

## **ІНФОРМАЦІЙНИЙ НАПРЯМОК ВЗАЄМОДІЇ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ З ІНШИМИ СУБ'ЄКТАМИ СЕКТОРУ БЕЗПЕКИ ТА ОБОРОНИ**

**Андрій Ернестович ЯЦИНА,**

*здобувач ПВНЗ «Університет  
сучасних знань»*

Взаємодія Служби безпеки України з іншими суб'єктами сектору безпеки та оборони є складним процесом, який реалізується за різними напрямками, серед яких особливе місце належить інформаційному. Так, зокрема Порядок електронної інформаційної взаємодії Служби безпеки України, Міністерства внутрішніх справ України та центральних органів виконавчої влади передбачає, що інформаційна взаємодія здійснюється з використанням інформаційних систем суб'єктів інформаційних відносин, зокрема засобами центральної підсистеми єдиної інформаційної системи Міністерства внутрішніх справ або системи електронної взаємодії державних електронних інформаційних ресурсів [1]. Інструкція про взаємодію правоохоронних органів у сфері боротьби з організованою злочинністю встановлює, що з метою вдосконалення механізму взаємодії створюється централізований банк даних для збирання, накопичення, оброблення та подальшого використання інформації про прояви організованої злочинності. Обмін оперативною інформацією між спеціальними підрозділами по боротьбі з організованою злочинністю органів внутрішніх справ і СБУ під час проведення спільних заходів здійснюється за наявності оперативно-розшукової справи за письмовим розпорядженням керівників відповідних спеціальних підрозділів, у разі здійснення кримінального провадження – керівника відповідного органу досудового розслідування [2]. Слід зазначити, що обмін інформацією в багатьох випадках є основою для визначення подальших напрямів взаємодії.

Інформацією є будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [3]. Особливістю інформаційного напрямку взаємодії СБУ та інших суб'єктів сектору безпеки та оборони є необхідність додержання вимог законодавства щодо захисту інформації з обмеженим доступом. Такою визнається: 1) конфіденційна інформація; 2) таємна інформація; 3) службова інформація: а) що міститься в документах суб'єктів владних повноважень, які становлять внутрішньослужбову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напрямку діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень; б) зібрана

в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці [4].

Діяльність сектору безпеки та оборони стосується й охорони інформації, яка віднесена до державної таємниці (секретна інформація) – це вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою [5]. За своїм значенням державна таємниця є не просто державним атрибутом, а суттєвим ресурсом та цінністю, від стану захищеності якої залежить успішність державного управління та й навіть сам факт існування держави. На сьогодні спеціально уповноваженим органом державної влади у сфері забезпечення охорони державної таємниці є СБУ і надання дозволу на здійснення діяльності, пов'язаної з державною таємницею, здійснюється нею на підставі заявок установ та результатів спеціальної експертизи щодо наявності умов для провадження діяльності, пов'язаної з державною таємницею [6, с. 86-87].

Як зазначають В.І. Гурковський, І.П. Козак та С.Ф. Дмитрук, одним із ключових аспектів є розробка і впровадження інноваційних технологій та цифрових рішень для забезпечення безперервного, швидкого та надійного зв'язку між СБУ та ЗСУ. Такі технології допоможуть оперативно реагувати на зміни бойової обстановки, забезпечуючи передачу важливої інформації в режимі реального часу. Використання інтелектуальних аналітичних систем дозволить ефективно обробляти значний обсяг даних, що допоможе у швидкому розумінні загроз та прийнятті обґрунтованих рішень. Зростаюча роль кібербезпеки, кіберборотьби та кіберзахисту є невід'ємною частиною ефективної взаємодії. Забезпечення конфіденційності та цілісності даних, а також захист від кібератак, є критично важливим для запобігання несанкціонованому доступу та запобіганню намаганням технічної розвідки противника отримати доступ до інформації [7]. Слід погодитися з необхідністю запровадження новітніх технологій у всі напрями взаємодії суб'єктів сфери безпеки та оборони як складовий елемент досягнення її успішності.

Тож, інформаційний напрямок взаємодії Служби безпеки України з іншими суб'єктами сектору безпеки та оборони має ключове значення для забезпечення ефективного функціонування національної системи безпеки. Його сутність полягає у створенні та підтриманні безперервного обміну даними, аналітичними матеріалами, розвідувальною інформацією та прогнозами між державними органами, що дозволяє своєчасно виявляти, оцінювати й нейтралізувати потенційні загрози державній безпеці. Взаємодія за цим напрямом виступає центральною ланкою у формуванні спільного інформаційно-аналітичного середовища, у якому об'єднуються результати оперативно-службової діяльності, розвідувальні дані та стратегічні оцінки безпекових ризиків. Такий підхід сприяє

формуванню узгоджених рішень, уникненню дублювання функцій і посиленню аналітичного потенціалу всього сектору безпеки. Крім того, інформаційний напрямок взаємодії має важливе значення для протидії інформаційним операціям противника, зокрема у сфері кібербезпеки, медіапростору та психологічного впливу. Отже, інформаційна співпраця Служби безпеки України з іншими суб'єктами сектору безпеки та оборони є фундаментальним чинником забезпечення стійкості держави, підвищення її адаптивності до новітніх загроз і збереження національної цілісності в умовах складного безпекового середовища.

### **Список використаних джерел**

1. Про затвердження Порядку 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. Наказ Служби безпеки України та Міністерства внутрішніх справ України від 13.10.2022 р. № 360/657. URL: <https://zakon.rada.gov.ua/laws/show/z1327-22#Text>
2. Про затвердження Інструкції про взаємодію правоохоронних органів у сфері боротьби з організованою злочинністю. Наказ Міністерства внутрішніх справ України та Центрального управління Служби безпеки України № 317/235 від 10 червня 2011 року URL: <https://zakon.rada.gov.ua/laws/show/z0822-11#Text>
3. Про інформацію. Закон України від 2 жовтня 1992 р. № 2657-XII URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>
4. Про доступ до публічної інформації. Закон України від 13 січня 2011 р. № 2939-VI. URL: <https://zakon.rada.gov.ua/laws/show/2939-17#Text>
5. Про державну таємницю Закон України від 21 січня 1994 р. № 3855-XII. URL: <https://zakon.rada.gov.ua/laws/show/3855-12#Text>
6. Охорона державної таємниці в Україні: навч. посіб. / Гуз А.М., Касперський І.П., Князев С.О., та ін. Київ: Нац. акад.. СБУ. 2017.216 с.
7. Гурковський В.І., Козак І.П., Дмитрук С.Ф. Технологічні та комунікаційні виклики взаємодії СБУ та ЗСУ під час збройної агресії: пошук інноваційних рішень. Наукові перспективи. № 8 (38). 2023. URL: <http://perspectives.pp.ua/index.php/np/article/view/6039/6073>