джерел:

1. Указ Президента України «Про Концепцію боротьби з тероризмом в Україні» від 05.03.2019 року № 53/2019. Редакція від 05.03.2019. URL: https://zakon.rada.gov.ua/laws/show/53/2019?lang=ru (дата звернення: 12.09.2023).

2. Закон України «Про Національну програму інформатизації» від 01.12.2022 року № 2807-IX. Редакція від 01.12.2022. URL: https://zakon.rada.gov.ua/laws/show/2807-20#Text (дата звернення: 12.09.2023).

3. Закон України «Про Концепцію Національної програми інформатизації» від 04.02.1998 року №75/98-ВР. Редакція від 01.01.2022. URL: https://ips.ligazakon.net/document/Z980075?an=4 (дата звернення: 12.09.2023).

4. Крутов В.В. Теоретико-правові і тактико-спеціальні проблеми боротьби з тероризмом (досвід системного дослідження) : монографія / НА СБУ, Київ, 1998.

5. Рижов І.М. Загрози терористичного характеру: формалізація, аналіз, оперативна протидія : монографія / НА СБУ, Київ, 2017.

6. Порядок електронної інформаційної взаємодії Служби безпеки України, Міністерства внутрішніх справ України та центральних органів виконавчої влади, діяльність яких спрямовується та координується Кабінетом Міністрів України через Міністра внутрішніх справ України : затверджений наказом СБУ, МВС України від 13.10.2022 року № 360/657. Редакція від 13.10.2022. URL: https://zakon.rada.gov.ua/laws/show/z1327-22#Text, (дата звернення: 12.09.2023).

7. Веб-ресурс «Державна ІТ-компанія «ІНФОТЕХ», ЄІС МВС». URL: https://infotech.gov.ua/projects/eis-mvs.

8. Порядок функціонування центральної підсистеми єдиної інформаційної системи Міністерства внутрішніх справ України : затверджений наказом МВС України від 16.09.2020 року № 665. Редакція від 18.02.2022. URL: https://zakon.rada.gov.ua/laws/show/z1092-20#Text, (дата звернення: 12.09.2023).

9. Інтернет-ресурс: «Український соціологічний портал, проєкт EU4DigitalUA представляє перший за воєнний час квартальний звіт про роботу системи «Трембіта»». URL: https://usp-ltd.org/proiekt-eu4digitalua-predstavliaie-pershyj-za-voiennyj-chas-kvartalnyj-zvit-pro-robotu-systemy-trembita/.

10. Веб-сайт «EDIN. Як правильно вибрати і запровадити СЕД». URL: https://edin.ua/shho-take-sed-yak-pravilno-vibrati-ta-vprovaditi/#.

11. Наказ МВС України від 22 квітня 2021 року № 301 «Про оголошення рішення колегії МВС України». Концепція програми інформатизації системи МВС України та центральних органів виконавчої влади, діяльність яких спрямовується і координується КМУ через міністра внутрішніх справ України, на 2021–2023 роки. URL: https://mvs.gov.ua/upload/document/aN0v4D2pv1R2colEwISK67mEYRjQXKTwBjAiNoBK.pdf.