http://dx.doi.org/10.5281/zenodo.3551285

**О. Л. Хитра,**
*кандидат юридичних наук,*
*доцент кафедри адміністративного права та*
*адміністративного процесу*
*Львівського державного університету*
*внутрішніх справ*
*https://orcid.org/0000-0002-3632-5101*

# ІНФОРМАЦІЙНО – ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ РЕАГУВАННЯ НА КРИЗОВІ СИТУАЦІЇ ЩО ЗАГРОЖУЮТЬ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ

**JEL Classification: K 19**
**SECTION "LAW": Право.**

**Анотація. У статті на підставі теорії та практики проаналізовано основні засади формування та реалізації державної інформаційної політики, яка визначає діяльність органів державної влади в сфері забезпечення реагування на кризові ситуації, що загрожують національній безпеці.**

**Окреслено, що дослідження інформаційної безпеки як конструктивно інтегрованої складової реагування на кризові ситуації, що загрожують національній безпеці України, доводить, що її чинниками системоутворення складаються з інформації, інформаційних процесів та інформаційно-технологічного забезпечення.**

**Доведено, що значне зростання ролі інформаційної безпеки в процесі налагодження суспільних відносин, а також активізація використання сучасних інформаційних технологій істотно впливають як на діяльність державного апарату загалом, так і на роботу систем сил безпеки та сил оборони зокрема, що значно знижує рівень реагування на кризові ситуації, що загрожують національній безпеці України, а також може перетворитися на джерело серйозних загроз розвитку держави.**

**В статті вказується на кіберзлочинність, яка як небезпечне явище у сфері інформаційно-правового реагування на кризові ситуації, що загрожує національній безпеці, виступає на сьогодні найпотужнішою загрозою у інформаційному просторі.**

**Враховуючи досить розповсюджену практику звернення пересічних громадян із запитами до органів державної влади щодо надання різного роду публічної інформації, запропоновано новації щодо активного залучення до сфери формування переліку інформації широкого кола представників громадськості як гаранта відповідного ступеня демократизму і відносної прозорості процесу розкриття таємності відомостей, а також запровадження досить прозорої процедури оскарження відмови в доступі до такої інформації.**

***Ключові слова:*** **національна безпека, криза, інформаційна безпека, кризова ситуація, що загрожує національній безпеці, реагування на кризову ситуацію, кіберзлочинність, кібертероризм.**

**Annotation. On the basis of theory and practice, the article analyzes the basic principles of formation and implementation of state information policy, which defines the activity of public authorities in the field of crisis response that threatens national security.**

**It is emphasized that the study of information security as a constructively integrated component of crisis response that threatens the national security of Ukraine, proves that its factors of system formation consist of information, information processes and information technology support.**

**It is proved that a significant increase in the role of information security in the process of establishing public relations, as well as the intensification of the use of modern information technologies, significantly affect both the activity of the state apparatus in general and the work of the security and defense forces in particular, which significantly reduces the level of crisis response. that threaten Ukraine's national security and could also become a source of serious threats to the country's development.**

**Now it is necessary to develop a new, holistic, scientifically sound system of guaranteeing information security, which should operate not only at the national level, but also to ensure the functioning of corporate organizations, individual legal entities and law enforcement agencies.**

**The article points to cybercrime, which, as a dangerous phenomenon in the field of information and legal response to crisis situations that threaten national security, is by far the most powerful threat in the information space. In this regard, given the lack of professional training of police officers in counteracting cyberterrorism, based on foreign experience of police practice, it is indicated that it is important to be aware in the system of educational institutions of the Ministry of Internal Affairs of Ukraine, in the system of educational institutions of the Ministry of Internal Affairs professional profiling of "information technologies".**

**Given the widespread practice of requesting ordinary citizens to request public authorities to provide various types of public information, innovations have been proposed to actively involve in the field of listing a wide range of members of the public as a guarantor of an adequate degree of democracy and relative transparency and transparency a sufficiently transparent procedure for challenging the denial of access to such information.**

***Keywords:*** **national security, crisis, information security, crisis situation threatening national security, crisis response, cybercrime, cyberterrorism.**

**Вступ**

**Постановка проблеми**

На сьогодні важко уявити особу, відірваної від інформаційних процесів, які позитивно чи негативно впливають на політичний, економічний і, в першу чергу, соціальний розвиток людського суспільства. І не даремно, зважаючи на ці проблеми, українська демократична правова держава, спираючись на Окінавську хартію глобального інформаційного суспільства (Окінава, 22 липня 2000 року) інші міжнародні нормативно-правові акти, Закони Україна, застосовуючи сучасну інформаційну технологію, з метою подолання кризових ситуацій, які суттєво вразливі від зовнішніх та внутрішніх викликів, повинна всіма доступними формами та методами зміцнювати основи інформаційної безпеки.

*Стан дослідження.* Актуальність проблем інформаційно – правового забезпечення реагування на кризові ситуації що загрожують національній безпеці України, особливо за останні п'ять років, постійно привертають до себе увагу теоретиків та практиків інформаційного права. Разом з тим, аналіз останніх публікацій сучасних авторів свідчить, що більшість їх зусиль спрямовано на розбудову системи логістичного забезпечення інформаційної безпеки окремих військових формувань та правоохоронних органів, проте комплексне інформаційно – правове забезпечення реагування саме на кризові ситуації що загрожують національній безпеці України досліджувалися не на достатньому рівні.

*Мета статті.* На основі аналізу положень чинного законодавства визначити стан та шляхи удосконалення інформаційно – правового забезпечення реагування на кризові ситуації що загрожують національній безпеці України.

**Результати дослідження**

Визначаючи провідну роль інформації, яку вона відіграє у розвитку суспільства, в статті 17 Основного закону України вказується, що забезпечення інформаційної безпеки є найважливішою функцією держави, справою всього Українського народу [1].

Відповідно до статті 107 Конституції України, Указу Президента України від 25 лютого 2017 року № 47/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України», пріоритетами державної політики в сфері інформаційної безпеки мають бути:

- створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них;
- удосконалення повноважень державних регуляторних органів, які здійснюють діяльність щодо інформаційного простору держави, з метою досягнення адекватного рівня спроможності держави відповідати реальним та потенційним загрозам національним інтересам України в інформаційній сфері;
- законодавче врегулювання механізму виявлення, фіксації, блокування та видалення з інформаційного простору держави, зокрема з українського сегмента мережі Інтернет, інформації, яка загрожує життю, здоров'ю громадян України, пропагує війну, національну та релігійну ворожнечу, зміну конституційного ладу насильницьким шляхом або порушення територіальної цілісності України, загрожує державному суверенітету, пропагує комуністичний та/або націонал-соціалістичний (нацистський) тоталітарні режими та їхню символіку;

- визначення механізмів регулювання роботи підприємств телекомунікацій, поліграфічних підприємств, видавництв, телерадіоорганізацій, телерадіоцентрів та інших підприємств, установ, організацій, закладів культури та засобів масової інформації, а також використання місцевих радіостанцій, телевізійних центрів та друкарень для військових потреб і проведення роз'яснювальної роботи серед військ та населення; заборони роботи приймально-передавальних радіостанцій особистого та колективного користування і передачі інформації через комп'ютерні мережі в умовах запровадження правового режиму воєнного стану;
- оптимізація законодавчих механізмів реалізації зобов'язань України в межах Європейської конвенції про транскордонне телебачення щодо держав, які не є підписантами зазначеної Конвенції;
- створення і розвиток структур, що відповідають за інформаційно-психологічну безпеку, насамперед у Збройних Силах України, з урахуванням практики держав – членів НАТО;
- розвиток і захист технологічної інфраструктури забезпечення інформаційної безпеки України;
- забезпечення повного покриття території України цифровим мовленням, насамперед у прикордонних районах, а також тимчасово окупованих територій;
- розвиток цифрового мовлення, унеможливлення впливу на його інфраструктуру суб'єктів, що пов'язані з державою-агресором;
- побудова дієвої та ефективної системи стратегічних комунікацій;
- розвиток механізмів взаємодії держави та інститутів громадянського суспільства щодо протидії інформаційній агресії проти України [2].

Дослідження та значення інформаційної безпеки у сучасному її розвитку, захист стратегічних, урядових та кризових комунікації, особливої уваги та актуальності набуває у період агресії Російської Федерації у Східних областях України із застосуванням технологій гібридної війни, яка перетворила інформаційну сферу на ключову арену протидії.

З метою визначення інноваційних підходів до формування системи захисту і розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації, комплексної протидії кризовим ситуаціям і актуальним загрозам національній безпеці в інформаційній сфері, 25 лютого 2017 року було видано Указ Президента України від №47/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України», в якому уточнено засади формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни. Вказана Доктрина базується на принципах додержання прав і свобод людини і громадянина, поваги до гідності особи, захисту її законних інтересів, а також законних інтересів суспільства та держави, забезпечення суверенітету і територіальної цілісності України [2].

Безперечно, Доктрина інформаційної безпеки України як і деякі інші державні програми не позбавлена критики, і ми цілком з цим погоджуємось, яка зводяться до браку «конкретики», відсутності дієвих механізмів інформаційної взаємодії між владою, ЗМІ та суспільством, сумнівності у її змісті форм реалізації, а саме, які положення повинні виконуватись і хто конкретно буде відповідати за їх невиконання, а також побоювання правозахисників та експертів утисків свободи слова в Інтернеті та інших засобах масової інформації. Крім того, за словами колишнього виконавчого директора Української Гельсінської спілки з прав людини В. Яворського, Доктрина закладає державну систему постійного моніторингу веб-ресурсів, а це, на його думку, передбачає встановлення цензурованих шлюзів, які відокремлять український інтернет від світу [3].

Дослідження інформаційної безпеки як конструктивно інтегрованої складової реагування на кризові ситуації, що загрожують національній безпеці України, доводить, що її чинники системоутворення складаються з інформації, інформаційних процесів та інформаційно-технологічного забезпечення. Проте аналіз зарубіжного досвіду забезпечення інформаційної безпеки вказує, що її система спирається на цілісність, доступність та конфіденційність інформації [4; 5]. Не вдаючись до їх загальної характеристики, нас більше також цікавити сутність конфіденційності інформації. Як відомо, враховуючи тлумачення ст. 21 Закону України «Про інформацію», що конфіденційна інформація є інформацією з обмеженим доступом, до якої належить службова та таємна інформація, сьогодні фізичні та юридичні особи в інформаційному полі стикаються із масою проблем, пов'язаних з перешкодами до інформації з обмеженим доступом. Причина цього неврегульованого процесу полягає у застарілості вказаних занадто «утаємлених» документів, витоки якої вже подавно не загрожують існуючим національним інтересам та цінностям.

До вказаних елементів системи інформаційної безпеки сучасні науковці крім інформаційно-психологічних та державно-ідеологічних [6, с. 62; 99] також відносять фінансовий; військовий; нормативно-правовий; соціальний; економічний; екологічний та інші аспекти [7].

На думку Б. Кормича, інформаційна безпека має суб'єктно-об'єктний склад, відтак з точки зору критерію основного об'єкта складовими інформаційної безпеки є інформаційна безпека особи, інформаційна безпека суспільства та інформаційна безпека держави. Крім того, держава, людина та громадськість

одночасно виступають і в якості суб'єктів інформаційної безпеки, своїми діями здійснюють захист важливої для них інформації та інформаційних процесів. Зокрема, до сфери інформаційної безпеки держави віднесені конкретні дії щодо забезпечення безпечних умов існуючих інформаційних процесів та забезпечення безпечного розвитку таких процесів у майбутньому, що охоплює регулювання питань захисту самої інформації, захисту інформаційної інфраструктури держави, захисту інформаційного ринку та створення безпечних умов розвитку інформаційних процесів [8, с. 30].

Крім того, одним з основних чинників, що обумовлюють ускладнення виконання законодавства у сфері інформації, є неналежне ставлення керівництва органів державної влади, місцевого самоврядування, підприємств, установ, організацій до здійснення контролю за забезпеченням охорони службової інформації, на підпорядкованих суб'єктах господарювання, а також недбале виконання службових обов'язків посадовими особами, відповідальними за охорону інформації з обмеженим доступом.

Отже, при розгляді питання про службову інформацію в контексті законодавства про доступ до інформації було виявлено декілька істотних проблем законодавчого регулювання, які, відповідно, істотно гальмують процес реагування на кризові ситуації, що загрожують національній безпеці.

З цього приводу, слід відмітити той факт, що хоча в Україні і було створено сприятливе законодавче поле, актуальними залишаються питання відкритості доступу до публічної інформації. Наприклад, у статті «Службові квартири у Вінниці роздають тільки «обраним» [9], на запитання журналістів Вінницькому міськвиконкому: чому одним дістаються службові квартири, а інші десятиліттями стоять у черзі, було проінформовано, що комунальну нерухомість міськвиконком активно роздає, але жорсткої звітності за це громаді не надається. Крім того, повідомили, що надання інформації щодо виділення службового житла у Вінниці за період з 2009 по 2011 роки взагалі є неможливою, оскільки 30 березня 2012 року було ліквідовано відділ з обліку та розподілу житла міської ради з вивільненням працівників з займаних посад. І даний облік не вівся. З надісланого журналістами повторного інформаційного запиту вдалось отримати копії витягів з рішень виконавчого комітету вінницької міської ради про надання службових квартир за 2012-2014 роки. У копіях є адреси але немає прізвищ отримувачів, міськвиконком послався на захист персональних даних. Хоча, за словами медіа-юриста О. Бурмагіна, цю інформацію не можна приховувати від громадськості. Проте, у ч. 5 ст.6 Закону України «Про доступ до публічної інформації» вказується, що «Не може бути обмежено доступ до інформації про розпорядження бюджетними коштами, володіння, користування чи розпорядження державним, комунальним майном, у тому числі до копій відповідних документів, умови отримання цих коштів чи майна, прізвища, імена, по батькові фізичних осіб та найменування юридичних осіб, які отримали ці кошти або майно». А відповідно до ч.3 ст.5 Закону України «Про захист персональних даних» не відноситься до інформації з обмеженим доступом інформація про отримання в будь-якій формі фізичною особою бюджетних коштів, державного чи комунального майна, крім випадків, передбачених статтею 6 Закону України «Про доступ до публічної інформації». Більш того, вказаний непоодинокий приклад свавільної діяльності органів державної влади, який трапляється на сьогодні повсякденно, вказує на порушення норм інформаційного законодавство і, в першу чергу, вимог Указу Президента України від 25.11.2017 №47/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»« щодо відкритості та прозорості держави перед громадянами в інформуванні громадян України про діяльність органів державної влади, налагодження ефективної співпраці зазначених органів із засобами масової інформації та журналістами [10].

Таким чином, враховуючи досить розповсюджену практику звернення пересічних громадян із запитами до органів державної влади щодо надання різного роду публічної інформації, нами запропоновано такі новації: по-перше, оскільки в роботі комісій з інформації, відповідальних за формування переліку інформації, що становить службову інформацію, беруть участь представники громадськості, це гарантує відповідну ступінь демократизму і відносної прозорості процесу розкриття таємності відомостей; по-друге, в законодавстві слід запровадити досить прозорі процедури оскарження відмови в доступі до такої інформації; по-третє, необхідно встановити не лише змістовні види інформації, які не можуть бути віднесені до службової інформації, але також види інформації, які можуть і відноситись до неї. Останній момент особливо важливо підкреслити, оскільки він найхарактерніше демонструє загальне концептуальне орієнтування законодавства в питанні про розкриття інформації. У розвинених зарубіжних державах законодавством про доступ до інформації визначається змістовний сектор інформаційного масиву, доступ до якого може бути обмежений, а уся решта інформаційного поля для громадян принципово відкрита. При цьому питання про виключення в наданні інформації вирішується в спеціалізованих законах про свободу інформації комплексно, а не тільки лише стосовно службової чи будь-якої іншої інформації з обмеженим доступом.

Значне зростання ролі інформаційної безпеки в процесі налагодження суспільних відносин, а також активізація використання сучасних інформаційних технологій істотно впливають як на діяльність державного апарату загалом, так і на роботу систем сил безпеки та сил оборони зокрема, що значно знижує рівень реагування

на кризові ситуації, що загрожують національній безпеці України. Адже інформатизація може не тільки завдати прямих збитків конкретній особі в разі несанкціонованого доступу до її даних, їхнього використання, модифікації або знищення, а й перетворитися на джерело серйозних загроз розвитку держави [11].

Нині постає необхідність у формуванні нової, цілісної, науково обгрунтованої системи гарантування інформаційної безпеки, котра має діяти не тільки на загальнодержавному рівні, а й забезпечувати функціонування корпоративних організацій, окремих юридичних осіб та правоохоронних органів. Протягом останніх років в Україні мали місце неодноразові спроби реалізації комплексу заходів, спрямованих на вдосконалення механізмів гарантування інформаційної безпеки. Однак, як свідчать статистичні дані, їхнє впровадження не ліквідувало загроз інформаційній безпеці (зокрема, й на рівні правоохоронних органів), тому її система потребує нагального перегляду та вдосконалення. Ці процеси безпосередньо пов'язані з переглядом чинної політики держави щодо гарантування інформаційної безпеки і, відтак, з докорінним реформуванням її системи [11].

З цього приводу Д.О. Красіков стверджує, що забезпечення інформаційної безпеки повинно здійснюватися за двома формами:

- організаційною (організація роботи, пов'язаної з обігом, збиранням, обробкою, зберіганням та використанням інформації, взаємодія щодо забезпечення інформаційної безпеки);
- правовою (видання наказів та розпоряджень, розроблення положень, інструкцій, складання планів тощо) [12, с. 11–15].

До аналізу правового змісту інформаційно-правового реагування на кризові ситуації, що загрожують національній безпеці спонукає поточний стан суспільно-політичного життя держави. Наявні в інформаційній сфері України суспільні відносини підпадають під дію положень понад чотирьох тисяч нормативно-правових актів різної юридичної сили, що актуалізує проблему узгодження регулятивних та охоронних норм, якими визначаються правові основи інформаційної діяльності, наслідки порушення встановлених щодо неї обмежень, заборон [13].

Основними нормативно-правовими актами, які спрямовані на правове забезпечення належного стану інформаційно-правового реагування на кризові ситуації, що загрожують національній безпеці є закони України «Про доступ до публічної інформації», «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 09.01.2007 № 537-V, «Про телекомунікації» від 18.11. 2003 № 1280-IV, «Про захист інформації в інформаційно-телекомунікаційних системах», «Про національну безпеку України», «Про Національну поліцію», Указ Президента України від 25 лютого 2017 року № 47/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про доктрину інформаційної безпеки України», та деякі інші нормативно-правові акти.

Важлива роль у виконанні національної інформаційної безпеки надана Міністерству внутрішніх справ України. Так, відповідно до покладених на нього завдань, МВС України «забезпечує в межах повноважень, передбачених законом, захист інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом» [14].

Особливо небезпечним явищем у сфері інформаційно-правового реагування на кризові ситуації, що загрожують національній безпеці виступає кіберзлочинність, яка на сьогодні є найпотужнішою загрозою у інформаційному просторі. З метою убезпечення цього злочину було прийнято Закон України від 05.10.2017 № 2163-VIII «Про основні засади забезпечення кібербезпеки України». Цей Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Поява терміну «кіберзлочини» пов'язують з розширенням технічної бази інформатизації. Зокрема, Т.Л. Тропина пропонує визначати кіберзлочини як «винне досконале суспільно небезпечне кримінально каране втручання в роботу комп'ютерів, комп'ютерних програм, комп'ютерних мереж, несанкціоноване модифікація комп'ютерних даних, а також інші протиправні суспільно небезпечні діяння, вчинені за допомогою або за допомогою комп'ютерів, комп'ютерних мереж і програм, а також за допомогою або за допомогою інших пристроїв доступу до модельованого за допомогою комп'ютера інформаційного простору» [15, с. 38].

Важливим в усвідомленні сутності кібертероризму, боротьбі з ним є підготовка в системі навчальних закладів Міністерства внутрішніх справ України відповідного кадрового потенціалу, з фаховою профілізацією «інформаційні технології». Також вказуючи на недостатній рівень професійної підготовки працівників поліції у протидії кібертероризму, повчальним для їх діяльності буде зарубіжної досвід поліцейської практики, який вимагає активізації роботи з уніфікації національного законодавства відповідно норм міжнародних договорів на прикладі діяльність Євроюсту, Європолу (англ. Europol Liaison Officer, ELO) та поліцейської служби Європейського Союзу [16].

**Висновки**

Основними завданнями поліцейської служби, на підставі здійснення інформаційно-пошукової та інформаційно-аналітичної роботи, є координація роботи у протидії міжнародній організованій злочинності і поліпшення інформаційного обміну між національними поліцейськими службами та з іншими органами державної влади України, органами правопорядку іноземних держав та міжнародними організаціями, яка повинна бути спрямована на:

- усунення загроз життю та здоров'ю фізичних осіб і публічній безпеці, що виникли внаслідок учинення кримінального, адміністративного правопорушення;
- підвищення доступності інформації;
- розшук підозрюваних, обвинувачених (підсудних) осіб, які ухиляються від відбування покарання або вироку суду;
- протидію фінансування тероризму, включаючи використання в цих цілях некомерційних організацій;
- надання технічного сприяння третім країнам.

Таким чином, інформаційно-правове реагування на кризові ситуації, що загрожують національній безпеці України повинно віддзеркалювати стан:

- захищеності прав та інтересів громадян, держави та суспільства;
- діяльності систем сил безпеки, оборони та правоохорони;
- протидії кіберзлочинності, з метою несанкціонованого втручання в роботу комп'ютерів, комп'ютерних програм та комп'ютерних мереж;
- не допущення свавілля держаних чиновників в процесі реалізації нормативно-правових актів в інформаційній сфері.

**Список використаних джерел**


1. Конституція України від 28.06.1996 № 254/96 ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.
2. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25.02.2017 № 47/2017. URL: https://www.president.gov.ua/documents/472017-21374.
3. Доктрина інформаційної безпеки України – це лише декларація – експерти. URL: https://www.radiosvoboda.org/a/28336852.html.
4. Michael Nieles, Kelley Dempsey, Victoria Yan Pillitteri. An Introduction to Information Security: Available at. URL: https://doi.org/10.6028/NIST.SP.800-12r1.
5. National Security Telecommunications and Information Systems Security. National Training Standard for Information Systems Security (Infosec): Available at. URL: www.cnss.gov/Assets/pdf/nstissi_4011.pdf.
6. Баришполец В.А. Информационно-психологическая безопасность: основные положения. *Информационные технологии*. 2013. № 2. Т. 5. С. 62.
7. Жатканбаева А. Е. Функциональные компоненты информационной безопасности. *Право и государство*. 2013. № 4 (61). С. 74.
8. Кормич Б. А. Організаційно-правові засади політики інформаційної безпеки України: монографія. Одеса: *Юридична література*. 2003. С. 28–32.
9. Службові квартири у Вінниці роздають тільки «обраним». URL: https://vn.20minut.ua/Podii/sluzhbovi-kvartiri-u-vinnitsi-rozdayut-tilki-obranim-1043 9067.html.
10. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25.02.2017 № 47/2017. URL: https://www.president.gov.ua/documents/472017-21374.
11. Субот А. Інформаційна безпека діяльності працівників правоохоронних органів. URL: http://veche.kiev.ua/journal/4459/.
12. Красіков Д. О. Правове забезпечення інформаційної безпеки в діяльності органів внутрішніх справ України: автореф. дис. ... канд. юрид. наук: 12.00.07. К., 2012. 20 с.
13. Питання забезпечення органами виконавчої влади доступу до публічної інформації: Указ Президента України від 05.05.2011 № 547/2011. *Урядовий кур'єр*. 2011. № 84.
14. Про затвердження Положення про Міністерство внутрішніх справ України: Постанова Кабінету Міністрів України від 28.10.2015 № 878. URL: http://zakon.rada.gov.ua/laws/show/878-2015-п.
15. Тропина Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: дисс. ... канд. юрид. наук: 12.00.08. Владивосток. 2005. 235 с.
16. Комісаров О., Хитра О. Модель інформаційно-комунікативного впливу суб'єктів забезпечення національної безпеки на джерело загроз. *Traektoriâ nauki = Path of Science, Section «law»*. 2019. Vol. 5. № 1. P. 3001–3011.