6. Нагребельний В.П., Чернадчук В.Д., Сухонос В.В. Фінансове право України. Загальна частина: Навчальний посібник / За заг. ред. члена-кореспондента АПрН України В.П. Нагребельного. Київ, 2003. 213 с.

7. Про місцеве самоврядування в України : Закон України від 21.05.1997 р. № 280/97-ВР. *Відомості Верховної Ради України*. 1997. № 24. Ст. 170.

8. Місцеві податки та збори. Центральний офіс реформ при Мінрегіоні. URL: https://storage.decentralization.gov.ua/uploads/library/file/261/Буклет_-_Місцеві_податки__перегляд___1_.pdf (дата звернення: 11.03.2019).

9. Податковий кодекс України : Закон України від 02.12.2010 р. № 2755-VI. *Відомості Верховної Ради України*. 2011. № 13-14. № 15-16, № 17. Ст. 112.

10. Про співробітництво територіальних громад : Закон України від 17.06.2014 р. № 1508-VII. *Відомості Верховної Ради України*. 2014. № 34. Ст. 1167.

УДК 341:004+342.9
DOI https://doi.org/10.32844/2618-1258.2019.4-2.39

ТАРАСЮК А.В.

ДОСВІД ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В ЗАРУБІЖНИХ КРАЇНАХ

Мета статті − аналіз найбільш складних і актуальних проблем забезпечення кібербезпеки в країнах ЄС і формування єдиної політики в цій сфері. Розглянуто загальні політичні та економічні чинники актуалізації проблем кібербезпеки на національному, наднаціональному та глобальному рівнях. На прикладі Румунії та Польщі проілюстровано становлення системи кіберзахисту в країнах Східної Європи. На прикладі Німеччини та Фінляндії показано, що політика у сфері забезпечення кібербезпеки у низці розвинених країн ЄС більш ефективна, ніж політика на наднаціональному загальноєвропейському рівні. Зроблено висновок, що відмінною рисою німецького підходу до забезпечення кібербезпеки є його комплексний і фундаментальний характер, який включає цілу систему нормативних актів, планів й інститутів. Виявлено основні підходи й тенденції, пов'язані з виробленням на наднаціональному рівні ЄС єдиної стратегії в області кібербезпеки. Встановлено, що основна проблема ефективного забезпечення кібербезпеки полягає у створенні в ЄС єдиного європейського політичного простору. Значна активність у цій сфері керівних органів ЄС стикається з нездатністю низки країн в повному обсязі виконати всі директиви, розпорядження, регламенти та інші нормативні акти. Через складні процедури узгодження на національному і наднаціональному рівнях, що вимагає значного часу, а також через несформованість в ЄС єдиного політичного простору держави і наднаціональні структури ЄС не завжди встигають вчасно реагувати на появу нових кіберзагроз. Проте, незважаючи на ці проблеми, система забезпечення кібербезпеки в країнах ЄС досить швидко розвивається і вдосконалюється, чому сприяє настільки ж швидке накопичення досвіду регулювання і координації дій країн − членів ЄС у сфері кібербезпеки. За результатами дослідження визначено, що в умовах розробки нашою державою національного законодавства у сфері кібернетичної безпеки (з урахування умов Угоди про асоціацію між Україною та ЄС) для України за умови відповідного корегування може бути корисним досвід ЄС щодо визначення або створення єдиного державного органу з питань кіберзахисту, здатного відповідати на кібератаки, сертифікації цифрових продуктів і послуг, заходи із захисту персональних даних користувачів комп'ютерних мереж, що передбачають значні штрафи за незаконне використання цих даних.

Ключові слова: *кібербезпека, ЄС, загрози, кіберпростір, інформація, дані.*

© ТАРАСЮК А.В. – кандидат юридичних наук, головний науковий співробітник Наукової лабораторії забезпечення інформаційної та кібернетичної безпеки (Науково-дослідний інститут інформатики і права Національної академії правових наук України)

The aim of the article is to analyze the most complex and urgent problems of cybersecurity in EU countries and to formulate a common policy in this area. Common political and economic factors for cybersecurity issues at national, supranational and global levels are considered. The example of Romania and Poland illustrates the emergence of a cyber defense system in Eastern Europe. The example of Germany and Finland shows that cybersecurity policies in a number of developed EU countries are more effective than policies at the supranational pan-European level. It is concluded that the hallmark of the German approach to cybersecurity is its complex and fundamental character, which includes a whole system of regulations, plans and institutions. The main approaches and trends related to the development of a unified EU cyber security strategy have been identified. It is established that the main problem of effective cyber security is to create a single European political space in the EU. Significant activity in this area of EU governing bodies is faced with the inability of a number of countries to fully comply with all directives, regulations, regulations and other regulations. Due to complex coordination procedures at the national and supranational levels, which require considerable time, as well as the lack of a single political space in the EU, EU states and supranational structures do not always have time to respond to the emergence of new cyber threats. However, in spite of these problems, the cybersecurity system in the EU countries is developing and improving quite rapidly, which contributes to the equally rapid accumulation of experience in regulating and coordinating EU member states in the field of cybersecurity. According to the results of the study, it is determined that in the conditions of our country's development of national legislation in the field of cyber security (taking into account the terms of the Association Agreement between Ukraine and the EU) for Ukraine, provided appropriate adjustment, it may be useful for the EU experience to identify or create a single state body for cyber defense capable of responding to cyberattacks, certification of digital products and services, measures to protect the personal data of users of computer networks, which entail significant penalties for illegal use of this data.

Key words: *cybersecurity, EU, threats, cyberspace, information, data.*

Вступ. Сьогодення ставить перед Україною нові виклики та надскладні завдання. Під час опору різноплановим проявам гібридної війни, розгорнутої Російською Федерацією, стало очевидним, що наша держава стикнулася з життєвою необхідністю захисту фундаментальних національних цінностей – незалежності, територіальної цілісності і суверенітету держави, свободи, прав людини й верховенства права, добробуту, миру й безпеки, а також у стислі терміни має забезпечити ефективне функціонування сектору безпеки й оборони в умовах обмежених ресурсів. З огляду на такі міркування вивчення досвіду зарубіжних країн є вельми актуальним для формування відповідної національної політики на сучасному етапі державотворення.

Постановка завдання. Питання забезпечення кібербезпеки хвилюють все світове співтовариство, адже глобальний інформаційний простір нині налічує понад 4,1 млрд користувачів. У кіберпросторі стикаються інтереси держав та їх об'єднань, корпорацій, фінансових груп, політичних партій та рухів, неурядових організацій тощо, а також активно діють різні кримінальні групи (хакери) і міжнародні терористи, здійснюється економічне і військове шпигунство, робляться спроби виведення з ладу об'єктів критичної інфраструктури [1, с. 125−127; 2, с. 2]. Отже, бурхливий розвиток інформаційних технологій і їх використання численними акторами для досягнення своїх політичних, економічних та інших цілей виводить забезпечення кібербезпеки на перший план.

Питання забезпечення кібернетичної безпеки, в тому числі в контексті проблематики забезпечення інформаційної та національної безпеки, досліджувались у працях В. Ліпкана, О. Баранова, Б. Кормича, О. Тронько, В. Бутузова, І. Діордіци, М. Погорецького, І. Сопілки, В. Шеломенцева, К. Макдональда, С. Марліна, С. Фокса, Д. Биго, М. Герке, М. Грокса, М. Дюмонт'є, Ф. Ширера та інших науковців. Водночас досвід забезпечення кібербезпеки у зарубіжних країнах, передусім із точки зору можливостей його використання у вітчизняних реаліях, лишається малодослідженим.

Мета цієї статті – проаналізувати найбільш складні та актуальні проблеми забезпечення кібербезпеки в зарубіжних країнах і формування державної політики у цій сфері.

Результати досліджень. Кібербезпека − досить широке поняття, яке охоплює різні засоби і підходи до забезпечення безпеки в кіберпросторі. Згідно з визначенням Міжнародного

союзу електрозв'язку, кібербезпека становить набір засобів, стратегії і принципи забезпечення безпеки, гарантії безпеки, підходи до управління ризиками, дії і практичний досвід, страхування і технології, які можуть бути використані задля захисту кіберсередовища, ресурсів організації і користувача. Кібербезпека включає заходи захисту і дії, що дають змогу здійснити захист кіберпростору як у цивільній, так і у військовій сфері від загроз, які пов'язані з його взаємозалежними мережами і інформаційною інфраструктурою або можуть завдати їм шкоди [2, с. 133].

Відповідно до зростаючої ролі кіберпростору багато держав створюють власні національні законодавчі норми та стратегії кібербезпеки. Так, нині 27 країн-членів НАТО, Європейський Союз (ЄС), 12 країн Європи, що не є членами НАТО, а також 38 країн з інших частин світу мають власні національні стратегії кібербезпеки [3]. З огляду на євроінтеграційний курс України, особливий інтерес у цьому контексті становить досвід забезпечення кібербезпеки у країнах ЄС.

Водночас варто враховувати, що країни ЄС різняться за рівнем соціально-економічного і технологічного розвитку, рівнем розвитку цифрової економіки та масштабами використання інтернету. У зв'язку з цим у низці країн ЄС національна стратегія з кібербезпеки розроблена недостатньою мірою, незважаючи на вимоги Європейської комісії.

З огляду на показники глобального рейтингу кібербезпеки (враховує показники країни у п'яти сферах: правові норми в області кібербезпеки і їх виконання; технічні заходи і наявність відповідних інструментів для їх реалізації; організаційні заходи у сфері кібербезпеки; розвиток потенціалу кібербезпеки; участь у міжнародному співробітництві щодо її забезпечення [4, с. 30]), найбільш передовими в галузі розробки і застосування національних стратегій кібербезпеки серед країн − членів ЄС є Норвегія, Естонія, ФРН, Австрія, Угорщина, Нідерланди [4, с. 14]. Найменш успішними в плані кібербезпеки серед країн, що входять в ЄС, є Румунія, Болгарія, Бельгія, Португалія, Греція [4, с. 15].

Наприклад, Національна стратегія забезпечення кібербезпеки Румунії, прийнята у 2013 р., передбачає, що Румунія забезпечує функціонування динамічного інформаційного середовища на основі функціональної сумісності й послуг, характерних для інформаційного суспільства, а також відповідність балансу основних прав і свобод громадян та інтересів національної безпеки, збільшення поінформованості щодо ризиків і загроз, пов'язаних із діяльністю, здійснюваною в кіберпросторі, а також способів запобігання та протидії їм. Держава виступає координатором заходів із забезпечення кібербезпеки, які спрямовані на досягнення таких цілей: адаптація законодавства до динаміки розвитку конкретних кіберзагроз; встановлення мінімальних вимог безпеки для національних кіберсистем, що забезпечують правильну роботу критичної інфраструктури та забезпечення її стійкості; усвідомлення й запобігання ризикам кібербезпеки; використання можливостей кіберпростору для просування національних інтересів, цінностей та цілей у кіберпросторі; сприяння та розвиток співробітництва державного і приватного секторів на національному рівні, а також міжнародне співробітництво у сфері кібербезпеки тощо [5].

Забезпечення кібернетичної безпеки Польщі покладається на Агентство внутрішньої безпеки (ABW), яке у 2013 р. розробило стратегію кібербезпеки, а у 2015 р. − Доктрину кібербезпеки Польщі. Під егідою ABW створено урядову команду реагування на комп'ютерні інциденти (CERT) [6], яка здійснює забезпечення і розвиток можливостей органів державного управління щодо захисту від кіберзагроз, передусім від загроз критичній інфраструктурі [7]. З ініціативи ABW також було створено Центр криптології при Міністерстві національної оборони, який здійснює захист інформації, забезпечує кібероборону та проведення наступальних кібероперацій [8].

Особливий інтерес становлять досвід і практика забезпечення кібербезпеки у ФРН. Варто мати на увазі, що економіка Німеччини перебуває в епіцентрі різних кібератак і промислового шпигунства і помітно страждає від них, тому питання кібербезпеки для неї є одним із ключових. Відмінною рисою німецького підходу до забезпечення кібербезпеки є його комплексний і фундаментальний характер. Ще в 2005 р. у ФРН був розроблений і прийнятий «Національний план захисту інформаційної інфраструктури», а в 2007 р. − «План реалізації захисту критичних елементів інфраструктури».

Створене в 1991 р. Федеральне управління з інформаційної безпеки Німеччини (BSI), яке є складовою частиною МВС, є головним органом, відповідальним за національну кібербезпеку ФРН. Цей орган формує політику і план дій в області інформаційної безпеки з метою запобігання, визначення і реагування на інциденти і кризи в цій сфері. BSI, зокрема, випускає попередження та оповіщення про віруси та інші шкідливі програми в IT-продуктах та послугах, дає рекомендації з протидії шкідливим програмам і діям, а також організовує інформаційний обмін із більш ніж 50 000 недержавних організацій, включаючи малий і середній бізнес.

У 2011 р. у ФРН була прийнята нова Федеральна стратегія кібербезпеки [9], орієнтована, насамперед, на захист критично важливих інформаційних структур і на виявлення додаткових можливостей у сфері забезпечення їх безкризового функціонування. Федеральна стратегія передбачає, що: безпека інформаційних технологій забезпечується спільними зусиллями громадянського суспільства і держави, при цьому комплекс інструментів захисту від кіберзагроз постійно розширюється; за допомогою Національного центру кібербезпеки (Nationales Cyber-Abwehrzentrum, NCAZ) відбувається оптимізація оперативного співробітництва між усіма органами державної влади та забезпечується захист від кібератак критично значущих об'єктів національної ІТ-інфраструктури та економіки; координація превентивних заходів і міждисциплінарних підходів у сфері кібербезпеки в державному і приватному секторах покладається на Національну раду кібербезпеки, яка виступає додатковою сполучною ланкою ІТ-управління на федеральному рівні за участю різних міністерств та інших федеральних органів; ефективний контроль за злочинністю в кіберпросторі включає в себе цілий комплекс інститутів за участю підприємців і компетентних правоохоронних органів для розробки відповідних рекомендацій [10, с. 28–29].

У квітні 2017 р. збройні сили ФРН також створили кіберкомандування (Cyber and Information Space Command, CIS), на яке покладається протидія хакерським і шпигунським атакам. Згідно з розробленим Бундесвером планом, до 2021 р. чисельність CIS становитиме 14,5 тис. співробітників.

Стратегія кібербезпеки Австрії визначає, що звичайні напади на Австрію стануть малоймовірними в недалекому майбутньому, натомість актуальними є нові проблеми глобального співтовариства [11]. Зокрема, як загрози в кіберпросторі, так і продуктивне його використання практично не обмежене, тому напади з кіберпростору та зловживання його можливостями становлять безпосередню загрозу безпеці й належному функціонуванню державного апарату, економіки, науки і суспільства. Отже, одним із головних пріоритетів Австрії є реалізація всеосяжної політики кібербезпеки, за якої зовнішня й внутрішня безпека, а також всі аспекти цивільної й військової безпеки тісно пов'язані та взаємозалежні. Забезпечення кібербезпеки здійснюється у проактивному форматі, що передбачає запобігання загрозам кіберпростору або мінімізацію їх впливу, а також базується на співробітництві у сфері забезпечення кібербезпеки на європейському й міжнародному рівні. Центральним органом у сфері забезпечення кібербезпеки є Центр боротьби з кіберзлочинністю (Cyber Crime Competence Center) Федерального міністерства внутрішніх справ Австрії. На нього також покладається здійснення правоохоронної діяльності у сфері кібербезпеки та боротьби з кіберзлочинністю [12].

Фінляндія займає перше місце за рівнем цифрової грамотності у рейтингу країн ЄС, а також друге місце – за показником поширення мережі широкосмужного зв'язку [13]. Стратегія кібербезпеки Фінляндії, затверджена у 2013 р., передбачає, що загрози, які виходять із кіберпростору, стають дедалі серйознішими, адже кібератаки можуть використовуватися як засіб політичного й економічного тиску поряд із військовими засобами, і закладає таке бачення кібербезпеки: Фінляндія може забезпечити свої життєво важливі функції і протистояти кіберзагрозам у всіх ситуаціях; громадяни, органи влади та юридичні особи можуть ефективно використовувати безпечний кіберпростір, що є результатом здійснення заходів кібербезпеки на національному й міжнародному рівнях; держава має бути готова до протидії кіберзагрозам. Розслідування кіберінцидентів у Фінляндії здійснює поліція, натомість організація кіберзахисту покладається на Сили оборони Фінляндії. Військовий кіберзахист включає в себе розвідку, кібератаки та ведення кібервійн, а також «інтелектуальне попередження» загроз [14].

Якщо вести мову про організацію забезпечення кібербезпеки в країнах Європи загалом, варто зауважити, що у 2013 р. була представлена стратегія кібербезпеки ЄС під назвою «Відкритий, безпечний і надійний кіберпростір». Метою цієї стратегії є підвищення стійкості та нарощування потенціалу в області кібербезпеки держав − членів ЄС, включаючи посилення боротьби з кіберзлочинністю, формування ефективної інфраструктури забезпечення інформаційної безпеки, розробку принципів координації міжнародної політики в області кібербезпеки. Серед інших значущих актів, спрямованих на формування єдиної політики ЄС із протидії кіберзагрозам, варто зазначити «Директиву ЄС з кібербезпеки» [15]. Відповідно до цієї директиви, держави-члени ЄС спільно з Європейською Комісією та Європейським агентством із мережевої та інформаційної безпеки (ENISA) мають створити групу взаємодії. Основними функціями цієї групи є обмін інформацією між її учасниками, а також боротьба із загрозами і інцидентами у сфері кібербезпеки. Крім того, директива містить вимогу створити мережу національних груп із метою організації швидкої і ефективної операційної взаємодії й підтримки країн − членів ЄС для вирішення транскордонних інцидентів у кіберпросторі. Ця директива, розроблена Європейською комісією

і схвалена Європарламентом, набула чинності в серпні 2016 р. З цього моменту почався процес імплементації основних положень директиви в національному законодавстві країн − членів ЄС і визначення операторів, які будуть на практиці забезпечувати кібербезпеку в Європі.

Ще одним заходом, покликаним посилити кібербезпеку ЄС, стало запропоноване Європейською комісією в 2017 р. введення сертифікатів для цифрової продукції і цифрових послуг, що випускаються в країнах ЄС. З точки зору Єврокомісії, сертифікація може відігравати вирішальну роль у посиленні безпеки і розвитку єдиного європейського ринку цифрових продуктів і послуг, оскільки сертифікати будуть дійсними на всій території ЄС і зможуть гарантувати відповідність продуктів і послуг вимогам кібербезпеки [9].

Важливим кроком на шляху захисту даних користувачів комп'ютерних мереж також став загальний регламент ЄС про захист даних (General Data Protection Regulation, GDPR), розроблений і схвалений Європейським парламентом ще в 2016 р., який набрав чинності у травні 2018 р. Цей регламент, покликаний регулювати поширення та використання особистих даних громадян країн ЄС, встановлює норми, відповідно до яких користувачі з країн ЄС мають право знати, як саме використовуються їхні персональні дані, які вони надають про себе в комп'ютерних мережах. Нові правила є екстериторіальними і поширюються на операторів, які обробляють персональні дані європейців не тільки в країнах ЄС, а й за його межами [9].

Деякі з перерахованих кроків ЄС у сфері кібербезпеки в разі відповідної адаптації і коригування можуть бути корисними Україні. До числа таких кроків, як видається, належать, наприклад, визначення або створення єдиного державного органу з питань кіберзахисту, здатного відповідати на кібератаки, сертифікація цифрових продуктів і послуг, заходи із захисту персональних даних користувачів комп'ютерних мереж, що передбачають значні штрафи за незаконне використання цих даних.

Висновки. Основна проблема ефективного забезпечення кібербезпеки полягає у створенні в ЄС єдиного європейського політичного простору. Значна активність у цій сфері керівних органів ЄС стикається з нездатністю низки країн у повному обсязі виконати всі директиви, розпорядження, регламенти та інші нормативні акти. Варто також враховувати, що паралельно з реакцією ЄС на актуальні кіберзагрози безперервно з'являються нові загрози кібербезпеки, на які держави і наднаціональні структури ЄС не завжди встигають вчасно реагувати. Переважно це відбувається через складні процедури узгодження на національному і наднаціональному рівнях, що вимагає значного часу, а також через несформованість в ЄС єдиного політичного простору. Проте, незважаючи на ці проблеми, система забезпечення кібербезпеки в країнах ЄС досить швидко розвивається і вдосконалюється, чому сприяє настільки ж швидке накопичення досвіду регулювання і координації дій країн − членів ЄС у сфері кібербезпеки.

В умовах розробки Україною національного законодавства у сфері кібернетичної безпеки (з огляду на умови Угоди про асоціацію між Україною та ЄС [16]) дієвим може виступити врахування досвіду ЄС, перспективних майбутніх планів, програм і проектів, а також участь у спільних європейських проектах із забезпечення кібернетичної безпеки.

Список використаних джерел:

1. Господарик Ю.П., Пашковская М.В. Международная экономическая безопасность. Москва, 2016. 416 с.

2. Schreier F., Weekes B., Winkler T.H. Cybersecurity: The Road Ahead. Geneva Centre for the Democratic Control of Armed Forces (DCAF). DCAF Horizon 2015 Working Paper No. 4. URL: https://dcaf.ch/sites/default/files/publications/documents/Cyber2.pdf (дата звернення 18.12.2019).

3. Камчатний М.В. Історія міжнародно-правового регулювання питань, пов'язаних із застосуванням комп'ютерних технологій. URL: http://oaji.net/pdf.html?n=2016/3229-1477308664.pdf (дата звернення 17.12.2019).

4. Глобальный индекс кибербезопасности и профили по киберблагополучию: отчет. Женева, ABI Research, 2015. 516 с.

5. Romania's Cyber Security Strategy and the National Action Plan on Implementation of the National Cyber Security (2013). URL: https://www.cert.ro/vezi/document/strategia-de-securitate-cibernetica (Accessed 24.09.2017).

6. Countering cyberterrorism. URL: http://msz.gov.pl/en/foreign_policy/security_policy/international_terrorism/countering_cyber_terrorism/&printMode=true (дата звернення 16.12.2019).

7. Ткачук Т.Ю. Забезпечення інформаційної безпеки: досвід окремих країн східної Європи. *Інформація і право*. 2017. № 4 (23). С. 62−72.

8. Доктрина кибезбезопасности Польши. URL: constitutions.ru/?p=11083 (дата звернення 18.12.2019).

9. Пантин В.И., Кардава Н.В. Кибербезопасность: проблемы формирования единой политики в Европейском Союзе. *Вестник Пермского университета. Политология.* 2018. № 3. С. 5−17.

10. Елин В.М. Сравнительный анализ правового обеспечения информационной безопасности в России и за рубежом : монография. Москва, 2016. 168 с.

11. Austrian Security Strategy (2013). URL: https://www.bka.gv.at/DocView.axd?CobId=52251 (дата звернення 18.12.2019).

12. Austrian Cyber Security Strategy (2013). URL: https://www.bka.gv.at/DocView.axd?CobId=50999 (дата звернення 18.12.2019).

13. ENISA Country Reports. URL: http://www.epractice.eu/files/media/media2624.pdf (дата звернення 18.12.2019).

14. Finland's Cyber Security Strategy (2013). URL: http://www.yhteiskunnanturvallisuus.fi/en/materials/doc_download/40-finlandas-cyber-security-strategy (дата звернення 18.12.2019).

15. Haeni R. 2016. Cybersecurity: New EU Directive. Published 20.07.2016. URL: https://news.pwc.ch/28616/cybersecurity-new-eu-directive-published/ (дата звернення 18.12.2019).

16. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони. URL: https://zakon.rada.gov.ua/laws/show/984_011 (дата звернення 18.12.2019).

УДК 342.6
DOI https://doi.org/10.32844/2618-1258.2019.4-2.40

ТРУБА Р.М.

СТРУКТУРА ТА ЕЛЕМЕНТИ АДМІНІСТРАТИВНО-ПРАВОВОГО СТАТУСУ ДЕРЖАВНОГО БЮРО РОЗСЛІДУВАНЬ УКРАЇНИ

У зв'язку із євроінтеграційними процесами в нашій державі актуалізуються питання, пов'язані із удосконаленням механізмів забезпечення прав і свобод людини та створенням ефективного механізму їх захисту. Корупція в Україні є однією із основних сучасних проблем держави, яка заважає її розвитку, тому одним із пріоритетних напрямів державної політики щодо їх захисту стала кардинальна зміна підходів до протидії корупції. Оскільки захист прав і свобод людини і громадянина включає у тому числі й запобігання, виявлення, припинення, розкриття та розслідування злочинів, забезпечення такого захисту потребує створення ефективної та дієвої системи державних органів, які виконують таку діяльність. Для цього в Україні було створене Державне бюро розслідувань – центральний орган виконавчої влади, який здійснює правоохоронну діяльність з метою запобігання, виявлення, припинення, розкриття та розслідування злочинів, віднесених до його компетенції. Створення цього органу вплинуло на удосконалення національного антикорупційного законодавства, також шляхом його створення було реформовано систему правоохоронних органів. Незважаючи на те, що на сьогодні все ще рано робити висновки про ефективність його функціонування, створення Державного бюро розслідувань потребує уваги з боку науковців з метою подальшого удосконалення правового регулювання його діяльності. Дослідження структури та елементів адміністративно-правового статусу Державного бюро розслідувань України дозволить нам встановити компетенцію цього органу, проаналізувати його правовий статус, а також визначити, чим саме цей орган відрізняється від інших правоохоронних

© ТРУБА Р.М. – директор (Державне бюро розслідувань)