Administrative law and process; finance law; information law

УДК 342.9

**Ковалів Мирослав Володимирович**
*кандидат юридичних наук, професор*
*Львівський державний університет внутрішніх справ*
**Kovaliv Myroslav**
*PhD in Law, Professor*
*Lviv State University of Internal Affairs*
*ORCID: 0000-0002-9730-8401*

**Литвин Наталія Анатоліївна**
*доктор юридичних наук, професор,*
*професор кафедри службового та медичного права*
*Навчально-науковий інститут права*
*Київського національного університету імені Тараса Шевченка*
**Lytvyn Nataliia**
*Doctor of Science in Law, Professor,*
*Professor of the Department of Service and Medical Law Scientific and*
*Educational and Scientific Institute of Law of the*
*Taras Shevchenko National University of Kyiv*
*ORCID: 0000-0003-4199-1413*

**Подоляка Анатолій Миколайович**
*доктор юридичних наук, професор,*
*заслужений юрист України*
*Міжрегіональна Академія управління персоналом*
**Podoliaka Anatolii**
*Doctor of Science in Law, Professor,*
*Honored Lawyer of Ukraine*
*Interregional Academy of Personnel Management*
*ORCID: 0000-0001-7486-8302*

**Шопіна Ірина Миколаївна**
*доктор юридичних наук, професор*
*Львівський державний університет внутрішніх справ*
**Shopina Iryna**
*Doctor of Science in Law, Professor*
*Lviv State University of Internal Affairs*
*ORCID: 0000-0003-3334-7548*

# ІНФОРМАЦІЙНА БЕЗПЕКА ВЗАЄМОДІЇ СУБ'ЄКТІВ ДЕМОКРАТИЧНОГО ЦИВІЛЬНОГО КОНТРОЛЮ ЗА ДІЯЛЬНІСТЮ МІНІСТЕРСТВА ОБОРОНИ УКРАЇНИ
# INFORMATION SECURITY OF THE INTERACTION OF SUBJECTS OF DEMOCRATIC CIVIL CONTROL OVER THE ACTIVITIES OF THE MINISTRY OF DEFENSE OF UKRAINE

***Анотація.*** *Метою статті є визначення особливостей інформаційної безпеки взаємодії суб'єктів демократичного цивільного контролю за діяльністю Міністерства оборони України.*

*З'ясовано особливості діяльності Міністерства оборони України як органу публічного адміністрування, що виконує функції органу військового управління. Акцентовано увагу на тому, що внаслідок демілітаризації Міністерство має статус цивільного відомства. Визначено, що наділення Міністерства оборони України правом формування та реалізації напрямів державної оборонної політики детермінує наявність активних контактів з різноманітними суб'єктами, що породжує велику кількість інформаційних ризиків.*

*Систематизовано інформаційні ризики, характерні для взаємодії Міністерства оборони України з суб'єктами демократичного цивільного контролю. По-перше, це ризики, пов'язані з витоком інформації з обмеженим доступом, яка стала відомою суб'єктами контрольної*

*діяльності під час здійснення їх повноважень. По-друге, це соціально-психологічні ризики, пов'язані з розголошенням/оприлюдненням відомостей та даних, які не носять закритого характеру, однак за своїм впливом на суспільну свідомість здатні викликати комплекс деструктивних реакцій. По-третє, це ризики, пов'язані з перевантаженістю систем військового управління за умов ведення бойових дій, що може мати своїми наслідками зниження ефективності функціонування Збройних Сил України та інших військових формувань.*

*Сформульовано визначення інформаційної безпеки взаємодії суб'єктів демократичного цивільного контролю за діяльністю Міністерства оборони України. Зроблено висновок, що основні напрями досліджуваної інформаційної безпеки охоплюють визначення конкретного рівня інформаційних ризиків та вжиття заходів для зменшення їх негативного впливу, удосконалення систем захисту даних в інформаційних мережах, виховання високого рівня інформаційної культури суб'єктів демократичного цивільного контролю над Силами оборони.*

***Ключові слова:*** *демократичний цивільний контроль, взаємодія, Міністерство оборони України, інформаційна безпека, Сили оборони, інформаційні ризики, публічне адміністрування, сектор безпеки і оборони, правовий режим воєнного стану.*

***Summary.*** *The purpose of the article is to determine the features of information security of interaction between subjects of democratic civil control over the activities of the Ministry of Defense of Ukraine.*

*The features of the activities of the Ministry of Defense of Ukraine as a public administration body that performs the functions of a military command body are clarified. Attention is focused on the fact that as a result of demilitarization, the Ministry has the status of a civilian department. Arguments are given that empowering the Ministry of Defense of Ukraine with the right to form and implement the directions of state defense policy determines the*

*presence of active contacts with various subjects, which gives rise to a large number of information risks.*

*The systematization is made by information risks, typical for the interaction of the Ministry of Defense of Ukraine with the subjects of democratic civil control. Firstly, these are the risks associated with the leakage of information with limited access, which became known to the subjects of control activities in the exercise of their powers. Secondly, these are socio-psychological risks associated with the disclosure/publication of information and data that are not of a closed nature; however, due to their influence on public consciousness, they can cause a complex of destructive reactions. Thirdly, these are the risks associated with the overload of military command and control systems in the conditions of combat operations, which may lead to a decrease in the effectiveness of the functioning of the Armed Forces of Ukraine and other military formations.*

*The definition is formulated by the information security of the interaction of subjects of democratic civilian control over the activities of the Ministry of Defense of Ukraine. The conclusion is made that the main directions of the studied information security cover the definition of a specific level of information risks and the adoption of measures to reduce their negative impact, the improvement of data protection systems in information networks, the education of a high level of information culture of subjects of democratic civilian control over the Defense Forces.*

***Key words:*** *democratic civil control, interaction, Ministry of Defense of Ukraine, information security, Defense Forces, information risks, public administration, security and defense sector, legal regime of martial law.*

**Постановка проблеми в загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями**. Проблеми побудови ефективної системи демократичного цивільного контролю над Силами оборони після початку повномасштабної російської збройної

агресії набули нової актуальності. Тривалий характер бойових дій та встановлення правового режиму воєнного стану потребують нині вироблення нових алгоритмів дій у сфері контролю. Особливостями сучасного стану розвитку демократичного цивільного контролю є застосування до багатьох сфер суспільних відносин правових приписів законодавства про воєнний стан. Водночас спостерігається наявність прогалин в інформаційному законодавстві, яке розроблялося з урахуванням тих умов, які складаються у мирний час, і не відповідає повною мірою реаліям сьогодення. При цьому найбільша кількість інформаційних ризиків концентрується у сфері взаємодії між суб'єктами публічного адміністрування сектора безпеки і оборони. Вказане обумовлює актуальність дослідження інформаційної безпеки взаємодії суб'єктів демократичного цивільного контролю за діяльністю Міністерства оборони України.

**Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми.** Проблеми, пов'язані із з'ясуванням сутності інформаційної безпеки, були предметом наукових досліджень таких вчених, як І. Арістова, яка розглянула проблеми інформаційної безпеки в контексті споживання телекомунікаційних послуг, а також в аспекті розвитку інформаційного суспільства та цифрової економіки [1; 2], К. Бєляков, який здійснив аналіз законодавства в секторі інформаційної безпеки з технолого-правових підходів та досліджував вказане питання в контексті процесу інформатизації в нашій державі [3; 4], О. Головко, предметом вивчення якої стала медіабезпека як один із елементів інформаційної безпеки [5], О. Дзьобань та О. Соснін, які вивчали вказану проблематику у розрізі нових вимірів загроз, пов'язаних з інформаційно-комунікаційною сферою [6] О. Довгань, який розглянув забезпечення інформаційної безпеки в контексті глобалізації [7], С. Єсімов, який дослідив особливості удосконалення нормативно-правового регулювання в сфері інформаційної безпеки [8], О. Золотар, яка вивчає проблеми інформаційної безпеки у ракурсі проблем

прав і свобод людини в інформаційному суспільстві, загроз інформаційній безпеці людини, стану правового забезпечення цієї сфери та перспектив його розвитку. [9], Б.Кормич, який вивчав організаціно-правові та політичні аспекти інформаційної безпеки [10], С. Онопрієнко, що розглянув питання інформаційної безпеки в контексті діяльності органів публічного адміністрування під час дії правового режиму воєнного стану [11], Н. Уханова, яка вивчає питання протидії інформаційним впливам та захисту людини і суспільства [12], Ф. Фурашев, який зробив значний внесок у розвиток правової термінології у досліджуваній сфері [13] та ін. Разом з тим інформаційна безпека взаємодії між суб'єктами сектора безпеки і оборони досліджена ще недостатньо, що обумовлює спрямованість наукових пошуків.

**Формулювання цілей статті (постановка завдання).** Метою статті є визначення особливостей інформаційної безпеки взаємодії суб'єктів демократичного цивільного контролю за діяльністю Міністерства оборони України.

**Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів**. Дослідження феномену інформаційної безпеки у роботах українських та зарубіжних науковців включають два основні підходи. Перший з них розглядає інформаційну безпеку як бажаний стан розвитку суспільних відносин, умов та чинників, що складаються у суспільстві, і характеризуються максимальним рівнем захищеності інформаційних прав, свобод та інтересів фізичних та юридичних осіб. Другий підхід розглядає інформаційну безпеку як сукупність активних дій учасників інформаційних правовідносин, вектор руху яких охоплює нівелювання інформаційних загроз та розбудови діючої системи попередження їх деструктивного впливу на суспільні відносини. Обидва підходи, статичний та динамічний, на нашу думку, є цілком обґрунтованими і уявляють собою різні аспекти досліджуваного явища. Разом з тим у межах даної статті ми

розглядаємо інформаційну безпеку у другому аспекті, що обумовлено активним характером взаємодії між суб'єктами демократичного цивільного контролю.

Взаємодія суб'єктів демократичного цивільного контролю лише розпочинає привертати увагу дослідників, разом з тим її важливість в умовах повномасштабної російської агресії постійно зростає. Це обумовлено необхідністю консолідації зусиль всіх органів публічної влади і всіх інститутів громадянського суспільства для перемоги над агресором. Взаємодія як наукова категорія звичайно трактується як сумісна або узгоджена у часі та просторі діяльність певного кола суб'єктів, спрямована на досягнення поставленої мети. Відповідно, взаємодія суб'єктів демократичного цивільного контролю, з урахуванням особливостей їх правового статусу, має розглядатися як узгоджена у часі та просторі діяльність суб'єктів контрольної діяльності, спрямована на пошук випадків порушення правових приписів та ліквідації їх негативного впливу на функціонування сектору безпеки і оборони. До особливостей цієї взаємодії слід віднести наступні: по-перше, немілітарний правовий статус суб'єктів контрольної діяльності; по-друге, зовнішній характер контролю (проведення внутрішньовідомчих контрольних заходів відбувається у системі внутрішньовідомчого контролю, який є іншим різновидом державного або публічного контролю); по-третє, поєднання у межах контрольної діяльності суб'єктів, що належать до різних гілок влади або до громадянського суспільства.

Саме третя особливість взаємодії суб'єктів демократичного цивільного контролю і є, на нашу думку, джерелом великої кількості інформаційних ризиків, обумовлених різнорідністю правових статусів суб'єктів означеного контролю, що знаходить свій прояв у існуванні різноманітних, переважно не узгоджених між собою, систем інформаційної безпеки. Органи законодавчої, виконавчої та судової влади, органи місцевого самоврядування, військові формування та правоохоронні органи,

громадські об'єднання мають власні алгоритми забезпечення інформаційної безпеки, не завжди вербалізовані та стандартизовані. Вказане не означає, що ми є прихильниками повної ідентичності систем інформаційної безпеки – навпаки, саме в їх полівекторності полягає, на наш погляд, оптимальний варіант стабільності загальнодержавної системи інформаційної безпеки. Однак виокремлення інформаційних ризиків, притаманних функціонуванню кожної з означених систем, є, на наш погляд, необхідною умовою забезпечення високого рівня інформаційної безпеки взаємодії суб'єктів демократичного цивільного контролю за діяльністю Міністерства оборони України.

Діяльність Міністерства оборони України має наступні особливості. По-перше, цей орган публічного адміністрування виконує функції органу військового управління, в його підпорядкуванні знаходяться Збройні Сили України, однак внаслідок демілітаризації він має статус цивільного відомства [14]. По-друге, наділення Міністерства оборони України правом формування та реалізації напрямів державної оборонної політики [15] детермінує наявність активних контактів з різноманітними суб'єктами, частина з яких має непідтверджений статус з точки зору можливої небезпеки для сфери оборони, у тому числі в контексті інформаційних правовідносин.

Інформаційно-правовий статус оборонного відомства обумовлений покладенням на нього низки повноважень в означеній сфері, до ских, зокрема, належать наступні: Міністерство оборони України провадить розвідувальну та інформаційно-аналітичну діяльність в інтересах національної безпеки та оборони держави; координує створення та розвиток ефективної системи стратегічних комунікацій у Міноборони та Збройних Силах як складової загальнодержавної системи стратегічних комунікацій, забезпечення її стійкості та адаптивності до реагування на виклики та загрози; бере участь у виконанні завдань державної інформаційної політики у сфері оборони, інформаційних заходах,

спрямованих на підвищення рівня обороноздатності держави та на протидію інформаційним операціям агресора (противника); проводить постійний моніторинг інформаційного середовища, виявляє потенційні та реальні інформаційні загрози в сфері оборони, здійснює відповідні заходи; засновує телерадіоорганізації, засоби масової інформації, офіційні друковані видання та бере участь у їх діяльності; забезпечує впровадження та розвиток новітніх інформаційних технологій у сфері оборони; відповідно до компетенції забезпечує електронну інформаційну взаємодію з органами державної влади під час обміну інформацією для здійснення повноважень, визначених законодавством та ін. [15]. Водночас слід сказати, що в цьому ж правовому документі визначено повноваження та напрями діяльності оборонного відомства у сфері здійснення демократичного цивільного контролю (п.п.80 п.4) та його право та обов'язок здійснювати взаємодію з широким колом різноманітних суб'єктів державного та недержавного сектору (п.7) [15].

Оскільки у правовому статусі Міністерства оборони України поєднуються елементи політичного, правового, військового, воєнного, комунікативного та інформаційного характеру, це породжує велику кількість інформаційних ризиків. Поняття інформаційних ризиків ще недостатньо досліджено у правових джерелах, однак в економічних науках воно вже стало предметом вивчення деяких науковців і розуміється як ризики втрати, несанкціонованої зміни інформації через перебої у функціонуванні інформаційних систем або за їх виходу з ладу, що призводить до втрати інформації. При цьому зауважується, що найбільш широке визначення включає ризик виникнення збитків внаслідок неправильної організації або навмисного порушення інформаційних потоків у системі організації [16]. З цього приводу хотілося б сказати, що у сфері національної безпеки шкода, спричинена суспільним відносинам внаслідок втрати або зміни інформації, може бути меншою, ніж шкода, яка настає внаслідок розголошення певних відомостей та даних. На відміну від

економічних наук, така шкода може носити не лише фінансовий, а й політичний характер, а в окремих випадках – характер небезпеки для життя і здоров'я, честі та гідності громадян України.

Інформаційні ризики, характерні для взаємодії Міністерства оборони України з суб'єктами демократичного цивільного контролю за його діяльністю включають, на нашу думку, три групи.

По-перше, це ризики, пов'язані з витоком інформації з обмеженим доступом, яка стала відомою суб'єктами контрольної діяльності під час здійснення їх повноважень. Такий виток може відбуватися як у процесі проведення контрольних заходів, так і після їх завершення, і здійснюватися внаслідок впливу великої кількості факторів (політичних, правових, технологічних, психологічних тощо). Вказане потребує активної комунікації між оборонним відомством та суб'єктами контрольної діяльності з метою відстеження найбільш вразливих для розголошення відомостей та даних, оприлюднення яких може спричинити значну небезпеку для діяльності військ/сил, а також постійної роз'яснювальної роботи з членами громадських рад при Міністерстві оборони України, інших суб'єктів сектору безпеки та оборони, журналістами, представниками волонтерських організацій тощо.

По-друге, це соціально-психологічні ризики, пов'язані з розголошенням/оприлюдненням відомостей та даних, які не носять закритого характеру, однак за своїм впливом на суспільну свідомість здатні викликати комплекс деструктивних реакцій (депресія, страх, розпач, почуття безпомічності тощо). Наявність вказаної групи ризиків потребує від суб'єктів контрольної діяльності постійного моніторингу етичності поширення певних відомостей та даних, застосування критерію перевищення користі від оприлюднення певної інформації над шкодою, що може бути нанесена при цьому державі Україна та її громадянам.

По-третє, це ризики, пов'язані з перевантаженістю систем військового управління за умов ведення бойових дій, що може мати своїми

наслідками зниження ефективності функціонування Збройних Сил України та інших військових формувань з-за використання обмежених управлінських ресурсів для здійснення несуттєвих (некорисних, другорядних) контрольних заходів, проведення яких за умов правового режиму воєнного стану не може бути визнано доцільним.

**Висновки з даного дослідження і перспективи подальших розвідок у даному напрямку.** Інформаційна безпека взаємодії суб'єктів демократичного цивільного контролю за діяльністю Міністерства оборони України – це сукупність дій посадових осіб органів публічної влади, військових формувань та правоохоронних органів, громадських об'єднань та інших суб'єктів, спрямована на нівелювання інформаційних ризиків у діяльності суб'єктів контрольної діяльності щодо пошуку випадків порушення правових приписів та ліквідації їх негативного впливу на функціонування оборонного відомства. Її основні напрями охоплюють визначення конкретного рівня інформаційних ризиків та вжиття заходів для зменшення їх негативного впливу, удосконалення систем захисту даних в інформаційних мережах, виховання високого рівня інформаційної культури суб'єктів демократичного цивільного контролю над Силами оборони.

Напрямами подальших наукових досліджень мають стати визначення змісту форм та методів забезпечення інформаційної безпеки під час здійснення демократичного цивільного контролю.

## Література

1. Арістова В. І., Сулацький Д. В. Інформаційна безпека людини як споживача телекомунікаційних послуг. Київ : Право України, 2013. 184 с.
2. Арістова І.В. Система права України в умовах інформаційного суспільства та цифрової економіки. *Приватне та публічне право*. 2020. № 3. С. 44-51.

3. Бєляков К.І. Законодавство в секторі інформаційної безпеки: технолого-правовий аналіз. *Актуальні проблеми управління інформаційною безпекою держави* : зб. тез наук. доп. наук.-практ. конф. (Київ, 30 березня 2018 р.) Київ, 2018. С. 15-16.
4. Бєляков К.І. Інформатизація в Україні: проблеми організаційного, правового та наукового забезпечення : монографія. Київ : КВІЦ, 2008. 576 с.
5. Головко О. М. Медіабезпека людини: засади інформаційно-правової політики : Монографія. Київ : Видавничий дім «АртЕк». 2019. 168 с.
6. Дзьобань О. П., Соснін О. В. Інформаційна безпека: нові виміри загроз, пов'язаних з інформаційно-комунікаційною сферою. *Гуманітарний вісник*. 2015. № 60. С. 24–34.
7. Довгань О. Д. Забезпечення інформаційної безпеки в контексті глобалізації: теоретико-правові та організаційні аспекти. Київ, 2015. 386 с.
8. Єсімов С. С. Шляхи удосконалення нормативно-правового регулювання в сфері інформаційної безпеки. *Наукові записки Львівського університету бізнесу та права*. 2013. Вип. 11. С. 73-76.
9. Золотар О. О. Інформаційна безпека людини: теорія і практика : монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 446 с
10. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України : Монографія. Одеса : Юридична література, 2003. 472 с.
11. Онопрієнко С. Функції забезпечення інформаційної безпеки публічного адміністрування в Україні за умов повномасштабної збройної агресії Російської Федерації. *Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки*. 2022. №2. С. 95-98.

12. Уханова Н. С. Проблеми протидії негативним інформаційним впливам та захисту інформаційної безпеки людини і суспільства : монографія / за заг. ред. В. Пилипчука. Київ-Одеса : Фенікс, 2022. 120 с.
13. Фурашев Ф. Сутність та визначення понять «інформаційна безпека» і «безпека інформації». *Інформація і право*. 2012. №2 (34). С. 51-59.
14. Koropatnik I., Karelin V., Boikov A., Shopina I., Khrystynchenko N. Activities of the Ministry of Defense in Ukraine and Military Administration during the Special Period. *Journal of Legal, Ethical and Regulatory Issues.* 2020. № 23(1). P. 1–6. URL: http://dspace.lvduvs.edu.ua/bitstream/1234567890/4857/1/scopus%20Activities-of-the-ministry-of-defense-in-Ukraine.pdf
15. Положення про Міністерство оборони України: затверджено постановою Кабінету Міністрів України від 26 листопада 2014 р. № 671. URL: https://zakon.rada.gov.ua/laws/show/671-2014-%D0%BF#Text.
16. Бондар О.С. Інформаційні ризики банків: аналіз і кількісна оцінка. *Вісник Білоцерківського державного аграрного університету.* 2008. Вип. 55. С. 79-83.

## References

1. Aristova, V. I., Sulatskyi, D. V. (2013). Informatsiina bezpeka liudyny yak spozhyvacha telekomunikatsiinykh posluh. Kyiv, 184. [in Ukrainian].
2. Aristova, I.V. (2020). Systema prava Ukrainy v umovakh informatsiinoho suspilstva ta tsyfrovoi ekonomiky. *Pryvatne ta publichne pravo,* № 3, 44-51. [in Ukrainian].
3. Bieliakov, K.I. (2018). Zakonodavstvo v sektori informatsiinoi bezpeky: tekhnoloho-pravovyi analiz. Aktualni problemy upravlinnia informatsiinoiu bezpekoiu derzhavy, Kyiv, 15-16. [in Ukrainian].
4. Bieliakov, K.I. (2008). Informatyzatsiia v Ukraini: problemy orhanizatsiinoho, pravovoho ta naukovoho zabezpechennia: monohrafiia. Kyiv, 576. [in Ukrainian].

5. Holovko, O. M. (2019). Mediabezpeka liudyny: zasady informatsiino-pravovoi polityky: Monohrafiia. Kyiv, 168. [in Ukrainian].
6. Dzoban, O. P., Sosnin, O. V. (2015). Informatsiina bezpeka: novi vymiry zahroz, poviazanykh z informatsiino-komunikatsiinoiu sferoiu. *Humanitarnyi visnyk,* № 60, 24–34. [in Ukrainian].
7. Dovhan, O. D. (2015). Zabezpechennia informatsiinoi bezpeky v konteksti hlobalizatsii: teoretyko-pravovi ta orhanizatsiini aspekty. Kyiv, 386. [in Ukrainian].
8. Yesimov, S. S. (2013). Shliakhy udoskonalennia normatyvno-pravovoho rehuliuvannia v sferi informatsiinoi bezpeky. *Naukovi zapysky Lvivskoho universytetu biznesu ta prava,* V. 11, 73-76. [in Ukrainian].
9. Zolotar, O. O. (2018). Informatsiina bezpeka liudyny: teoriia i praktyka : monohrafiia. Kyiv, 446. [in Ukrainian].
10. Kormych, B.A. (2003). Orhanizatsiino-pravovi zasady polityky informatsii noi bezpeky Ukrainy: Monohrafiia. Odesa, 472. [in Ukrainian].
11. Onopriienko, S. (2022). Funktsii zabezpechennia informatsiinoi bezpeky publichnoho administruvannia v Ukraini za umov povnomasshtabnoi zbroinoi ahresii Rosiiskoi Federatsii. Visnyk Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. Viiskovo-spetsialni nauky, №2, 95-98. [in Ukrainian].
12. Ukhanova, N. S. (2022). Problemy protydii nehatyvnym informatsiinym vplyvam ta zakhystu informatsiinoi bezpeky liudyny i suspilstva: monohrafiia. Kyiv-Odesa, 120. [in Ukrainian].
13. Furashev, F. (2012). Sutnist ta vyznachennia poniat «informatsiina bezpeka» i «bezpeka informatsii». *Informatsiia i pravo*, №2 (34), 51-59. [in Ukrainian].
14. Koropatnik, I., Karelin, V., Boikov, A., Shopina, I., Khrystynchenko, N. (2020). Activities of the Ministry of Defense in Ukraine and Military Administration during the Special Period. *Journal of Legal, Ethical and Regulatory Issues,* 23 (1), 1–6. URL:

http://dspace.lvduvs.edu.ua/bitstream/1234567890/4857/1/scopus%20Activities-of-the-ministry-of-defense-in-Ukraine.pdf [in English].

15. Polozhennia pro Ministerstvo oborony Ukrainy: zatverdzheno postanovoiu Kabinetu Ministriv Ukrainy vid 26 lystopada 2014. № 671. URL: https://zakon.rada.gov.ua/laws/show/671-2014-%D0%BF#Text [in Ukrainian].
16. Bondar, O.S. (2008). Informatsiini ryzyky bankiv: analiz i kilkisna otsinka. *Visnyk Bilotserkivskoho derzhavnoho ahrarnoho universytetu,* V. 55, 79-83. [in Ukrainian].