

УДК 327.8

Г. Перепелиця, д-р політ. наук, проф.,
А. Дрозд, магістр
Київський національний університет імені Тараса Шевченка, Київ, Україна

СПЕЦСЛУЖБИ УКРАЇНИ ПЕРЕД СУЧАСНИМИ І МАЙБУТНІМИ ВИКЛИКАМИ

Проаналізовано оптимальні напрямки і шляхи розвитку міжнародного співробітництва, розбудови та реформування українських спецслужб з огляду на існуючу геополітичну ситуацію, а також сучасні і майбутні виклики українській та європейській безпеці.

Ключові слова: спецслужби України, Служба безпеки, Служба зовнішньої розвідки, ЄС, міжнародне співробітництво, реформа, розбудова, повномасштабне військове вторгнення РФ.

Нині українські спецслужби, як і інші органи, відповідальні за безпеку нашої держави, зіштовхнулися з безпрецедентним викликом – повномасштабним військовим вторгненням Російської Федерації. Гостро як ніколи постали наступні питання: "Яким чином використання можливостей міжнародного співробітництва може і має сприяти українським спеціальним службам у подоланні РФ?", "Як забезпечити належну інтеграцію України до європейського безпекового співтовариства з огляду на природну для неї роль форпосту європейської безпеки?", і найголовніше: "Яким чином реформувати і розбудувати спроможності спецслужб України у світлі унікальних викликів і загроз з боку Росії?".

Зважаючи на безпрецедентність нинішньої ситуації, досліджень у цьому напрямку досі не проводилося. Самі ж спецслужби, зрозуміло, зайняті безпосередньо боротьбою за власне виживання та виживання української держави. Однак не рухатись за течією, а знайти обдумані відповіді на вищезазначені питання дуже важливо.

Так, зважаючи на унікальний досвід і знання щодо форм і методів російської агресії, що здобуваються українськими розвідувальними та контррозвідувальними органами під час війни, очікувано, що саме співробітництво спеціальних служб може довести безальтернативну необхідність інтеграції України до ЄС з погляду безпекових інтересів Союзу. Служба безпеки України (СБУ) та Служба зовнішньої розвідки України (СЗРУ) зможуть підтримувати інституції ЄС та спецслужби держав-членів ЄС. Для української ж сторони важливою буде згуртована міжнародна підтримка і нарощування взаємодії з провідними безпеково-аналітичними центрами ЄС. Отже, роль міжнародного співробітництва в післявоєнний період буде значно зростати. Уся безпекова спільнота Європи повинна розуміти, що саме завдяки гібридним інформаційним технологіям, стратегічним комунікаціям, операціям впливу та непрозору лобіюванню Росія ще після 2014 року не опинилася за залізною завісою. А отже, протидія цим технологіям та операціям Росії має стати тим, довкола чого необхідно згуртуватися спецслужбам країн Європи. Варто сподіватися, що безальтернативною є створення системи колективного спротиву російським операціям впливу та дезінформації.

Як зазначено вище, в результаті війни, що триває, українські спецслужби отримують величезну кількість розвідувальних даних, знань і досвіду щодо діяльності російських військових і спецслужб, а також способів діяльності, пов'язаних з гібридною війною та кібервійною, розповсюдженням неправдивої інформації, різними формами тиску, маніпуляціями, мережевими операціями, терористичною та злочинною діяльністю, руйнуванням критичної інфраструктури та військовими діями.

Тому зі споживачів вони перетворюються на провідних донорів та гарантів загальноєвропейської безпеки, адже російська загроза є викликом номер один для фізичного існування держав Європи, зокрема східної. Таким чином, як нині, так і в післявоєнний час, СБУ і СЗР

мають хорошу можливість налагодити та розвивати сталу співпрацю з багатьма службами та центрами передового досвіду країн-членів ЄС, досліджувати майбутні стратегічних та оперативних зв'язків з ними на користь інтенсифікації та координації європейських зусиль у протидії російській загрозі. Нещодавно підписана в Брюсселі угода між ЄС та Україною про обмін інформацією з обмеженим доступом, безсумнівно, матиме великий вплив, усуваючи проблеми, які виникали раніше.

З початком Росією нового військового вторгнення на територію України, способи діяльності та потреби українських спецслужб зазнали надзвичайних змін перед очима викликів фізичному існуванню української держави та нації. Наразі спецслужби виконують бойові завдання в координації з іншими воєнізованими підрозділами безпосередньо у зонах бойових дій. СБУ виявляє та притягує до відповідальності агентів ворожих спецслужб, котрих загарбники намагаються залучити як до відкритої, так і до підпільної війни проти України. Наразі українські спецслужби відіграють значну роль у протидії російській агресії – як на полі бою (спеціальний підрозділ "Альфа" СБУ), у зоні бойових дій (зовнішня розвідка та військова контррозвідка), у протидії розвідувально-диверсійній, та підривній діяльності (підрозділи контррозвідки та боротьби з тероризмом, Антитерористичний центр при СБУ). Також СБУ тримає кібероборону – запобігає загрозам у національному інформаційному та кіберпросторі. Власне, за інформацією ЗМІ, вторгненню РФ передували дві масштабні кібератаки на вебресурси державної влади України (у січні та лютому) [3].

Багатовекторна протидія ворогу необхідна для забезпечення стабільної роботи інформаційних систем органів державної влади, об'єктів критичної інфраструктури та життєзабезпечення. Тож за нинішніх обставин найнагальнішими потребами спецслужб України є матеріальна підтримка, розвідка, включаючи супутникову, та міжнародні відносини. Задоволення саме цих потреб є терміновим і закладає основу для майбутньої співпраці з міжнародними партнерами у післявоєнній ситуації. Керівництво держави, ймовірно, буде зацікавлене у загальній розбудові спроможностей, викориненні корупції та російського впливу в секторі безпеки. Стратегічна підтримка, спеціальне навчання та технічні можливості потребують надійних національних та міжнародних партнерів, адже самотужки забезпечити повноцінний конкурентний розвиток спецслужб внутрішніми потребами неможливо.

У пошуку найперспективніших партнерів на міжнародній арені варто відштовхуватись від того, що наразі держави Європи розділилися на ті, які підпадають під безпосередню загрозу з боку Росії та ті, які захищені від неї в силу відстані та географії (більшою мірою) і в силу історичних факторів (меншою мірою). Так, у більшій небезпеці перебувають держави-безпосередні сусіди Російської Федерації, а також ті, території яких свого часу входили до Російської Імперії, щодо яких Росією

© Перепелиця Г., Дрозд А., 2022

робилися спроби включення в зону свого культурного та інформаційного впливу.

Тому варто приділяти увагу інтенсифікації безпекового співробітництва та співробітництва на рівні спецслужб з більшістю держав, що входять до давно створених ініціатив на кшталт наступних:

- Вишеградська група (Польща, Словаччина, Угорщина та Чеська Республіка – V4). У політичному плані V4 одноставно підтримує надання європейської перспективи для країн-кандидатів, вбачаючи в подальшому розвитку процесів євроінтеграції запоруку стабільності і безпеки всього регіону ЦСЄ.

- "Бухарестська дев'ятка" (Болгарія, Естонія, Латвія, Литва, Польща, Румунія, Словаччина, Угорщина, Чехія), що оформилася у 2014 році з метою консолідації східного флангу НАТО та просування позицій країн в його межах.

- "Тримор'я", що об'єднує 12 країн Центральної та Східної Європи. У разі надання в перспективі цьому діалогу безпекового виміру, за потенційної участі в ньому України, країн Балтії, Польщі, Румунії, Молдови та Грузії, контури Балто-Чорноморського союзу будуть ставати дедалі чіткішими.

Водночас, необхідно пам'ятати про хиткість вищеперелічених утворень, зумовлену несприятливою для України зовнішньою політикою Угорщини, лідери якої сповідують "невтручання в питання чужої війни на шкоду національним інтересам Угорщини". У цьому зв'язку однозначно перспективним видається співробітництво та створення мережі довіри на рівні спецслужб у вужчих форматах: "Люблінський трикутник" (Польща, Латвія, Україна), Альянс України, Великої Британії і Польщі, а також у форматі взаємодії з країнами Скандинавії. Останній формат ще не оформився, однак, зважаючи на консолідацію цими країнами зусиль з подолання російської загрози й ініціативу вступу до НАТО Фінляндії та Швеції, варто розраховувати на його формальне чи неформальне оформлення. У досягненні стратегічної цілі євроінтеграції може допомогти взаємодія зі спецслужбами країн, які скептично ставляться до перспективи українського членства в ЄС.

Окрему увагу хотілося б приділити взаємній вигоді і перспективам взаємодії українських спецслужб з європейськими безпековими інституціями та центрами передових практик. Інтеграція до європейської системи безпеки можлива і має відбуватися перш за все шляхом об'єднання зусиль, налагодженню оперативної взаємодії, обміну інформацією та досвідом з такими центрами. Найперспективнішими партнерами у цьому ключі вважаються наведені нижче.

Розвідувально-ситуаційний центр ЄС (EU INTSEN) [4] – це орган Служби зовнішніх зв'язків Європейського Союзу під керівництвом Верховного представника ЄС. Він відіграє важливу роль у практичній реалізації Спільної зовнішньої і безпекової політики та Спільної політики безпеки і оборони. Центр взаємодіє з різними органами ЄС, які ухвалюють рішення, проводить спеціальні брифінги, наприклад, для високого представника/віцепрезидента, спеціальних представників ЄС, різних органів Ради та Європейського парламенту. Місія EU INTSEN полягає в тому, щоб надавати високому представнику аналіз розвідувальних даних, забезпечувати інформування на випередження та ситуаційну обізнаність. Центр робить це шляхом моніторингу та оцінки міжнародних подій, зосереджуючись, зокрема, на чутливих географічних зонах, питаннях тероризму та розповсюдження зброї масового знищення та інших глобальних загроз. EU INTSEN не є оперативним ві-

домством і не має жодних можливостей для збору інформації. Оперативний рівень розвідки є відповідальністю служб держав-членів. EU INTSEN займається лише стратегічним аналізом, оцінкою загроз і прогнозуванням – як коротко- так і довгостроковим – на основі відкритих джерел і розвідданих. INTSEN управляє аналітичним центром при Раді Європейського Союзу в Брюсселі та Військовим штабом Європейського Союзу. Він складається з понад 110 співробітників. Близько 70% співробітників є представниками спецслужб. INTSEN також отримує інформацію від Frontex та Європолу.

Окрім доступу до інформаційних потоків, тісніша взаємодія СБУ та СЗР з INTSEN водночас сприятиме посиленню співпраці зі службами країн-членів ЄС, зокрема Франції, Німеччини, Італії, Нідерландів, Іспанії, Швеції, Фінляндії, які беруть активну участь у роботі INTSEN.

Агентство Європейського Союзу з кібербезпеки (ENISA) [5] сприяє досягненню високозагального рівня кібербезпеки в Європі. Агентство Європейського Союзу з кібербезпеки, засноване у 2004 році та посилене Законом ЄС про кібербезпеку, сприяє кіберполітиці ЄС, забезпечує підвищену надійність продуктів, послуг і процесів у сфері інформаційно-комунікаційних технологій, співпрацює з державами-членами та органами ЄС і допомагає Європі готуватися до кібервикликів завтрашнього дня. Шляхом обміну знаннями, розбудови потенціалу та підвищення обізнаності Агентство співпрацює зі своїми ключовими партнерами, щоб зміцнити довіру, підвищити стійкість інфраструктури Союзу та, зрештою, забезпечити безпеку європейського суспільства та громадян. ENISA акумулювала унікальний досвід багатьох країн-членів ЄС щодо підвищення кібербезпеки на всіх рівнях: від обміну інформацією про загрози до підвищення обізнаності, державно-приватного партнерства, правової бази та обміну даними.

Центр реагування на надзвичайні ситуації у сфері цифрових технологій (CERT-EU) [6] – це постійна команда реагування на надзвичайні ситуації у цифровій сфері на сторожі безпеки інституцій, агентств та органів ЄС. Команда складається з експертів у галузі IT-безпеки з головних інституцій ЄС (Європейська комісія, Генеральний секретаріат Ради, Європейський парламент, Комітет регіонів, Економічний та соціальний комітет). Центр тісно співпрацює з іншими CERT в країнах-членах ЄС і за їх межами, а також зі спеціалізованими компаніями з IT-безпеки.

Центр досконалості НАТО у сфері стратегічних комунікацій (StratCom COE) [7]. Окрім досліджень та тренінгів для урядів із питань стратегічної комунікації, Центр досконалості НАТО має значний досвід у протидії ворожій інформаційній діяльності державних та недержавних суб'єктів. Учасники з цивільного та військового, приватного та академічного секторів застосовують сучасні технології та віртуальні інструменти для аналізу, дослідження та прийняття рішень. Ядром StratCom COE є група міжнародних експертів. З моменту свого заснування в 2014 році StratCom COE в Ризі став центром знань з стратегічних комунікацій, об'єднуючи військові, академічні, бізнесові та державні знання.

Інститут Європейського Союзу з досліджень безпеки (EUISS) [8] – це агентство, яке займається аналізом питань зовнішньої політики, політики безпеки та оборони. Його основна місія полягає в тому, щоб допомогти ЄС та його державам-членам у здійсненні Спільної зовнішньої політики та політики безпеки, включаючи Спільну політику безпеки та оборони, а також інші зовнішні дії Союзу.

Центр досконалості у сфері протидії гібридним загрозам (Hybrid CoE) [9] у Хельсінкі – це міжнародна незалежна мережева організація, що працює над удосконаленням загальноурядового та загальносуспільного підходу до протидії гібридним загрозам. Хоча розуміння мінливості безпекового середовища має істотне значення, недостатньо лише аналізувати загрози, необхідно також мати конкретні інструменти протидії їм. Отже, ключове завдання Центру – розвиток можливостей країн-членів у сфері запобігання та протидії гібридним загрозам. Це досягається шляхом обміну кращими практиками, тестування нових ідей та підходів, а також проведення навчальних курсів та тренінгів.

Центр відіграє важливу роль як сполучна ланка між ЄС та НАТО, забезпечуючи платформу для стратегічних обговорень, спільних навчань і тренінгів. Досконалість досягається завдяки міжурядовим та міжгалузевим мережам Центру, до складу яких входять понад 1200 практиків та експертів, які працюють над завданнями, пов'язаними з гібридними загрозами у країнах-членах, ЄС, НАТО, приватному секторі та наукових установах. Як актор, що об'єднує інших акторів із різних секторів суспільства, Центр також відіграє ключову роль у багатосторонній дискусії про гібридні загрози, оприлюднюючи велику кількість різноманітних публікацій та взаємодіючи з різними партнерами у цій галузі.

Бернський клуб (фр. Club de Berne) [10] – організація для обміну розвідданими між спецслужбами 28 держав Європейського союзу, Норвегії та Швейцарії, названа на честь міста Берна (Швейцарія), де розташована її штаб-квартира. Бернський клуб існує з 1971 року і має характер неофіційного форуму співробітників спецслужб, де відбувається обмін даними, досвідом та думками, а також обговорення актуальних питань розвідувальної спільноти. Клуб не має секретаріату і не приймає жодних рішень, обов'язкових до виконання спецслужбами Євросоюзу. Бернський клуб та пов'язана з ним Група протидії тероризму (заснована після терактів у США 2001 року) також є інструментом неформального спілкування експертів з протидії тероризму та вироблення рекомендацій для політичних інститутів ЄС, контакти з якими підтримує через Розвідувально-ситуаційний центр ЄС (підрозділ Європейської служби зовнішньополітичної діяльності). Група протидії тероризму, яка формально не входить до ЄС, виступає як сполучна ланка між Бернським клубом та керівництвом ЄС, а ротація її керівництва відбувається за аналогією з головуванням країн ЄС.

Супутниковий центр ЄС (EU SATCEN) [11] підтримує прийняття рішень та дії Європейського Союзу у сфері спільної зовнішньої політики та політики безпеки, зокрема Спільної політики безпеки та оборони, надаючи продукти і послуги за рахунок експлуатації відповідних космічних технологій і супутніх даних, включаючи супутникові знімки та аерофотозйомки.

EU SATCEN працює під наглядом Комітету з політики та безпеки й оперативним керівництвом Верховного представника ЄС з питань закордонних справ і політики безпеки. Основними "клієнтами" є Європейська служба зовнішніх зв'язків, країни-члени ЄС, місії та операції ЄС, Європейська комісія, інші агенції ЄС, такі як Frontex, треті держави та міжнародні організації, такі як ООН та ОБСЄ. SatCen співпрацює з національними та міжнародними установами в галузі космосу. Він тісно взаємодіє з Європейським оборонним агентством, Європейською комісією та Європейським космічним агентством, а також іншими установами та міжнародними організаціями. Враховуючи обмежені можливості України у космічний

сфері, налагодження оперативного обміну даними з EU SATCEN буде винятково корисним для українських спецслужб як у воєнний, так і у повоєнний період.

Європейський центр протидії кіберзлочинності при Європолі (EC3) [12] пропонує оперативну, стратегічну, аналітичну та криміналістичну підтримку розслідуванням держав. EC3 служить центром криміналістичної інформації та розвідки; підтримує операції та розслідування, пропонує оперативний аналіз, координацію та експертизу; забезпечує високоспеціалізовану технічну та цифрову криміналістичну підтримку для розслідувань та операцій; сприяє оперативному, технічному та стратегічному співробітництву між правоохоронними органами та іншими відповідними кіберспільнотами й установами (наприклад, Євроюст, EEAS, ENISA, CERT-EU, Комісія, Рада тощо); забезпечує цілодобову оперативну та технічну підтримку правоохоронних органів для негайного реагування на невідкладні кіберінциденти; сприяє роботі Спільної робочої групи з боротьби з кіберзлочинністю (J-CAT) у боротьбі з кіберзлочинністю; підтримує навчання та розбудову потенціалу для відповідних органів держав-партнерів; надає різноманітні продукти стратегічного аналізу, які дозволяють приймати обґрунтовані рішення щодо боротьби з кіберзлочинністю; забезпечує встановлення зв'язків між правоохоронними органами, приватним сектором, науковими колами та іншими партнерами; сприяє підготовці та проведенню стандартизованих профілактичних та інформаційних кампаній і заходів.

Після досвіду повномасштабної війни Україна зіштовхнеться з необхідністю розробки нової моделі реформування і розбудови спеціальних служб, позаяк на даний час вже очевидно, що далеко не всі підходи, пропонувані раніше Міжнародною дорадчою групою у межах запланованої реформи сектору безпеки України відповідно до стандартів ЄС, є застосовними для України зважаючи на воєнні та повоєнні реалії. Глобальними та регіональними міжнародними організаціями, зокрема ООН (Резолюція Ради Безпеки ООН № 2553 [1]) та ЄС (Рамкове рішення ЄС щодо реформування сектору безпеки від 2016 року [2]), роками напрацьовувалися універсальні підходи до реформування сектору безпеки. Однак, проаналізувавши відповідні документи, доходимо висновку, що усіма ними визначаються лише цілі і ключові принципи реформи сектору безпеки: прозорість, ефективність, доступність та підзвітність, а головне – дотримання і захист прав і свобод людини. При цьому конкретні кроки і методи їх досягнення згідно з Лісабонською угодою 2009 року, що визначає окрім іншого підходи до безпекової політики ЄС, залишаються на розсуд держави.

Щодо реформування і розбудови українських спецслужб у повоєнний період можна передбачити, що СЗР стане орієнтованою більшою мірою на політичну та економічну розвідку, більш відкритою до міжнародного співробітництва. Вона буде готова налагодити та розвивати стійку співпрацю з центрами передового досвіду країн-членів ЄС, досліджувати майбутнє стратегічних та оперативних зв'язків з ними на користь активізації та координації загальноєвропейських зусиль у протидії російській загрозі. Можливими напрямками співпраці будуть навчання та безпекова перевірка персоналу, нарощування спроможностей і модернізація за рахунок конкретних проектів технічної допомоги.

Очікувано, що, з огляду на перманентну російську загрозу, СБУ залишиться переважно "військовою службою" з чисельністю близько 30 000 осіб, як це є на даний час. Злочини проти гуманітарного права, масово

скоєні російськими окупантами, вже розслідуються СБУ (під наглядом Генпрокуратури) і будуть розслідуватися в післявоєнний період.

СБУ зосередить свою діяльність на контррозвідувальній протидії загрозам національній безпеці України та міжнародній безпеці, що вимагатиме від неї відмовитися від діяльності в інших сферах, таких як боротьба з контрабандою, організованою злочинністю та корупцією тощо. Загальна тенденція післявоєнного періоду полягатиме в наданні СБУ більших можливостей, включаючи більш наступальний характер діяльності. Як підкреслив президент Зеленський у розмові з журналістами, безпека буде темою номер один в Україні протягом наступних десяти років (Україна стане свого роду "великим Ізраїлем"). Може виникнути тенденція підпорядковувати питання прав людини цьому пріоритету. Тому очікувано, що міжнародна спільнота має стати основним лобістом того, щоб гарантії прав людини та антикорупційні заходи залишалися невід'ємним фактором при утворенні будь-яких нових структур і режимів роботи. Тому питання нагляду, у тому числі парламентсько-го, стане ще важливішим.

Спецслужби Ізраїлю можуть стати прикладом за критеріями сфери компетенції, оперативності роботи, технічного оснащення, підготовки та підбору персоналу, а от підконтрольність спецслужб одній особі (Прем'єр-міністру Ізраїлю) не є прикладом для наслідування, оскільки в Україні (як втім і всюди) це може спричинити служіння спецслужб не інтересам народу, а інтересам політичної еліти, чого допустити не можна.

За критерієм управління та нагляду необхідно шукати інші моделі для наслідування, наприклад, на досвіді Фінляндії чи Нідерландів. Моделі Комітету із питань нагляду за розвіддіяльністю Фінляндії та Уповноваженого з питань нагляду за розвіддіяльністю можуть служити прикладом для наслідування при втіленні в життя ухваленого Закону України "Про розвідку", а саме положення про Комітет з питань національної безпеки, оборони та розвідки. Ознайомившись з регламентом роботи Комітету, методами діяльності, процедурою підбору кадрів та безпекової перевірки, а також обов'язковим характером його рішень, можна оцінити їх на предмет можливості подальшої адаптації до українських реалій.

З досвіду роботи спецслужб Нідерландів [13] уваги заслуговує підхід до перевірки компетентності та добросовістності особового складу. Метою оцінки професійної етики та добросовістності (далі – безпекова перевірка) є встановлення того, чи створюватиметься загроза національній безпеці, якщо особа перебуватиме на посаді, яка передбачає конфіденційність або ризик хабарництва, шахрайства чи шантажу. Під час скринінгу акцент робиться на дослідженні наступних аспектів: судимість, підризна та антидемократична діяльність, залежності, фінансова вразливість, небажаний вплив, оманлива поведінка, безвідповідальна та ризикована поведінка. Під час цього процесу досліджуються різні аспекти життя відповідної особи такими методами як індивідуальні бесіди, вивчення активів (у тому

числі закордонних), направлення інформаційних запитів для отримання необхідної інформації від органів поліції та місцевого самоврядування, бесіди з родичами та приближеними особами.

У повоєнний період співпраця з колегами з ЄС та НАТО у форматі навчальних обмінів сформує критичну масу високопрофесійних офіцерів, які прагнуть до західних стандартів і допоможе побудувати децентралізовані більш оперативні та повноважні спецслужби порівняно з російською моделлю, для якої характерні авторитаризм і централізована вертикаль командування в радянському стилі.

Висновок полягає в необхідності зосереджуватися не на формі, а на змісті, тобто на досягненні згаданих раніше принципів прозорості, підзвітності, ефективності та доступності сектору безпеки, у тому числі спеціальних служб, прийнятими для України методами, які можна як адаптувати на основі наявного іноземного досвіду, так і розробити самостійно. У воєнний та повоєнний періоди значення міжнародного співробітництва спецслужб України для забезпечення як державної, так і загальноєвропейської безпеки, неухильно зростатиме. На передній план вийде розвиток взаємодії з провідними безпеково-аналітичними центрами ЄС, спецслужбами країн Балтії, Скандинавії, а також Великої Британії.

Список використаних джерел

1. UN Resolution 2553 adopted by the Security Council on 3 December 2020. URL: Security Council – Resolution 2553 (2020) | United Nations Peacekeeping
2. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Elements for an EU-wide strategic framework to support security sector reform // EUROPEAN COMMISSION, Strasbourg, 5.7.2016. URL: EUR-Lex – 52016JC0031 – EN – EUR-Lex (europa.eu)
3. Звернення Голови СБУ І. Баканова з нагоди 30-річчя створення СБУ [Електронний ресурс]. – Режим доступу: Звернення Голови СБУ Івана Баканова з нагоди 30-річчя створення Служби безпеки України (ssu.gov.ua)
4. Розвідувально-ситуаційний центр ЄС [Електронний ресурс]. – Режим доступу: EU Intelligence and Situation Centre (EU INT-CEN) – Infogalactic: the planetary knowledge core
5. Сайт Агентства ЄС з кібербезпеки [Електронний ресурс]. – Режим доступу: ENISA (europa.eu)
6. Центр реагування на надзвичайні ситуації у сфері цифрових технологій [Електронний ресурс]. – Режим доступу: CERT-EU (europa.eu)
7. Центр досконалості НАТО у сфері стратегічних комунікацій [Електронний ресурс]. – Режим доступу: StratCom | NATO Strategic Communications Centre of Excellence Riga, Latvia (stratcomcoe.org)
8. Інститут Європейського Союзу з досліджень безпеки [Електронний ресурс]. – Режим доступу: EUISS Homepage | European Union Institute for Security Studies (europa.eu)
9. Центр досконалості у сфері протидії гібридним загрозам [Електронний ресурс]. – Режим доступу: Hybrid CoE – Hybrid CoE – The European Centre of Excellence for Countering Hybrid Threats
10. Бернський клуб [Електронний ресурс]. – Режим доступу: The Club de Berne: a black box of growing intelligence cooperation – about:intel (aboutintel.eu)
11. Супутниковий центр ЄС [Електронний ресурс]. – Режим доступу: SatCen – European Union Satellite Centre (europa.eu)
12. Європейський центр протидії кіберзлочинності при Європолі [Електронний ресурс]. – Режим доступу: European Cybercrime Centre – EC3 | Europol (europa.eu)
13. Government competency guide // Ministry of Internal Affairs of the Netherlands. [Електронний ресурс]. – Режим доступу: competentiegids_rijk_01112018.pdf (functiegebouwrijksverheid.nl)

Надійшла до редколегії 12.12.22

H. Perepelytsia, Dr Hab. (Political), Prof.,
A. Drozd, Master Student
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

SPECIAL SERVICES OF UKRAINE IN CONDITIONS OF CURRENT AND FUTURE CHALLENGES

The article analyzes the optimal directions and ways of development of international cooperation, capacity building and reform of Ukrainian special services in the view of the current geopolitical situation, as well as current and future challenges to Ukrainian and European security.

Keywords: special services of Ukraine, Security Service, Foreign Intelligence Service, EU, international cooperation, reform, capacity building, full-scale military invasion of the Russian Federation.