УДК 342.951(477) DOI: https://doi.org/10.32631/pb.2025.1.06

ВАДИМ ВОЛОДИМИРОВИЧ ПОЛОВНІКОВ,
доктор юридичних наук, доцент,
Національна академія Державної прикордонної служби України імені Богдана Хмельницького,
кафедра управління;
https://orcid.org/0000-0002-8054-909X,
e-mail: vpolovnikov@ukr.net

ІНФОРМАЦІЙНА БЕЗПЕКА ОСОБОВОГО СКЛАДУ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ: ПРОБЛЕМНІ ПИТАННЯ НОРМАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ

Проаналізовано чинне законодавство України, яке регулює суспільні відносин в інформаційній сфері діяльності сил безпеки і оборони, зокрема Державної прикордонної служби України, наукові погляди вчених щодо змісту понять інформаційної безпеки особи, суспільства і держави. За результатами аналізу визначено поняття «інформаційна безпека особового складу (службових і посадових осіб) Державної прикордонної служби України» з урахуванням необхідності забезпечення громадянських прав і обов'язків в інформаційній сфері та виконання вимог, що визначаються специфікою службової діяльності й правовим статусом особового складу щодо збирання, зберігання, використання та поширення інформації.

Запропоновано інформаційну безпеку особового складу Державної прикордонної служби України розглядати у структурному аспекті і як певний стан. У структурному аспекті поняття «інформаційна безпека особового складу Державної прикордонної служби України» має такі складові: захищеність конституційних прав і свобод людини щодо інформації; захищеність інформаційних мереж і послуг, персональних даних, інформації з обмеженим доступом; захищеність від ворожої пропаганди, викривлення інформації, дезінформації, фейків тощо; захищеність від негативного впливу інформації, завдання шкоди фізичному і психічному здоров'ю, етичним, духовним, психологічним, фізичним, соціальним та іншим засадам побудови суспільних (інформаційних) відносин. Як стан інформаційна безпека визначається ступенем досягнення найбільшої відповідності (збалансованості) між життєво важливими особистими і службовими (державними) інтересами особового складу Державної прикордонної служби України та їх захищеності у сфері збирання, зберігання, обробки, аналізу й обміну інформацією.

Наголошено на необхідності вдосконалення нормативно-правового регулювання суспільних відносин в інформаційній сфері діяльності особового складу Державної прикордонної служби України, а також надано пропозиції щодо внесення змін і доповнень до чинного законодавства України, зокрема Закону України «Про Державну прикордонну службу України» та інших підзаконних нормативно-правових актів.

Ключові слова: *безпека, інформаційна безпека особи, суспільства і держави, особовий склад, Державна прикордонна служба України, інформація, інформаційно-психологічний вплив.*

Оригінальна стаття

ВСТУП. У статті 17 Конституції України зазначено, що забезпечення інформаційної безпеки України є однією з найважливіших функцій держави, справою всього Українського народу[1]. Забезпечення інформаційної безпеки України є також одним з основних напрямів державної інформаційної політики (ст. 3 Закону України «Про інформацію»), а до суб'єктів інформаційних відносин ст. 4 цього Закону віднесено фізичних осіб, юридичних осіб, об'єднання громадян, суб'єктів владних повноважень[2].

[1] Конституція України : Закон України від 28.06.1996 № 254к/96-ВР // База даних (БД) «Законодавство України» / Верховна Рада (ВР) України. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр (дата звернення: 26.12.2024).

[2] Про інформацію : Закон України від 02.10.1992 № 2657-XII // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: 26.12.2024).

Державна прикордонна служба України (далі – ДПСУ) є правоохоронним органом спеціального призначення, тобто державною інституцією, яка, окрім виконання основних завдань, також відповідає за дотримання інших норм законодавства, зокрема щодо забезпечення інформаційної безпеки України. Це охоплює як інформаційну безпеку особи, суспільства й держави загалом, так і безпеку ДПСУ, її особового складу та службової діяльності.

До особового складу ДПСУ належать військовослужбовці, державні службовці та працівники, які за своїм правовим статусом є службовими і посадовими особами ДПСУ і які залежно від посад, котрі вони обіймають, виконують різноманітні внутрішні та зовнішні функції, зокрема в інформаційній сфері, та є суб'єктами інформаційних відносин. Всі вони користуються загальними правами й обов'язками людини та громадянина України щодо доступу до інформації та користування нею, належать до певних верств населення й суспільства і здійснюють службову діяльність, перебуваючи у складі державного органу, наділеного владними повноваженнями, що покладає на них певні обов'язки та права, визначені нормативно-правовими актами та посадовими інструкціями.

За порушення вимог чинного законодавства України до службової діяльності, реалізації професійних та особистих інтересів, зокрема в інформаційній сфері, службова (посадова) особа ДПСУ може бути притягнута до різних видів відповідальності. За порушення законодавства України про інформацію передбачена дисциплінарна, цивільно-правова, адміністративна або кримінальна відповідальність.

Водночас порушення законодавства України про інформацію службовою (посадовою) особою ДПСУ, коли вона є суб'єктом правопорушення, – це один бік питання. Інформаційна безпека особового складу, коли службові (посадові) особи стають об'єктом посягання, а особовий склад загалом – об'єктом інформаційно-психологічного впливу, тиску чи маніпуляцій, – інший.

Важливу роль у цьому відіграє чітка правова визначеність цих питань, яка має ґрунтуватися на якісному нормативно-правовому регулюванні та єдиному розумінні сутності поняття інформаційної безпеки особового складу правоохоронного органу на прикладі ДПСУ. Це враховує необхідність дотримання громадянських прав і обов'язків осіб в інформаційній сфері, а також виконання вимог, що висуваються до них у зв'язку з належністю до ДПСУ. Вимоги стосуються як службової діяльності, так і приватного життя, зважаючи на специфіку їхнього правового статусу як під час служби (праці) у відповідному органі (підрозділі) ДПСУ, так і в позаслужбовий час.

МЕТА І ЗАВДАННЯ ДОСЛІДЖЕННЯ. *Метою* статті є з'ясування сутності та змісту поняття «інформаційна безпека особового складу ДПСУ», нормативно-правового регулювання питань забезпечення інформаційної безпеки особового складу ДПСУ в чинному законодавстві України. Для досягнення мети дослідження необхідно вирішити такі *завдання*: 1) проаналізувати чинне законодавство України, яке регулює суспільні відносини в інформаційній сфері, та визначені законодавцем поняття інформаційної безпеки; 2) дослідити теоретичні напрацювання щодо розуміння поняття «інформаційна безпека» через з'ясування його сутності як складової інших видів безпеки, зокрема національної; 3) з'ясувати сутність інформаційної безпеки особового складу ДПСУ в сучасних умовах.

ОГЛЯД ЛІТЕРАТУРИ. Значний внесок у дослідження різних аспектів інформаційної безпеки як складової національної безпеки, державної інформаційної політики зробили такі вітчизняні науковці, як-от: О. Баранов, І. Бондар, В. Гурковський, О. Данильян, О. Дзьобань, О. Довгань, І. Дятлова, П. Квіткін, В. Кононович, В. Курганевич, І. Кушнір, В. Ліпкан, О. Логінов, М. Панов, В. Петрик, Л. Петрова, Г. Почепцов, М. Присяжнюк, Т. Ткачук, Л. Харченко, В. Шатун та ін.

Зокрема, П. Квіткін, І. Дятлова та Л. Петрова (2021) провели теоретико-методологічний аналіз інформаційної безпеки особистості, М. Шевчук (2023) досліджував генезу поняття інформаційної безпеки як складової національної безпеки, О. Олійник (2011) – позитивні та негативні впливи інформаційної революції на забезпечення інформаційної безпеки особи, суспільства, держави, О. Заєць (2010) – захищеність особи від негативного інформаційно-психологічного впливу як напрямок інформаційної безпеки України, В. Богуславський (2016) – завдання та принципи державної інформаційної політики у сфері забезпечення особистої безпеки працівників сил охорони правопорядку, М. Закіров і С. Закірова (2022) – дилему інформаційної безпеки особистості в інформаційному суспільстві, К. Іванчук (2021) – комунікативну особистість мережі Інтернет у контексті забезпечення інформаційної безпеки держави, І. Кушнір (2018) – співвідношення понять «інформаційна безпека» та «захист інформації» в діяльності ДПСУ.

Однак, попри значний рівень наукового осмислення проблем інформаційної безпеки, в

умовах стрімкого розвитку інформаційних технологій, засобів та способів поширення інформації, особливо в умовах ведення інформаційної війни рф проти України, яка є основою гібридної російсько-української війни, нагальними є питання вдосконалення забезпечення інформаційної безпеки не лише особового складу ДПСУ, а й інших складових сил безпеки і оборони України, що й зумовлює актуальність наукової статті.

МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ. Під час проведення дослідження було використано комплекс методів наукового пізнання, що дозволило вибудувати структуру та логічну послідовність викладення його результатів. Зокрема, аксіологічний метод сприяв осмисленню сутності поняття «безпека» та його інтерпретації в інформаційній сфері. Метод контент-аналізу дозволив проаналізувати масив чинного законодавства України і виокремити ті нормативно-правові акти, у яких йдеться про безпеку та інформаційну безпеку. Діалектичний підхід допоміг розглянути розвиток теорії безпеки та її взаємозв'язок з іншими процесами. Порівняльно-правовий метод став у пригоді при порівнянні подібних та відмінних ознак у визначеннях понять «безпека» та «інформаційна безпека». Логічний підхід дозволив урахувати різні погляди науковців на розуміння явища інформаційної безпеки та його уніфікацію. Системний підхід допоміг розглянути взаємозв'язки між різними складовими елементами безпеки в інформаційній сфері. Функціональний підхід було застосовано для висвітлення особливостей забезпечення безпеки залежно від суб'єкта її забезпечення, а також суб'єкта й об'єкта посягань. Антропологічний підхід було використано при дослідженні категорії «інформаційна безпека» у контексті особистої поведінки людини як громадянина у приватному і сімейному житті, під час служби (роботи) і виконання службових обов'язків для формування чіткого уявлення про сутність інформаційної безпеки та її нормативно-правового регулювання.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ ТА ДИСКУСІЯ. Питання інформаційної безпеки стали особливо актуальними у зв'язку з агресією рф, однією з основних складових якої, крім воєнних дій, є активне використання агресором пропаганди, застосування різноманітних інформаційних технологій впливу, інформаційно-психологічних операцій щодо населення рф, України та інших країн світової спільноти тощо. Інформація стала одним із тих видів зброї, що надала російсько-українській війні характер гібридної. Підміна понять, уведення в оману, викривлення історії, навішування ярликів, дискредитація, перекручування фактів, заплутування, залякування, виправдовування злочинів тощо є звичною й поширеною практикою в реалізації завдань інформаційної політики рф щодо супроводу загарбницьких намірів і дій на території України. Ідеологічні та інші наративи, дезінформація, фейки наповнюють сучасний інформаційний простір не лише України, а й інших держав і потребують вироблення у населення стійкого інформаційного імунітету, забезпечення його інформаційної безпеки. Особливо це стосується України та країн, населення яких звикло до подання в медіа правдивої інформації.

Одним з об'єктів інформаційного та психологічного впливу є особовий склад сил безпеки і оборони України, зокрема й ДПСУ, а одним з об'єктів посягань – його інформаційна безпека. Від правильного розуміння організаційних, теоретико-правових та інших особливостей використання інформації з різною метою в сучасних умовах залежить рівень обізнаності особового складу в цій сфері, успішність дій із запобігання загрозам та ризикам, їх виявлення, уникнення або усунення, створення необхідних умов для ефективної протидії негативному впливу інформації тощо.

Слід зазначити, що в чинному законодавстві України й науковій літературі поки немає єдиного погляду на зміст поняття «інформаційна безпека», а також інших пов'язаним із ним понять, зокрема «безпека особи», «особиста безпека», «власна безпека», «безпека життєдіяльності особового складу (персоналу)», «внутрішня безпека» тощо. Це стосується й діяльності особового складу ДПСУ.

Загальний для багатьох сфер життєдіяльності термін «безпека» у чинному законодавстві України розглядається по-різному: як відсутність неприпустимого ризику, пов'язаного з можливістю завдання будь-якої шкоди; як комплекс заходів, а також людські і матеріальні ресурси, призначені для захисту від актів незаконного втручання та інших протиправних посягань; як властивість об'єкта забезпечувати відсутність ризику; як стан, за якого ризик шкоди чи ушкодження обмежений до прийнятного рівня; як відсутність загрози життю і здоров'ю людей, що перевищує граничний ризик; як відсутність ризику (або недопустимого ризику), пов'язаного з можливістю завдання шкоди та/або збитків; як запобігання тому, що суперечить закону та загрожує порядку, тощо[1].

[1] Термін «Безпека» // БД «Законодавство України» / ВР України. URL: https://zakon.rada.

Так, наприклад, у банківській сфері інформаційна безпека також розглядається порізному: як бажаний результат, що забезпечує збереження конфіденційності, цілісності та доступності інформації[1]; як стан захищеності, за якого гарантується функціональність, безперервність роботи, відновлюваність, цілісність і стійкість інформаційних, електронних комунікаційних, інформаційно-комунікаційних та/або технологічних систем, конфіденційність, цілісність і доступність електронних інформаційних ресурсів, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних загроз штатному режиму їхнього функціонування та несанкціонованого втручання в їхню роботу[2]; як комплекс організаційних заходів банку, програмних і технікo-технологічних засобів, що діють на всіх організаційних рівнях і захищають інформацію від випадкових та/або навмисних загроз, наслідком яких може стати порушення доступності, цілісності чи конфіденційності інформації про діяльність банку або його клієнтів[3].

У першому випадку йдеться про безпеку інформації, у другому – про безпеку систем та ресурсів, у третьому – про комплекс організаційних заходів, що забезпечують захист інформації. Усе це тією чи іншою мірою стосується інформаційної безпеки, проте охоплює різні її аспекти та об'єкти посягань.

У Законі України «Про телекомунікації», який втратив чинність, інформаційна безпека телекомунікаційних мереж розглядалась як здатність телекомунікаційних мереж забезпечувати захист інформації[4]. У цьому визначенні телекомунікаційні мережі розглядались як суб'єкт забезпечення захисту, а інформація – як об'єкт захисту. У новому Законі України «Про електронні комунікації» дається визначення поняття «безпека мереж і послуг» як здатність електронних комунікаційних мереж і послуг протистояти діям, що становлять загрозу доступності, цілісності чи конфіденційності таких мереж і послуг, а також даних, що зберігаються, передаються чи обробляються, та пов'язаних із ними послуг, які надаються або доступ до яких здійснюється через електронні комунікаційні мережі чи послуги[5].

Законодавець відмовився від поняття «інформаційна безпека телекомунікаційних мереж» і запровадив поняття «безпека мереж і послуг», чим, на нашу думку, розширив зміст поняття «безпека», не обмежуючи його лише захистом інформації. Замість поняття «здатність забезпечувати захист від різних загроз» використано поняття «здатність протистояти діям, що становлять загрозу». У цьому визначенні суб'єктом протистояння діям, що становлять загрозу, є електронні комунікаційні мережі та послуги, а об'єктом захисту від таких дій є самі мережі та послуги, а також дані, що перебувають в обігу, та пов'язані з ними послуги[6]. В обох зазначених вище законах така здатність може розглядатись як одна з функцій систем мереж і послуг, їхня властивість.

Усе зазначене складно співвіднести з можливим розумінням поняття «інформаційна безпека людини», адже людина є одним з основних суб'єктів її забезпечення. Це проявляється у здатності людини протистояти завданню їй шкоди та діям, що становлять загрозу її поглядам, переконанням, фізичному й психічному здоров'ю тощо. Негативними наслідками цього можуть бути руйнування цілісності особистості, системи її відносин з іншими людьми та державою (Петрик та ін., 2019).

У науковій літературі більше уваги приділяється інформаційній безпеці окремої людини, особи, особистості, тобто пересічному

gov.ua/laws/term/1742 (дата звернення: 26.12.2024).

[1] Про затвердження Положення про захист інформації та кіберзахист учасниками платіжного ринку : постанова Правління Нац. банку України від 19.05.2021 № 43 // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/v0043500-21 (дата звернення: 26.12.2024).

[2] Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури : постанова Кабінету Міністрів України від 24.03.2023 № 257 // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/257-2023-п (дата звернення: 26.12.2024).

[3] Про затвердження Положення про організацію системи внутрішнього контролю в банках України та банківських групах : постанова Правління Нац. банку України від 02.07.2019 № 88 // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/v0088500-19 (дата звернення: 26.12.2024).

[4] Про телекомунікації : Закон України від 18.11.2003 № 1280-IV // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/1280-15 (дата звернення: 12.26.2024). Втратив чинність.

[5] Про електронні комунікації : Закон України від 16.12.2020 № 1089-IX // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/1089-20 (дата звернення: 26.12.2024).

[6] Там само.

громадянину України без урахування його посади, місця роботи та набутого у зв'язку із цим правового статусу службової (посадової) особи, суб'єкта владних повноважень тощо. Також існує багато різних визначень поняття «інформаційна безпека», які ґрунтуються на таких підходах, як наявність певних мінімально необхідних умов існування її суб'єктів, встановлених міжнародним та національним законодавством; як ступінь або стан захищеності; як надійність створення, зберігання та споживання інформації; як комплекс заходів; як процес; як органічна єдність ознак, таких як стан, властивість, а також управління загрозами й небезпеками, що забезпечує вибір оптимального шляху їх усунення та мінімізації негативних наслідків.

Нормативне визначення поняття «інформаційна безпека України» міститься у Стратегії інформаційної безпеки[1]. Воно охоплює інформаційну безпеку людини, суспільства й держави, які, попри певні особливості, тісно взаємопов'язані.

Якщо взяти за основу це визначення, то інформаційна безпека людини – це стан захищеності життєво важливих інтересів, за якого належним чином забезпечуються її конституційні права і свободи на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, а також ефективна система захисту і протидії завданню шкоди через поширення негативних інформаційних впливів, зокрема скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване поширення, використання й порушення цілісності інформації з обмеженим доступом[2]. Тобто людина не залишається на самоті, існує ефективна система захисту і протидії.

Інформаційна безпека науковцями зазвичай розглядається як стан захищеності особи, суспільства і держави, за якого досягається інформаційний розвиток (технічний, інтелектуальний, соціально-політичний, морально-етичний), а сторонні інформаційні впливи не завдають йому суттєвої шкоди. При цьому, на думку вчених, інформаційна безпека особи – це стан захищеності психіки та здоров'я людини від деструктивного інформаційного впливу, який призводить до неадекватного сприйняття нею дійсності та (або) погіршення її фізичного стану (Петрик та ін., 2019).

О. Заєць (2010) вважає, що головною проблемою інформаційної безпеки є балансування між свободою доступу до інформації та необхідністю її обмеження в інтересах безпеки життєдіяльності. Для вирішення цієї проблеми, на його думку, потрібен системний нормативно-правовий механізм, який, з одного боку, забезпечуватиме захист інформаційних прав і свобод, а з другого – громадський і державний контроль та регулювання рівня інформаційної безпеки. Але в цьому разі йдеться лише про правові аспекти проблеми, які стосуються захисту та контролю і не торкаються правосвідомості особи, її фізичного і психологічного здоров'я, політичної зрілості, патріотичних переконань тощо.

Погоджуємося з думкою П. Квіткіна, І. Дятлової та Л. Петрової (2022), що в дослідженнях, присвячених проблемам інформаційної війни, загрозам інформаційній безпеці суспільства та особистості, не приділяється достатньої уваги особистісному фактору. Поза аналізом залишається важливий аспект: особистість, свідомість і психіка якої зазнали деструктивних впливів або яка неадекватно сприймає процеси суспільної життєдіяльності, стає ретранслятором інформаційних матеріалів медіа або джерелом поширення власного сприйняття й оцінки дійсності.

Вчені вважають, що до чинників, які впливають на інформаційну безпеку особистості, належать: рівень сформованості світоглядно-ментальної складової інформаційної безпеки особистості, що ґрунтується на її світогляді, системі гуманітарних і соціально-економічних знань, переконаннях, системі цінностей і ціннісних орієнтацій, життєвих позиціях та ідеалах; рівень сформованості когнітивної складової інформаційної безпеки особистості, що проявляється в її вміннях аналізувати й оцінювати інформацію, процеси суспільної життєдіяльності; рівень сформованості інформаційної культури особистості, що проявляється в опануванні нею знань щодо технологій інформаційних та інформаційно-психологічних впливів, формуванні культури користування

[1] Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28.12.2021 № 685/2021 // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/685/2021 (дата звернення: 26.12.2024).

[2] Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28.12.2021 № 685/2021 // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/685/2021 (дата звернення: 26.12.2024).

сучасними технічними засобами інформації та комунікації (Квіткін, Дятлова, Петрова, 2022).

Тобто йдеться, зокрема, про рівень готовності особи протистояти ідеологічному впливу (тиску) ворожої пропаганди, вміння розрізняти правду і неправду, розуміння наслідків впливу на свідомість, психіку, погляди, цінності та поведінку осіб, наявність в особи необхідних знань, навичок і умінь безпечного користування інформаційними ресурсами в усіх сферах життєдіяльності в сучасних умовах. Це стосується як приватного життя, так і служби (роботи) у державних органах, зокрема в ДПСУ, що передбачає не лише можливість здійснення загальних прав і виконання обов'язків людини та громадянина в повсякденному житті, а й необхідність дотримання службових прав та обов'язків. Це охоплює певні обмеження щодо збору, зберігання, оприлюднення та поширення інформації, а також суворе дотримання правил і вимог роботи з відкритою інформацією та інформацією з обмеженим доступом тощо

І. Кушнір (2018) розглядає інформаційну безпеку в діяльності ДПСУ як функціонування системи своєчасного реагування на випередження, недопущення й усунення інформаційних загроз, що можуть завдати шкоди суб'єктам у прикордонній сфері, об'єктам інформаційно-правового захисту, прикордонній безпеці, а також забезпеченню збереження, цілісності інформації та встановленого порядку доступу до неї. Водночас такий підхід до визначення не конкретизує сутність інформаційної безпеки особового складу ДПСУ.

Обсяг інформації, що постійно надходить із різних джерел і використовується особовим складом ДПСУ в службовій діяльності та приватному житті, потребує чіткого усвідомлення її впливу та сприйняття посадовими й службовими особами, а також різними верствами населення тієї чи іншої країни. Важливо розуміти, до яких наслідків це може призвести або вже призводить в умовах інформаційного протиборства з рф (Половніков, Шеремет, 2023).

Ми погоджуємося з думкою О. Зайця (2010), що нинішній етап розвитку інформаційних технологій характеризується можливістю інформаційної дії на індивідуальну й суспільну свідомість, унаслідок чого неминучою противагою свободи інформації стає проблема інформаційної безпеки, що зайвий раз підтверджує необхідність належного захисту прав і законних інтересів людини, суспільства і держави в цій сфері. Причини цього криються як у зростаючій залежності людини і суспільства від інформації, так і в реалізації економічних і політичних інтересів з використанням інформаційних технологій. У зв'язку із цим актуалізується проблема захищеності особи від негативного інформаційно-психологічного впливу як одного з напрямів інформаційної безпеки України.

Отже, кожного разу під час розгляду поняття «безпека» постають логічні питання: про безпеку кого (чого) йдеться; захист кого (чого) і від кого (чого) здійснюється; хто (що) забезпечує захист; йдеться про бажаний результат, процес дій (зусиль), оперативний стан чи порядок (організацію) здійснення заходів із забезпечення безпеки та/або протидії загрозам та їхню мету тощо.

На нашу думку, інформаційна безпека особового складу ДПСУ як правоохоронного органу спеціального призначення повинна охоплювати такі складові: безпеку реалізації конституційних прав і свобод людини щодо інформації; безпеку інформаційних мереж і послуг; захист персональних даних; охорону та захист інформації з обмеженим доступом (конфіденційної, таємної та службової інформації); захист від ворожої пропаганди, викривлення інформації, дезінформації, фейків тощо; захист від негативного впливу інформації, завдання шкоди фізичному і психічному здоров'ю, етичним, духовним, психологічним, фізичним, соціальним та іншим засадам побудови суспільних (інформаційних) відносин.

Забезпечення інформаційної безпеки передбачає забезпечення реалізації всіх цих елементів у комплексі. Рівень забезпечення інформаційної безпеки (захищеності) визначається (оцінюється) станом надійності (ефективності) системи забезпечення інформаційної безпеки.

Зокрема, про захист персональних даних має дбати як сама особа, так і контролюючі та правоохоронні органи з метою недопущення протиправного отримання та обробки й, відповідно, подальшого використання інформації (відомостей чи сукупності відомостей) про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована (Головенко та ін., 2012).

Все це здійснюється за рахунок збереження конфіденційності, цілісності та доступності інформації, захисту інформації про приватне і сімейне життя, службову діяльність посадової (службової) особи, суб'єкта владних повноважень відповідно до службових обов'язків за посадою.

Сьогодні в чинному законодавстві України, яке регулює діяльність особового складу ДПСУ, немає чітко визначених положень щодо інформаційної безпеки.

Закон України «Про державний кордон України» визначає, що держава гарантує громадянам України, які беруть участь в охороні державного кордону України, захист життя і здоров'я від кримінально протиправних посягань[1]. У Законі України «Про Державну прикордонну службу України» йдеться лише про наявність у складі органів ДПСУ підрозділів забезпечення внутрішньої безпеки та власної безпеки. Статтею 19 цього Закону передбачено обов'язки ДПСУ, серед яких зазначено виконання відповідно до законодавства системи особливих заходів щодо захисту військовослужбовців та працівників ДПСУ від зазіхань на життя, здоров'я, честь, майно у зв'язку з їхньою службовою діяльністю, а також їхніх близьких родичів[2].

Немає жодної згадки про інформаційну безпеку особового складу, власну (особисту) або внутрішню безпеку і в Положенні про Адміністрацію Державної прикордонної служби України. Йдеться лише про те, що Адміністрація ДПСУ відповідно до покладених на неї завдань вживає особливих заходів для захисту військовослужбовців і працівників ДПСУ від зазіхань на їхнє життя, здоров'я, честь і майно у зв'язку зі службовою діяльністю, а також для захисту членів їхніх сімей. Голова ДПСУ забезпечує в межах повноважень, передбачених законом, реалізацію державної політики щодо державної таємниці, захисту інформації з обмеженим доступом, контроль за їх збереженням в Адміністрації ДПСУ[3]. Так само відсутні відповідні норми і у Положення про регіональне управління Державної прикордонної служби України[4].

Тобто передусім йдеться про захист від перешкоджання виконанню службовими (посадовими) особами ДПСУ покладених на них законом обов'язків і здійсненню наданих їм прав, а також від посягань на життя, здоров'я, житло й майно цих осіб та їхніх близьких родичів у зв'язку зі службовою діяльністю, спрямованою на протидію протиправній діяльності. Такий захист передбачений законами України «Про державний захист працівників суду і правоохоронних органів»[5] та «Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві»[6].

Положенням про орган охорони державного кордону Державної прикордонної служби України до основних завдань та повноважень таких органів віднесено лише участь у заходах із захисту військовослужбовців та працівників ДПСУ від зазіхань на життя, здоров'я, честь, майно у зв'язку з їхньою службовою діяльністю, а також їхніх близьких родичів. Водночас орган охорони державного кордону відповідно до покладених на нього завдань: здійснює управління телекомунікаційними та інформаційно-телекомунікаційними системами, захист інформації, що міститься в них; планує і здійснює заходи із забезпечення охорони державної таємниці та захисту інформації з обмеженим доступом, функціонування та безпеки застосування засобів зв'язку, автоматизації, криптографічного та технічного захисту інформації тощо[7]. Тобто йдеться про загальні заходи забезпечення безпеки інформації в ДПСУ і безпеки її засобів внутрішніх комунікацій.

---

[1] Про державний кордон України : Закон України від 04.11.1991 № 1777-XII // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/1777-12 (дата звернення: 26.12.2024).

[2] Про Державну прикордонну службу України : Закон України від 03.04.2003 № 661-IV // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/661-15 (дата звернення: 26.12.2024).

[3] Про затвердження Положення про Адміністрацію Державної прикордонної служби України : Постанова Кабінету Міністрів України від 16.10.2014 № 533 // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/533-2014-п (дата звернення: 26.12.2024).

[4] Про затвердження Положення про регіональне управління Державної прикордонної служби України : наказ Адміністрації Державної прикордонної служби України від 17.10.2003 № 173. Окреме видання.

[5] Про державний захист працівників суду і правоохоронних органів : Закон України від 23.12.1993 № 3781-XII // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/3781-12 (дата звернення: 26.12.2024).

[6] Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві : Закон України від 23.12.1993 № 3782-XII // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/3782-12 (дата звернення: 26.12.2024).

[7] Про затвердження Положення про орган охорони державного кордону Державної прикордонної служби України : наказ МВС України від 30.11.2018 № 971 // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/z1468-18 (дата звернення: 26.12.2024).

У визначенні поняття «власна безпека особового складу ДПСУ» теж відсутні згадки про інформаційну безпеку. Під забезпеченням власної безпеки військовослужбовців і працівників ДПСУ та їхніх близьких родичів розуміють систему заходів державного захисту від перешкоджання виконанню покладених на них законом обов'язків і здійсненню наданих прав, а також від посягань на життя, здоров'я, житло і майно зазначених осіб та їхніх близьких родичів у зв'язку зі службовою діяльністю цих осіб[1].

Порівняно з військовослужбовцями і працівниками ДПСУ, найбільш детально про повноваження державного службовця щодо інформації в процесі виконання службових обов'язків йдеться в Законі України «Про державну службу». Так, згідно з п. 9 ч. 1 ст. 4 Закону одним із принципів здійснення державної служби є принцип прозорості – відкритість інформації про діяльність державного службовця, крім випадків, визначених Конституцією та законами України. Пунктами 12, 13 ч. 1 ст. 8 цього ж Закону визначено, що державний службовець зобов'язаний зберігати державну таємницю та персональні дані осіб, що стали йому відомі у зв'язку з виконанням посадових обов'язків, а також іншу інформацію, яка відповідно до закону не підлягає розголошенню; надавати публічну інформацію в межах, визначених законом[2].

Отже, завдання ДПСУ у сфері забезпечення інформаційної безпеки в Законі України «Про Державну прикордонну службу України» та інших нормативно-правових актах не визначено. Такі завдання можна виокремити в процесі аналізу розділу «Механізми реалізації визначеної мети та завдань» Стратегії інформаційної безпеки на період до 2025 року. У ньому йдеться про те, що сили оборони, до яких відповідно до Закону України «Про національну безпеку України» належить і ДПСУ, у межах компетенції забезпечують проведення комплексу різноманітних заходів, серед яких: здійснення правових, організаційних, технічних, інформаційних та інших дій щодо забезпечення власної інформаційної безпеки, у тому числі захисту єдиного інформаційного середовища сил оборони, зокрема в місцях дислокації, розгортання та застосування угруповань, військових частин та підрозділів ДПСУ та інших військових формувань, утворених відповідно до законів України; протидія інформаційним операціям та іншим заходам інформаційного впливу, спрямованим проти ДПСУ; донесення достовірної інформації до військовослужбовців ДПСУ тощо (Половніков, Шеремет, 2023).

Це передбачає необхідність окремого розгляду питань інформаційної безпеки державних органів, їхнього особового складу. Відповідно окремий комплекс заходів органів (підрозділів) ДПСУ має стосуватися забезпечення інформаційної безпеки, яка охоплює інформаційну безпеку особи (особового складу) як складову власної (особистої) безпеки, а також інформаційну безпеку органів (підрозділів) ДПСУ як складову їхньої внутрішньої безпеки.

На думку Д. Матохнюка (2013), внутрішня безпека правоохоронного органу – це сукупність адміністративно-правових, оперативно-розшукових, контррозвідувальних, розвідувальних заходів щодо забезпечення інтересів правоохоронного органу у стабільному функціонуванні шляхом усунення негативних виявів антисоціального характеру у правоохоронній структурі (власна безпека), злочинного впливу на неї ззовні та забезпечення особистої безпеки правоохоронців, які проходять службу у відповідних органах.

Таке визначення заслуговує на увагу. Водночас, на нашу думку, внутрішня безпека ДПСУ – це, зокрема, її інформаційна безпека, яка охоплює особисту інформаційну безпеку особового складу (його захищеність від негативного інформаційно-психологічного впливу, втручання в його особисте (приватне) життя та спонукання (залучення) до протиправних та антисоціальних дій), а також захищеність органів (підрозділів) ДПСУ від протиправного деструктивного втручання в їхню службову діяльність шляхом порушення порядку та правил роботи з інформацією, використання окремих службових і посадових осіб для завдання шкоди стабільності й ефективному функціонуванню органу (підрозділу) ДПСУ через вчинення ними протиправних діянь.

Забезпечення внутрішньої безпеки ДПСУ передбачає здійснення комплексу організаційних, адміністративно-правових, оперативно-

[1] Про затвердження Інструкції про порядок організації та здійснення заходів власної безпеки військовослужбовців і працівників Державної прикордонної служби України та їх близьких родичів : наказ Адміністрації Держ. прикордон. служби України від 28.04.2004 № 354 // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/z0637-04 (дата звернення: 26.12.2024).

[2] Про державну службу : Закон України від 10.12.2015 № 889-VIII // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/889-19 (дата звернення: 26.12.2024).

розшукових, контррозвідувальних, розвідувальних та інших заходів щодо забезпечення інтересів ДПСУ у стабільному й ефективному функціонуванні органів (підрозділів) шляхом усунення ризиків та загроз у сфері службової діяльності особового складу, його інформаційної безпеки – захищеності від ризиків і загроз деструктивного і дезорганізуючого інформаційно-психологічного впливу, порушень вимог щодо захисту інформації, що можуть завдати шкоди життю, здоров'ю, інтересам служби (роботи) й ефективному функціонуванню органу (підрозділу) ДПСУ у звичайних умовах та нестандартних (надзвичайних) ситуаціях тощо.

ВИСНОВКИ. З урахуванням вищезазначеного можемо дійти таких висновків.

1. Інформаційна безпека особового складу ДПСУ є складним явищем та окремим видом безпеки, яку слід розглядати як у структурному аспекті, так і як певний стан.

У структурному аспекті інформаційна безпека особового складу ДПСУ, з одного боку, є складовою власної (особистої) безпеки військовослужбовця, державного службовця і працівника ДПСУ, а з другого – складовою внутрішньої безпеки органу (підрозділу) ДПСУ і ДПСУ у цілому як правоохоронного органу держави, що визначає стан забезпечення відомчої і державної безпеки. Ці дві складові тісно поєднані між собою. Крім того, структура інформаційної безпеки особового складу ДПСУ охоплює такі її елементи, як-от: система життєво важливих інтересів, прав і свобод людини і громадянина у сфері збирання, зберігання, обробки, аналізу та обміну інформацією; система ризиків і загроз, зумовлених різними факторами, процесами і діями в інформаційній сфері, а також суб'єктів (носіїв) загроз; система управління ризиками і загрозами в інформаційній сфері, система захисту та протидії тощо.

Як стан інформаційна безпека особового складу ДПСУ характеризується ступенем досягнення найбільшої відповідності (збалансованості) між життєво важливими особистими і службовими (державними) інтересами та їх захищеності у сфері збирання, зберігання, обробки, аналізу та обміну інформацією для оптимального функціонування системи суспільних відносин у цій сфері, що відповідають вимогам чинного законодавства України, інтересам особи, суспільства і держави.

2. З метою підтримання інформаційної безпеки особового складу ДПСУ в належному стані кожному військовослужбовцю, державному службовцю і працівнику ДПСУ необхідно суворо дотримуватись вимог щодо роботи зі службовою інформацією, бути пильним та уникати небезпеки (розпізнавати її (ризики й загрози в інформаційній сфері) і не потрапляти в неї), запобігати її проявам (знати заходи безпеки і дотримуватися їх, поводитись так, щоб не створювати небезпеку), діяти на випередження (у разі необхідності правильно скористатися знаннями, уміннями і навичками протидії ризикам та загрозам в інформаційній сфері).

3. Для належного нормативно-правового регулювання питань щодо інформаційної безпеки особового складу ДПСУ необхідно внести зміни до Закону України «Про Державну прикордонну службу України», положень про Адміністрацію ДПСУ, регіональне управління та орган охорони державного кордону ДПСУ щодо їхніх обов'язків і прав у сфері забезпечення інформаційної безпеки особового складу ДПСУ та визначення цього поняття.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Богуславський В. В. Завдання та принципи державної інформаційної політики у сфері забезпечення особистої безпеки працівників сил охорони правопорядку. *Науковий вісник Дніпропетровського державного університету внутрішніх справ.* 2016. № 4. С. 31–38.

2. Головенко Р., Котляр Д., Нестеренко О., Шевченко Т. Науково-практичний коментар до Закону України «Про доступ до публічної інформації» / за заг. ред. Д. Котляра. Київ : ГО «Фундація „Центр суспільних медіа"», 2012. 335 с.

3. Заєць О. В. Захищеність особи від негативного інформаційно-психологічного впливу як напрямок інформаційної безпеки України. *Вісник Харківського національного університету внутрішніх справ.* 2010. Вип. 4 (51), ч. 2. С. 149–155.

4. Закіров М. Б., Закірова С. Г. Дилема інформаційної безпеки особистості в інформаційному суспільстві. *Наукові праці Національної бібліотеки України імені В. І. Вернадського.* 2022. Вип. 63. С. 50–64. DOI: https://doi.org/10.15407/np.63.050.

5. Іванчук К. В. Комунікативна особистість мережі Інтернет у контексті забезпечення інформаційної безпеки держави. *Закарпатські філологічні студії.* 2021. Вип. 16. С. 135–139. DOI: https://doi.org/10.32782/tps2663-4880/2021.16.25.

6. Квіткін П., Дятлова І., Петрова Л. Інформаційна безпека особистості: теоретико-методологічний аналіз. *Вісник Національного юридичного університету імені Ярослава Мудрого. Серія: Філософія, філософія права, політологія, соціологія*. 2021. Т. 4, № 51. С. 46–62. DOI: https://doi.org/10.21564/2663-5704.51.241998.

7. Квіткін П., Дятлова І., Петрова Л. Інформаційна безпека особистості: фактори гомеостазису. *Вісник Національного юридичного університету імені Ярослава Мудрого. Серія: Філософія, філософія права, політологія, соціологія*. 2022. Т. 1, № 52. С. 136–147. DOI: https://doi.org/10.21564/2663-5704.52.250658.

8. Кушнір І. П. Співвідношення понять «інформаційна безпека» та «захист інформації» в діяльності Державної прикордонної служби України. *Науковий вісник Міжнародного гуманітарного університету. Серія: Юриспруденція*. 2018. № 35, т. 1. С. 81–84.

9. Матохнюк Д. Б. Поняття та визначення внутрішньої безпеки правоохоронного органу. *Науковий вісник Національної академії внутрішніх справ.* 2013. № 2. С. 77–82.

10. Олійник О. В. Позитивні та негативні впливи інформаційної революції на забезпечення інформаційної безпеки особи, суспільства, держави. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2011. Вип. 25–26. С. 321–328.

11. Половніков В. В., Шеремет В. О. Щодо завдань Державної прикордонної служби України у сфері забезпечення інформаційної безпеки // Сектор безпеки і оборони України на захисті національних інтересів: актуальні проблеми та завдання в умовах воєнного стану : тези ІІ Міжнар. наук.-практ. конф. (м. Хмельницький, 23 листоп. 2023 р.) / Нац. акад. Держ. прикордон. служби України ім. Богдана Хмельницького ; Нац. ун-т оборони України ; Харків. нац. ун-т Повітряних Сил ім. І. Кожедуба та ін. Хмельницький : Вид-во НАДПСУ, 2023. С. 988–990.

12. Соціальна інженерія (системний аналіз) : навч. посіб. / В. М. Петрик, В. Г. Курганевич, В. Г. Кононович та ін. ; за заг. ред. В. І. Курганевича, В. М. Петрика. Київ, 2019. 200 с.

13. Шевчук М. О. До питання генези поняття інформаційної безпеки як складової національної безпеки. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2023. Вип. 78, ч. 2. С. 134–139. DOI: https://doi.org/10.24144/2307-3322.2023.78.2.21.

Надійшла до редакції 30.12.2024

Прийнята до опублікування 11.03.2025

REFERENCES

1. Bohuslavskiy, V. V. (2016). Objectives and principles of the state information policy in the area of personal security forces of law enforcement personnel. *Scientific Bulletin of Dnipropetrovsk State University of Internal Affairs, 4*, 31–38.

2. Holovenko, R., Kotliar, D., Nesterenko, O., & Shevchenko, T. (2012). *Scientific and practical commentary on the Law of Ukraine "On Access to Public Information"* (D. Kotliar, Ed.). Foundation "Center for Public Media".

3. Ivanchuk, K. V. (2021). Communicative personality of the internet in the context of ensuring the information security of the state. *Transcarpathian Philological Studie, 16*, 135–139. https://doi.org/10.32782/tps2663-4880/2021.16.25.

4. Kushnir, I. P. (2018). The correspondence of concepts of "information security" and "information protection" in activities of the State Border Guard Service of Ukraine. *Scientific Herald of International Humanitarian University, 35*(1), 81–84.

5. Kvitkin, P., Diatlova, I., & Petrova, L. (2021). Personal information security: theoretical and methodological analysis. *The Bulletin of Yaroslav Mudryi National Law University. Series: Philosophy, Philosophies of Law, Political Science, Sociology, 4*(51), 46–62. https://doi.org/10.21564/2663-5704.51.241998.

6. Kvitkin, P., Diatlova, I., & Petrova, L. (2022). Personal information security: factors of homeostasis. *The Bulletin of Yaroslav Mudryi National Law University. Series: Philosophy, Philosophies of Law, Political Science, Sociology, 1*(52), 136–147. https://doi.org/10.21564/2663-5704.52.250658.

7. Matokhniuk, D. B. (2013). The concept and definition of internal security of a law enforcement agency. *Scientific Herald of the National Academy of Internal Affairs, 2*, 77–82.

8. Oliinyk, O. V. (2011). Positive and negative impacts of the information revolution on ensuring information security of the individual, society, and the state. *Combating Organized Crime and Corruption (Theory and Practice), 25–26*, 321–328.

9. Petryk, V. M., Kurhanevych, V. H., & Kononovych, V. H. et al. (2019). *Social engineering (system analysis)* (V. I. Kurhanevych, V. H., & V. M. Petryk, Eds.). Kyiv.

10. Polovnikov, V. V., & Sheremet, V. O. (2023, November 23). *Regarding the tasks of the State Border Guard Service of Ukraine in the field of ensuring information security* [Conference presentation abstract]. International Scientific and Practical Conference "The security and defense sector of Ukraine in the protection of national interests: current problems and tasks in conditions of martial law", Khmelnytskyi, Ukraine.

11. Shevchuk, M. O. (2023). On the question of the genesis of the concept of information security as a component of national security. *Uzhhorod National University Herald. Series: Law, 78*(2), 134–139. https://doi.org/10.24144/2307-3322.2023.78.2.21.

12. Zaiets, O. V. (2010). Protection of the individual from negative informational and psychological influence as a direction of information security in Ukraine. *Bulletin of Kharkiv National University of Internal Affairs, 4*(52), 149–155.

13. Zakirov, M. B., & Zakirova, S. H. (2022). The Dilemma of Information Security of the Individual in the Information Society. *Academic Papers of Vernadsky National Library of Ukraine, 63*, 50–64. https://doi.org/10.15407/np.63.050.

Received the editorial office: 30 December 2024

Accepted for publication: 11 March 2025

VADYM VOLODYMYROVYCH POLOVNIKOV,
Doctor of Law, Associate Professor,
Bohdan Khmelnytskyi National Academy
of the State Border Service of Ukraine,
Department of Management;
ORCID: https://orcid.org/0000-0002-8054-909X,
e-mail: vpolovnikov@ukr.net

INFORMATION SECURITY OF THE PERSONNEL OF THE STATE BORDER GUARD SERVICE OF UKRAINE: PROBLEMATIC ISSUES OF NORMATIVE AND LEGAL REGULATION

The article analyses the current legislation of Ukraine which provides for normative and legal regulation of public relations in the information sphere of activity of security and defence forces, in particular, the State Border Guard Service of Ukraine, and also the scientific views of scholars on the content of the concepts of information security of an individual, society and the State.

Based on the results of the analysis, the study provides a definition of the concept of information security of the personnel (officers and officials) of the State Border Guard Service of Ukraine with due regard for the need to ensure civil rights and obligations in the information sphere and to fulfil the requirements determined by the specifics of official activities and the legal status of personnel regarding the collection, storage, use and dissemination of information.

It is proposed to consider information security of the personnel of the State Border Guard Service of Ukraine in the structural aspect as a certain state and as a process. In the structural aspect, the concept of information security of the personnel of the State Border Guard Service of Ukraine includes the following components: protection of constitutional rights and freedoms of a person with regard to information; protection of information networks and services; protection of personal data; protection of restricted information; protection against hostile propaganda, distortion of information, disinformation, fakes, etc. Information security as a state is determined by the degree of achievement of the greatest correspondence (balance) between the vital personal and official (state) interests of the personnel of the State Border Guard Service of Ukraine in the field of collection, storage, processing, analysis and exchange of information. In the functional aspect, information security is identified with the concept of "ensuring security" and is viewed as a set of organisational, legal, technical, managerial and other measures which constitute the process of ensuring the security of public relations in the information sphere.

The author emphasises the need to improve the legal and regulatory framework for the activities of the personnel of the State Border Guard Service of Ukraine in the information sphere, and also provides proposals for amending the current legislation of Ukraine, in particular, the Law of Ukraine "On the State Border Guard Service of Ukraine".

Keywords: *security, information security of an individual, society and the state, personnel, State Border Guard Service of Ukraine, information, information and psychological influence.*

Цитування (ДСТУ 8302:2015): Половніков В. В. Інформаційна безпека особового складу Державної прикордонної служби України: проблемні питання нормативно-правового регулювання. *Право і безпека*. 2025. № 1 (96). С. 67–77. DOI: https://doi.org/10.32631/pb.2025.1.06.

Citation (APA): Polovnikov, V. V. (2025). Information security of the personnel of the State Border Guard Service of Ukraine: problematic issues of normative and legal regulation. *Law and Safety, 1*(96), 67–77. https://doi.org/10.32631/pb.2025.1.06.