УДК 342.9: 004.056: 351.74
DOI: 10.32342/3041-2218-2024-2-9-9

ОЛЕКСАНДР МОСКАЛИК,
аспірант Сумського державного університету
ORCID: 0009-0002-9998-6027

АДМІНІСТРАТИВНО-ПРАВОВІ ЗАСАДИ УЧАСТІ ДЕРЖАВНОГО БЮРО РОЗСЛІДУВАНЬ В ІНФОРМАЦІЙНИХ ВІДНОСИНАХ

У статті розглядаються адміністративно-правові засади участі Державного бюро розслідувань (ДБР) в інформаційних відносинах України. Акцентовано увагу на перспективах оптимізації статусу ДБР як учасника інформаційних відносин. На основі аналізу актів чинного законодавства проаналізовано роль і функціональне навантаження ДБР у забезпеченні національної безпеки крізь призму управління інформаційною сферою з урахуванням триваючих змін інформаційної складової соціального розвитку українського суспільства. Окрему увагу приділено аспектам забезпечення захисту інформації в умовах сучасних кіберзагроз та відсутності єдиних стандартів збереження та обробки даних. Висвітлено проблематику функціонування системи органів забезпечення правопорядку, яка виникає у цьому зв'язку. У статті презентовано авторський підхід до характеристики особливостей правових та організаційних аспектів участі ДБР в обробці інформації та, зокрема, механізмів зберігання, опрацювання та використання конфіденційних даних. Обґрунтовано важливість впровадження міжнародних стандартів забезпечення безпеки інформації у діяльності ДБР, ініціювання інноваційних моделей обробки інформації в умовах правового режиму воєнного стану. З огляду на швидкий розвиток інформаційних технологій і постійне вдосконалення методів створення кіберзагроз, запропоновано оновлення правових засад регулювання взаємодії Державного бюро розслідувань з іншими державними органами та міжнародними партнерами. Цей процес передбачає створення інтегрованої системи кіберзахисту, яка забезпечить високий рівень безпеки інформаційних систем на всіх етапах обробки даних починаючи від збору і закінчуючи їх використанням. Доведено, що необхідність удосконалення цих механізмів детермінується як глобальними викликами, так і специфічними вимогами, які ставляться до роботи правоохоронних органів у сфері захисту національної безпеки та конфіденційної інформації. Окреслено контури перспективної програми підготовка персоналу ДБР у сфері кібербезпеки. Вона включає у себе як спеціальне навчання існуючого складу, так і підготовку нових фахівців, здатних ефективно реагувати на сучасні кіберзагрози та володіти необхідними знаннями щодо оперативної і високотехнологічної протидії їм. Систематична підготовка спеціалістів вимагає розробки спеціальних навчальних програм і курсів, що охоплюють всі аспекти кібербезпеки, від основних принципів захисту інформації до глибоких технічних знань щодо протидії кібератакам та виявлення ступеня їх загроз. У висновках підкреслюється необхідність розробки єдиного підходу до захисту інформаційних систем у ДБР, удосконалення правової регламентації та посилення співпраці на міжнародному рівні для поліпшення кіберзахисту, що дозволить підвищити ефективність роботи структурних підрозділів ДБР, зберігаючи при цьому конфіденційність та безпеку інформації.

Ключові слова: право, адміністративно-правові засади, Держане бюро розслідувань, інформаційні відносини, кіберзахист, конфіденційна інформація.

Постановка проблеми. Інформаційні відносини відіграють ключову роль у функціонуванні сучасної держави, особливо у сфері правоохоронної діяльності. Державне бюро розслідувань (ДБР – далі) як спеціалізований правоохоронний вносить вагомий внесок у забезпечення верховенства права, протидії злочинності та захисті інтересів держави, громадян і суспільства. Участь ДБР в інформаційних відносинах є багато-

аспектною і передбачає, передусім, збирання, обробку, зберігання та використання інформації, що має вирішальне значення для виконання покладених на нього завдань.

В умовах правового режиму воєнного стану актуальність зазначеної проблематики набуває особливої значущості. Ефективне регулювання участі ДБР в інформаційних відносинах є запорукою забезпечення правопорядку, національної безпеки, ефективної протидії дезінформаційним загрозам та захисту національного інформаційного середовища. Більш того, роль ДБР у виявленні та запобіганні інформаційним загрозам, таким як кібератаки та поширення неправдивої інформації, з кожним днем посилюється за умов як внутрішніх, так і зовнішніх загроз національній державності України.

Стан дослідження. На сучасному етапі розвитку правової науки дедалі все більша увага вчених приділяється дослідженню даної тематики, зокрема у даній сфері працювали та працюють: Р. Богданов, О. Лятіна, О. Синєокий, М. Фігель, В. Кохановська, Г. Шорохова та інші. Проте, зазначені напрацювання не носять комплексного характеру, що вказує на доцільність збагачення наукової доктрини з обраної проблематики.

Метою статті є висвітлення базових аспектів адміністративно-правового регулювання участі ДБР в інформаційних відносинах з урахуванням актуальних викликів і загроз національному інформаційному середовищу.

Виклад основного матеріалу. Інформація є ключовим ресурсом, від якого залежить розвиток та функціонування як окремих інститутів держави та суспільства в цілому. Зважаючи на це, дослідження інформаційної сфери набуває пріоритетного значення серед науковців, зокрема в галузі правознавства. Сучасне суспільство, без сумніву, можна охарактеризувати як інформаційне – новий тип суспільства, в якому виникають, розвиваються та припиняються інформаційні правовідносини.

Правовідносини завжди перебувають у центрі уваги науковців завдяки їхній складності, багатогранності та динамічності. Водночас це одна з основних правових категорій, яка отримала глибоке теоретичне обґрунтування та визнання. Така двоїстість свідчить про необхідність постійного дослідження правовідносин з різних точок зору. Як слушно зауважує О.І. Лятіна, гармонійне поєднання та вільне використання різноманітних підходів у вивченні правовідносин та соціальних процесів дозволяють глибше розкрити численні риси та властивості цих явищ, а також сформувати об’єктивне та багатовимірне уявлення про правове життя суспільства [1, с. 403].

В рамках даного дослідження в першу чергу варто з’ясувати суть інформаційних правовідносин. У законодавстві України не закріплено визначення поняття «інформаційні правовідносини» та не визначені їх ознаки, що ускладнює що ускладнює формування чітких меж цього правового явища та унеможливлює його системне регулювання. Це спричиняє нормативні прогалини у сфері інформаційних взаємодій, що особливо актуалізується в умовах стрімкого розвитку цифрових технологій.

У статті 3 Закону України «Про інформацію» (далі – Закон) визначаються ключові принципи інформаційних відносин [2]. Серед них – гарантованість права на інформацію, відкритість і доступність інформації, свобода її обміну, достовірність і повнота, а також свобода вираження поглядів і переконань. Важливими аспектами є правомірність отримання, використання, поширення, зберігання та захисту інформації, а також забезпечення захисту особистого і сімейного життя людини від втручань.

У статті 4 наведено вище Закону деталізуються суб’єкти інформаційних відносин, до яких належать фізичні та юридичні особи, об’єднання громадян, органи державної влади, а також об’єкт цих відносин, яким виступає інформація. Таким чином, Закон закладає основи регулювання інформаційних відносин, визначаючи їх учасників та базові принципи.

Також немає єдності серед науковців, щодо визначення поняття «інформаційні правовідносини». Так для прикладу, О.В. Синєокий визначає інформаційні правовідносини як суспільні зв’язки, що формуються у процесі створення, розподілу та використання інформації. Ці відносини регулюються нормами інформаційного права, а їх учасники наділені відповідними юридичними правами та обов’язками [3, с.98]. В свою чергу науковець М.В. Фігель описує інформаційні правовідносини як суспільні зв’язки, врегульовані нормами інформаційного права, учасники яких мають юридичні права та обов’язки, що стосуються створення, розподілу та використання інформації відповідно до встановлених приписів [4, с. 234].

В. О. Кохановська вважає, що інформаційні правовідносини являють собою суспільні відносини, що регулюються інформаційно-правовими нормами, де учасники мають взаємні права та обов'язки, встановлені та гарантовані цими нормами [5, с. 17].

З огляду на вищевикладене можемо сформувати власне розуміння поняття «інформаційні правовідносини» – це врегульовані нормами інформаційного права суспільні відносини, що виникають у процесі створення, обробки, поширення, використання та захисту інформації, учасники яких наділені взаємними юридичними правами та обов'язками, спрямованими на забезпечення правомірного обміну інформацією та захист інформаційних прав суб'єктів.

Г. М. Шорохова вважає, що глобалізація та інформатизація значно впливають на розвиток сучасного світу. У період науково-технічного прогресу та активного впровадження інформаційних технологій, інформація стає важливим ресурсом для перетворень у державі та суспільстві. Вона є необхідною для ефективного функціонування органів внутрішніх справ, адже без неї неможливе виконання завдань, реалізація управлінських рішень та оцінка ситуації. Правопорядок вимагає постійного вдосконалення, що можна забезпечити лише через належне інформаційне забезпечення [6, с. с. 44].

Згідно з Законом України «Про Державне бюро розслідувань», бюро є центральним органом виконавчої влади зі спеціальним статусом, а також правоохоронним органом спеціального призначення. ДБР створюється Кабінетом Міністрів України на основі закону, діючи в межах виділених для утримання органів виконавчої влади коштів [7].

ДБР займає центральну роль у національній системі інформаційної безпеки України, виконуючи важливі функції, спрямовані на захист даних та протидію інформаційним загрозам. Як орган, що спеціалізується на розслідуванні злочинів, ДБР опікується збором, аналізом та обробкою великої кількості чутливої інформації, що робить його діяльність у сфері інформаційної безпеки критично важливою. Примітно, що однією з основних функцій ДБР є інформаційно-аналітична діяльність. Зазначений напрямок передбачає створення та використання баз даних для розслідувань, а також прогнозування ризиків. У цьому контексті захист конфіденційної інформації є ключовим завданням. Використання сучасних методів кіберзахисту, таких як шифрування даних, багаторівнева аутентифікація та регулярний аудит інформаційних систем, сприяє зменшенню ризиків несанкціонованого доступу або втручання у роботу систем.

Ефективність діяльності ДБР у сфері інформаційної безпеки значною мірою залежить від співпраці з іншими державними органами, зокрема з Службою безпеки України, Міністерством внутрішніх справ і Міністерством цифрової трансформації України. Ця координація дозволяє посилити захист національного інформаційного простору через спільне використання ресурсів та обмін інформацією.

Законодавчою основою для діяльності ДБР у сфері інформаційної безпеки є нормативно-правові акти, такі як Закони України «Про захист інформації в інформаційно-телекомунікаційних системах», «Про державну таємницю» та «Про захист персональних даних». Однак, як показує практика, існує потреба в удосконаленні правового регулювання, зокрема щодо визначення правового статусу інформації на різних етапах її обробки та використання.

Важливим аспектом є міжнародна співпраця ДБР у сфері кіберзахисту. Інтеграція до міжнародних ініціатив та обмін досвідом з іншими країнами дозволяє використовувати сучасні технології та найкращі практики для підвищення ефективності захисту інформаційних систем. Це особливо актуально в умовах глобальної цифровізації, яка постійно ускладнює виклики в сфері інформаційної безпеки.

Таким чином, ДБР виконує не лише функції правоохоронного органу, а й є важливим елементом національної системи інформаційної безпеки. Розвиток технічної бази, впровадження інноваційних технологій, удосконалення правового регулювання та розширення міжнародної співпраці є перспективними напрямами для підвищення ефективності його діяльності [7].

Богданов Р.І. зазначає, що інформаційне забезпечення діяльності територіальних управлінь ДБР є ключовим аспектом їхньої ефективності [8, с 151]. І в аспекті цього вважаємо, що необхідно дослідити роль Державного бюро розслідувань у системі інформаційних правовідносин.

Одним із ключових аспектів роботи Державного бюро розслідувань у сфері інформаційних відносин є його відповідальність за управління та обробку конфіденційної інформації, пов'язаної з розслідуваннями, що проводяться. Це вимагає не лише дотримання чинного законодавства, а й забезпечення належного рівня захисту персональних даних. Це включає в себе ефективну та безпечну обробку інформації, пов'язаної з розслідуваннями, в яких беруть участь державні службовці та працівники правоохоронних органів. ДБР працює в рамках правових механізмів, які регулюють доступ до такої інформації, обмін нею та її захист, що підкреслює важливість Бюро в загальній системі адміністративного та кримінального права.

У контексті адміністративно-правових засад участі ДБР в інформаційних відносинах, зазначені функції інформаційного забезпечення є ключовими для ефективного виконання його завдань у сучасних умовах. Інформативна функція сприяє точному прийняттю управлінських та правоохоронних рішень, що є основою для належного функціонування ДБР у правовому полі. Управлінська функція дозволяє ефективно управляти процесами та забезпечувати якісний контроль. Організаційно-комунікативна функція забезпечує гармонійну взаємодію в межах органу і з іншими структурами, що є важливим для успішної реалізації адміністративно-правових завдань. Освітньо-виховна функція підвищує професійний рівень співробітників, що, у свою чергу, сприяє зміцненню правової культури у сфері інформаційних відносин. В умовах постійних викликів та необхідності адаптації до нових інформаційних технологій, ці функції є основою для подальшого розвитку та вдосконалення участі ДБР в інформаційних відносинах [8, с. 197].

Так, відповідно до Закону України «Про доступ до публічної інформації» ДБР виконує функції розпорядника публічної інформації [9]. Це означає, що орган зобов'язаний надавати інформацію на запити зацікавлених осіб, за умови, що доступ до такої інформації не обмежений законодавством. Водночас ДБР має забезпечувати дотримання режиму захисту інформації з обмеженим доступом, зокрема державної таємниці.

ДБР є невід'ємною частиною забезпечення цілісності та прозорості інформації в контексті кримінальної юстиції України, охороняючи законні права громадян та забезпечуючи ефективне проведення розслідувань без зовнішнього втручання.

Зовнішні форми інформаційного забезпечення діяльності територіальних управлінь ДБР є важливими для реалізації адміністративно-правових засад участі в інформаційних відносинах. Запити, обліки, обмін даними, підготовка звітів і участь у різноманітних заходах забезпечують ефективну взаємодію з іншими органами влади та правоохоронними структурами. Ці форми допомагають органам ДБР оперативно реагувати на виклики сучасності, підвищувати якість управлінських рішень та сприяти ефективному виконанню завдань у сфері інформаційних відносин [10].

Варто зазначити, що на даному етапі нашого життя, в умовах ведення повномасштабних бойових дій країною агресором так і ведення гібридної війни перед Державним бюро розслідувань постає низка загроз котрі потребують їх вирішення та підтримання інформаційної безпеки. До таких проблем належить кіберзагрози. Так, як було згадано вище ДБР має справу з інформацією, яка має обмежений доступ та є стратегічно важливою для держави.

Інформаційна безпека – це сукупність заходів, стратегій і політик, спрямованих на захист інформаційних ресурсів, даних і пов'язаної з ними інфраструктури від загроз, які можуть призвести до несанкціонованого доступу, втрати, пошкодження або неналежного використання інформації. Вона охоплює забезпечення конфіденційності, цілісності та доступності даних, а також заходи, що протидіють кібератакам, витокам інформації та іншим небезпекам, які можуть мати суттєві наслідки для організацій, держав і окремих осіб [11].

Проблеми, пов'язані з використанням інформаційних систем, мають ключове значення в контексті адміністративно-правових засад участі ДБР в інформаційних відносинах, адже сучасна цифровізація та кіберзагрози суттєво впливають на ефективність функціонування цього органу [12].

По-перше, одним із важливих аспектів є забезпечення доступності, цілісності та конфіденційності інформаційних ресурсів і супутньої інфраструктури. Зокрема, інформаційна діяльність ДБР залежить від стабільної роботи інформаційних систем, які використовують-

ся для збору, обробки та зберігання даних. Порушення цілісності або доступності інформації, наприклад, внаслідок технічних збоїв або кіберзагроз, може негативно вплинути на хід розслідувань і результати правоохоронної діяльності. Витік конфіденційних даних, зокрема оперативної інформації, може створити серйозні ризики для національної безпеки та прав осіб, залучених до слідчих дій.

По-друге, інформаційна безпека в діяльності ДБР — це не лише технічні заходи, а й адміністративно-правове регулювання, яке включає встановлення чітких правил для захисту інформаційних ресурсів. У цьому контексті ключовою проблемою є нормативно-правова невизначеність статусу інформації, яка збирається під час розслідувань. Законодавство недостатньо деталізує правила обробки, зберігання й передачі даних, зокрема тих, що отримані під час оперативно-розшукової діяльності. Це створює ризики неналежного використання даних або їх втрати. Крім того, не визначено чітких механізмів доступу до інформації іншими органами, що може створювати конфлікти компетенції та уповільнювати обмін даними.

Закон України «Про Державне бюро розслідувань» не дає чіткого визначення, чи є зібрана інформація доказом, службовою інформацією, чи такою, що має обмежений доступ. Вищезгаданий закон також не уточнює, коли зібрана інформація переходить у статус доказу, або чи має вона спеціальний правовий статус на етапі оперативної діяльності. Якщо звернутися до кримінально процесуального кодексу України [13], а саме до статті 84 в якій зазначається, що доказами є фактичні дані, отримані у встановлений законом спосіб, однак знову ж таки, дана стаття не розрізняє інформацію, зібрану в результаті оперативно-розшукової діяльності та процесуального провадження.

Вважаємо, що дану проблему можна вирішити шляхом внесення змін до Закону України «Про Державне бюро розслідувань» чітко визначивши, яка інформація, зібрана під час розслідувань, є доказом, службовою інформацією чи такою, що має обмежений доступ. Зокрема, слід зазначити, що зібрана інформація може мати різний правовий статус на різних етапах розслідування: на початковій стадії вона може класифікуватися як оперативна інформація, яка після її перевірки та належного оформлення може набувати статусу доказу. Варто також зазначити, що дана проблематика належить не лише для ДБР, але й для більшості правоохоронних органів України.

У контексті сучасних кіберзагроз захист конфіденційної інформації набуває критичної важливості для органів, що здійснюють роботу з інформацією, зокрема для ДБР. Основними проблемами є ризики кібератак, несанкціонованого доступу до інформаційних систем та втручання в бази даних, що може не тільки знижувати ефективність функціонування органів, а й ставити під загрозу безпеку інформації. Це стає особливо актуальним в умовах воєнного стану, коли інтенсивність кібератак значно зростає, що потенційно може призвести до серйозних наслідків.

Однією з ключових проблем є недостатня кількість кваліфікованих фахівців у сфері кібербезпеки, обмежені ресурси на розвиток інфраструктури для захисту даних, а також недостатня інтеграція національних і міжнародних стандартів кібербезпеки в усіх сферах державного управління. В Україні зокрема фіксуються проблеми з захистом персональних даних, що є особливо важливим аспектом для таких органів, як ДБР, які мають справу з великою кількістю чутливої інформації, що потребує належного захисту [14].

Відсутність єдиних стандартів захисту інформації в Державному бюро розслідувань є ще однією із серйозних проблем, яка може впливати на ефективність роботи та національну інформаційну безпеку. Відсутність уніфікованих стандартів захисту інформації призводить до розбалансованості в підходах до безпеки, зокрема щодо управління даними та реагування на кіберзагрози. Це підтверджується численними дослідженнями в сфері інформаційної безпеки.

Організація систем захисту інформації в державних установах, зокрема в Державному бюро розслідувань, повинна базуватися на міжнародно визнаних стандартах, таких як ISO/IEC 27001. Дотримання цих стандартів забезпечує систематичний підхід до управління ризиками та гарантує високий рівень кібербезпеки. Проте в Україні часто спостерігається недостатній рівень адаптації зазначених стандартів до специфіки національної правової системи та організаційної структури, що створює додаткові труднощі для їх ефективного впровадження в діяльність державних органів [15].

Висновок. Чинні на сьогодні адміністративно-правові засади участі Державного бюро розслідувань у інформаційних відносинах є однією із запорук стабільного розвитку інформаційної сфери та убезпечення її складових від загроз противоправного втручання. Основними проблемами правового змісту, які обумовлюють певну обмеженість інформаційної дієздатності ДБР є відсутність єдиних стандартів захисту інформації, недостатня адаптація міжнародних норм до національного законодавства, а також недостатній рівень кадрового потенціалу в сфері, зокрема, протидії кіберзагрозам. Відповідно, важливим є вдосконалення законодавчої бази для забезпечення чіткого визначення статусу інформації, зібраної під час оперативної діяльності, її класифікації та використання в доказовій базі.

Впровадження міжнародно визнаних стандартів, таких як ISO/IEC 27001, посилення співпраці з міжнародними партнерами та формування внутрішніх інструкцій для управління інформацією можуть значно підвищити рівень ефективності системи захисту інформації в ДБР. Подальша оптимізація участі ДБР в інформаційних відносинах можлива лише за умови первинного впровадження у діяльність ДБР інноваційних технологій, посиленні інституційної спроможності та інтеграції найкращих зарубіжних практик участі подібних до ДБР структур у забезпеченні інформаційної безпеки держави. Нормативне забезпечення виконання зазначених завдань можливе лише за умов системного та скоординованого підходу до нормотворчості спеціалістів з органів законодавчої і виконавчої влади, наукового середовища і громадянського суспільства.

Список використаних джерел

1. Лятіна О.І. Поняття правовідносин у контексті законницької та юридичної доктрин. *Часопис Київського університету права*. 2013. № 4. С. 403-406.

2. Про інформацію: Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 03.12.2024).

3. Синєокий О.В. Високотехнологічне інформаційне право України. Харків: Право, 2010. С. 360.

4. Фігель М.В. Доступ до інформації та електронне урядування. Київ: Факт, 2004. С. 336.

5. Кохановська О. В. Теоретичне підґрунтя для визначення ролі нотаріуса у захисті інформаційних прав учасників цивільних правовідносин. *Бюлетень Міністерства юстиції України*. 2010. № 8. С. 16-24.

6. Бандурка О.М. Теорія і практика управління органами внутрішніх справ України: монографія. Харків: Скорпіон ЛТД, 2012. Т. 4. 756 с.

7. Про Державне бюро розслідувань: Закон України від 12.11.2015 № 794-VIII. URL: https://zakon.rada.gov.ua/laws/show/794-19#Text (дата звернення: 25.11.2024).

8. Богданов Р.І. Адміністративно-правовий статус територіальних управлінь державного бюро розслідувань: дис. … канд. юрид. наук: 12.00.07. Харків, 2024. 368 с.

9.Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 04.12.2024).

10. Богданов Р.І. Поняття та значення інформаційного забезпечення територіальних управлінь Державного бюро розслідувань. Взаємодія громадянського суспільства з сектором безпеки і оборони: сучасні виклики: тези доп. учасників наук.-практ. конф. (Харків, 21 груд. 2021 р.), с. 158-160. URL: https://library.pp-ss.pro/index.php/ndippsn_20211221/article/view/bohdanov.

11. Залєвська І.І., Удренас Г.І. Інформаційна безпека в Україні в умовах російської військової агресії. *Південноукраїнський правничий часопис*. 2022. №1. С. 20–26.

12. Виздрик В., Мельник О. Інформаційна безпека в Україні. *Grail of Science.* 2023. №24. С.196–202. URL: https://doi.org/10.36074/grail-of-science.17.02.2023.034.

13. Кримінальний процесуальний кодекс України : Кодекс України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 08.12.2024).

14. Кібербезпека: Україна може стати джерелом інновацій світового рівня. *Міністерство цифрової трансформації України.* 2019. URL: https://thedigital.gov.ua/news/kiberbezpeka-ukraina-mozhe-staty-dzherelom-innovaciy-svitovogo-rivnya.

15. Захарова О. В., Рудий А. Т. Засади захисту інформації в інформаційних системах підрозділів МВС. *Науковий вісник Львівського державного університету внутрішніх справ*. 2013. № 4. С. 349–357. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/2043/1/4-2013zovspm--.pdf.

ADMINISTRATIVE AND LEGAL BASIS OF THE PARTICIPATION OF THE DBR IN INFORMATION RELATIONS

Oleksandr M. Moskalyk, Postgraduate student of Sumy State University.
E-mail: S_moskal@ukr.net
DOI: 10.32342/3041-2218-2024-2-9-9

Key words: *administrative and legal principles, DBR, information relations, cyber protection, confidential information.*

The article examines the administrative and legal foundations of the participation of the State Bureau of Investigation (SBI) in Ukraine's informational relations, with a focus on contemporary challenges and development prospects for this institution. The author analyzes the role of the SBI in ensuring national security through information management and the protection of confidential data amid dynamic changes in the informational space. Special attention is paid to issues of information protection in the face of modern cyber threats and the absence of unified standards for data storage and processing, which present significant challenges for law enforcement activities. The article also highlights legal and organizational aspects of working with information, particularly mechanisms for storing, processing, and using confidential data. The author emphasizes the importance of implementing international information security standards and integrating them into the national legal framework, considering contemporary challenges, especially under martial law conditions. Given the rapid development of information technologies and the constant evolution of cyber threats, the need for regular updates to the legal mechanisms governing the interaction of the SBI with other state bodies and international partners becomes evident. This process involves creating an integrated cybersecurity system that ensures a high level of security for information systems at all stages of data processing, from collection and storage to usage. The need to improve these mechanisms stems not only from global challenges, such as the increasing number of cyberattacks, but also from specific demands placed on law enforcement agencies in protecting national security and confidential information. One of the key aspects requiring attention is the comprehensive training of personnel in the field of cybersecurity. This includes both the education of existing staff and the preparation of new specialists capable of effectively responding to modern cyber threats and possessing the necessary knowledge about cutting-edge information protection technologies. Systematic training demands the development of specialized training programs and courses covering all aspects of cybersecurity, from the basic principles of information protection to advanced technical knowledge in combating cyberattacks and identifying vulnerabilities in systems. The conclusion emphasizes the need to develop a unified approach to protecting information systems in the SBI, improve legal regulation, and enhance international cooperation to strengthen cybersecurity. This will improve the efficiency of the bureau's operations while maintaining the confidentiality and security of information in the face of modern challenges.

References

1. Liatina, O.I. (2013). *Poniattia pravovidnosyn u konteksti zakonnytskoi ta yurydychnoi doktryn* [The concept of legal relations in the context of legalistic and juridical doctrines]. *Chasopys Kyivskoho universytetu prava* [Kyiv University Law Journal], no. 4, pp. 403–406.

2. The Verkhovna Rada of Ukraine (1992), The Law of Ukraine "On Information", available at: https://zakon.rada.gov.ua/laws/show/2657-12#Text [in Ukrainian].

3. Synieokyi, O.V. (2010). *Vysokotekhnolohichne informatsiine pravo Ukrainy* [High-tech information law of Ukraine]. Kharkiv, Pravo Publ., 360 p.

4. Fihel, M.V. (2004). *Dostup do informatsii ta elektronne uriaduvannia* [Access to information and e-governance]. Kyiv, Fakt Publ., 336 p.

5. Kokhanovska, O.V. (2010). *Teoretychne pidgruntia dlia vyznachennia roli notariusa u zakhysti informatsiinykh prav uchasnykiv tsyvilnykh pravovidnosyn* [Theoretical foundations for defining the role of notaries in protecting the information rights of participants in civil relations]. *Biuleten Ministerstva yustytsii Ukrainy* [Bulletin of the Ministry of Justice of Ukraine], no. 8, pp. 16–24.

6. Bandurka O.M. (2012). *Teoriia i praktyka upravlinnia orhanamy vnutrishnikh sprav Ukrainy* [Theory and practice of management of internal affairs bodies of Ukraine]. Monograph, Kharkiv, Skorpion LTD, 756 p.

7. The Verkhovna Rada of Ukraine (2015), The Law of Ukraine “On the State Bureau of Investigation”. Available at: https://zakon.rada.gov.ua/laws/show/794-19#Text [in Ukrainian].

8. Bohdanov, R.I. (2024). *Administratyvno-pravovyi status terytorialnykh upravlin derzhavnoho biuro rozsliduvan* Diss. kand. yuryd. nauk [Administrative and legal status of the territorial offices of the State Bureau of Investigation Cand. of Legal. sci. diss.]. Kharkiv, 368 p.

9. The Verkhovna Rada of Ukraine (2011), The Law of Ukraine “On Access to Public Information”, available at: https://zakon.rada.gov.ua/laws/show/2939-17#Text [in Ukrainian].

10. Bohdanov, R.I. (2021). *Poniattia ta znachennia informatsiinoho zabezpechennia terytorialnykh upravlin Derzhavnoho biuro rozsliduvan. Vzaiemodiia hromadianskoho suspilstva z sektorom bezpeky i oborony* [The concept and importance of information support for the territorial offices of the State Bureau of Investigation. In Interaction of Civil Society with the Security and Defense Sector: Current Challenges] *Tezy dop. uchasnykiv nauk.-prakt. konf*. [Theses of additional participants of the scientific-practical conference]. Kharkiv, pp. 158–160. Available at: https://library.pp-ss.pro/index.php/ndippsn_20211221/article/view/bohdanov.

11. Zalievska, I.I., Udrenas, H.I. (2022). *Informatsiina bezpeka v Ukraini v umovakh rosiiskoi viiskovoi ahresii* [Information security in Ukraine under conditions of Russian military aggression]. *Pivdennoukrainskyi pravnychyi chasopys* [Southern Ukrainian Law Journal], pp. 20-26.

12. Vyzdryk, V., Melnyk, O. (2023). *Informatsiina bezpeka v Ukraini* [Information security in Ukraine]. *Grail of Science* [Grail of Science], pp. 196–202. Available at: https://doi.org/10.36074/grail-of-science.17.02.2023.034.

13. The Verkhovna Rada of Ukraine (2012), The Law of Ukraine “Criminal Procedure Code of Ukraine”. Available at: https://zakon.rada.gov.ua/laws/show/4651-17#Text [in Ukrainian].

14. *Ministerstvo tsyfrovoi transformatsii Ukrainy* (2019). [Ministry of Digital Transformation of Ukraine] *Kiberbezpeka: Ukraina mozhe staty dzherelom innovatsii svitovoho rivnia* [Cybersecurity: Ukraine can become a source of world-class innovations]. Available at: https://thedigital.gov.ua/ news/kiberbezpeka-ukraina-mozhe-staty-dzherelom-innovaciy-svitovogo-rivnya.

15. Zakharova, O.V., Rudyi, A.T. (2013). *Zasady zakhystu informatsii v informatsiinykh systemakh pidrozdiliv MVS* [Principles of information protection in the information systems of the Ministry of Internal Affairs units]. *Naukovyi visnyk Lvivskoho derzhavnoho universytetu vnutrishnikh sprav* [Scientific Bulletin of the Lviv State University of Internal Affair], no. 4, pp. 349–357. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/2043/1/4-2013zovspm--.pdf.

Одержано 13.12.2024.