

Scientific and technical journal «Technogenic and Ecological Safety»

RESEARCH ARTICLE
OPEN ACCESS

ФОРМАЛІЗАЦІЯ ОЦІНКИ ТА УПРАВЛІННЯ СТАНОМ БЕЗПЕКИ

Б. Б. Бандурян¹, В. В. Ковалевський², Д. Л. Цвайгов²¹Інститут електрофізики і радіаційних технологій Національної академії наук України, Харків, Україна²ГО «Національна асоціація кібербезпеки», Київ, Україна

УДК 614.8:504.06:519.87

DOI: 10.52363/2522-1892.2021.1.4

Отримано: 23 лютого 2021

Прийнято: 21 квітня 2021

Cite as: Bandurian B., Kovalevskij V., Tsvaigov D. (2021). Formalization of safety assessment and management. Technogenic and ecological safety, 9(1/2021), 26–30. doi: 10.52363/2522-1892.2021.1.4

Анотація

Стаття є першою зі серії статей, об'єднаних єдиною темою удосконалення організації системи управління безпекою країни. Статтю обмежено розглядом загальних принципів організації управління безпекою країни. Запропоновано розподіляти всю діяльність та цінності країни на три типи потенціалів, які характеризуються кількісними, або об'єктивними формальними параметрами і передбачають різний тип управляючих впливів; описувати потенціалами поточний, цільовий, прогностичний стан країни та припустимі обмеження потенціалів.

Складові комплексних параметрів запропоновано поділяти на три групи: позитивні потенціали, які доцільно нарощувати, негативні потенціали, які доцільно зменшувати, та пасивні потенціали, які не формалізовано, або відношення до яких не визначено. З зазначених складових вплив на прийняття рішень мають позитивні і негативні компоненти. Пасивна складова з часом може трансформуватись в позитивну або в негативну складову.

Приведено приклади застосування підходу, що пропонується.

Ключові слова: безпека, оцінка стану безпеки, організація системи безпеки, інфрачервоне сканування.

Постановка проблеми

Актуальність удосконалення системи національної безпеки визначена головними законодавчими актами України. Забезпечення безпечних умов життєдіяльності суспільства визначено Концепцією національної безпеки України в якості пріоритетного національного інтересу України. Сьогодні теоретичні й практичні питання організації державного управління у цій сфері безпеки недостатньо досліджені і розроблені. Існують досить суперечливі погляди щодо понятійно-категорійного апарату, цінностей, інтересів, загроз та їх реалізації, шляхів, засобів та способів запобігання негативних тенденцій та захисту національних інтересів.

Розгляд всього обсягу поглядів та об'єктивної інформації, які характеризують безпеку країни, дає можливість розгляду окремих проблем, але не дає можливості кількісно оцінити безпеку всієї країни. В значній частині сучасний підхід носить декларативний характер, без інформації, необхідної для прийняття рішень на практиці. Тому прийняття рішень часто базується на помилкових поглядах управлінців та політиків вищої ланки.

З зазначеного випливає потреба в достовірному інформаційному забезпеченні прийняття оптимальних рішень і перспективність напрямку підвищення значимості об'єктивної інформації і поширення області формальних процедур прийняття рішень.

Аналіз останніх досліджень і публікацій

Розгляд шляхів удосконалення системи управління є постійним напрямком діяльності наукових колективів.

За напрямком, що запропоновано, накопичено значний досвід, який трансформовано у документи практичного застосування. Наприклад, розроблено систему стандартів ISO з безпеки, якості та управління.

В Україні окремо значимим документом є Національний класифікатор України Класифікатор надзвичайних ситуацій ДК 019:2010 та низка документів, які регламентують надзвичайні ситуації [2]. В документах опрацьовані алгоритми визначення, кількісні та об'єктивні якісні показники ознак надзвичайних ситуацій. Найбільш цінним в зазначених документах є те, що показники надзвичайних ситуацій були погоджені з усіма міністерствами та відомствами країни. Фактично Класифікатори легітимно визначають кількісні характеристики стану техногенної безпеки.

Робота з удосконалення системи безпеки в Україні проводиться постійно. Прикладом зазначеної діяльності останнього часу є розробка Проекту Закону України Про критичну інфраструктуру [11] (далі – Проект Закону).

На жаль, як в Україні, так і в іншому світі, в межах існуючих класичних підходів до управління, немає повної економічної, наукової та соціальної концепції, яка могла б стати керівництвом для однозначного вирішення практичних питань на нижчих рівнях.

Постановка завдання та його вирішення

Виходячи з визначення актуальності, достовірної оцінки загроз та ефективного управління станом всієї сукупності процесів та об'єктів, значимих для національної безпеки країни, пропонується підхід удосконалення управління системою безпеки за напрямком підвищення значимості об'єктивної інформації і поширення області формальних процедур прийняття рішень.

Стаття є першою складовою з серії статей, об'єднаних єдиною темою удосконалення організації системи управління безпекою країни. Статтю обмежено розглядом загальних принципів удосконалення організації управління безпекою країни.

Стан безпеки пропонується характеризувати сукупністю потенціалів – кількісних характеристик, або об'єктивних якісних ознак процесів та об'єктів, значимих для життєдіяльності країни.

Кількість потенціалів, для об'єктивного відображення стану безпеки, буде з часом мінятися і залежить від рівня знань, уявлень, прийнятих методик, інших обставин.

Нечутливість методики оцінки стану безпеки від змін локальних методик нижчого рівня забезпечується введенням розподілу всіх потенціалів на три групи потенціалів з можливістю переведення потенціалів з групи до групи в залежності від умов, знань та рівня можливостей.

Структуру техногенної безпеки за розподілом на потенціали проілюстровано схемою (рис. 1).

Всі складові техногенної діяльності характеризуються трьома групами потенціалів.

Організацію управління за запропонованими принципами проілюстровано схемою на рис. 2.

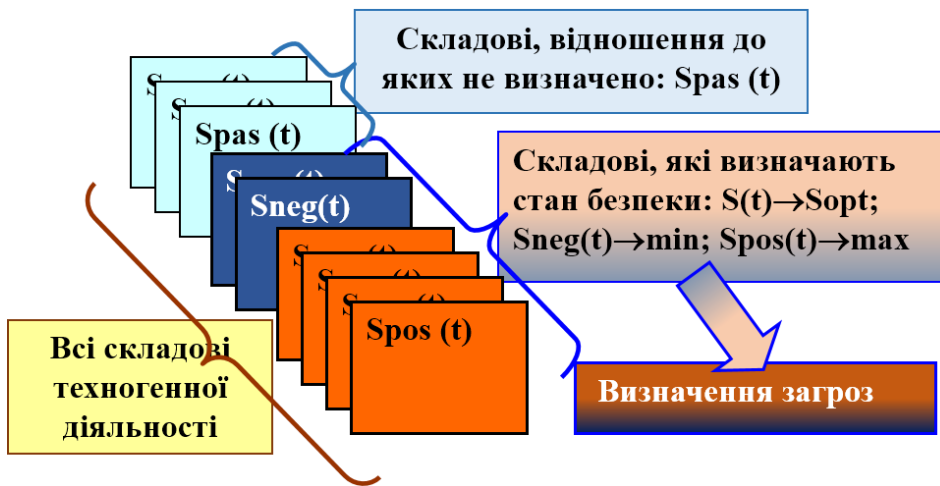


Рисунок 1 – Структура складових техногенної безпеки

У кожен момент часу t стан безпеки оцінюється значеннями комплексного параметру поточного стану безпеки:

$$S(t) = Spos(t) + Sneg(t) + Spas(t)$$

і значеннями комплексного параметру прогнозного стану безпеки на час f :

$$Sprg(f) = Sprg(f) + Sprg(f) + Sprg(f).$$

Складові комплексних параметрів поділяються на 3 групи:

- група з нижнім індексом «pos» (positive) – «позитивний» – потенціал, якій доцільно нарощувати $Spos(t) \rightarrow \max$;
- група з нижнім індексом «neg» (negative) – «негативний» – потенціал, якій доцільно зменшувати $Sneg(t) \rightarrow \min$;
- група з нижнім індексом «pas» (passive) – «пасивний» – потенціал, якій не формалізовано, або відношення до якого не визначено.

З зазначених складових вплив на прийняття рішень мають позитивна і негативна компоненти.

Пасивна складова з часом може трансформуватись в позитивну або в негативну складову.

Початковий стан безпеки фіксується значеннями $Spos(0)$ і $Sneg(0)$, які відображуються в паспортах об'єктів.

Запланований перспективний (цільовий) стан безпеки на час T ($S(T)$), визначається директивно в плануючих документах потенціалами $Spos(T)$ і $Sneg(T)$ та значеннями обмежень $Ssaf$, $\min Sneg$, $\max Spos$.

Метою управління буде оптимальний перевід об'єкту управління від поточного до цільового стану:

$$S(t) \rightarrow S(T)$$

Завданнями управління на кожен поточний час t буде досягнення оптимального впливу на об'єкт управління:

$$S(t) \rightarrow Sopt(t)$$

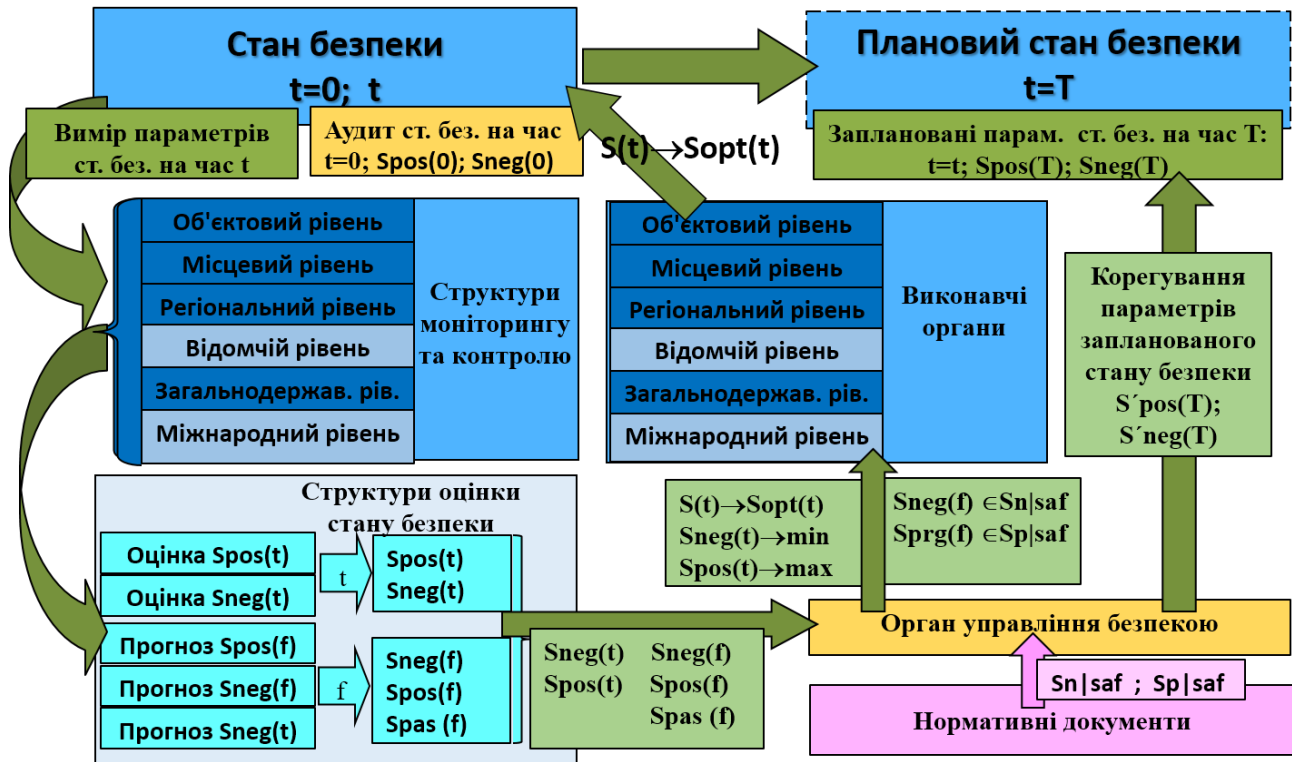


Рисунок 2 – Схема організації управління безпекою

За кількісними показниками буде:

- Sneg(t) → min;
- Spos(t) → max;
- Sneg(f) ∈ Sn|saf;
- Sprg(f) ∈ Sp|saf.

Прикладне застосування.

Законодавча база, що дозволяє оцінювати та розвивати систему безпеки держави за множиною значимих потенціалів безпеки, в Україні існує.

Окрему увагу необхідно уділити показникам прогнозування розвитку України в упереджену точку. Акцентуємо увагу лише на трьох напрямках розвитку, які можуть привести до революційного впливу на стан безпеки. По-перше, це впровадження систем отримання об'єктивної інформації за схемою трьох груп потенціалів шляхом обробки інфрачервоного спектру. Напрямок отримання інформації за допомогою аналізу інфрачервоних спектрів об'єктів сканування є одним з самих перспективних в силу високої інформативності інфрачервоного спектру і можливості пасивного сканування [4, 5, 6, 7, 8]. Збір та обробку інформації за цим напрямком доцільно проводити комплексно зі створенням постійно поновлюваного інформаційного поля за ієрархічним принципом – від використання космічних та авіаційних засобів до досліджень безпосередньо на об'єкті [8]. Метод, дозволяє швидко отримати об'єктивну інформацію як на глобальному рівні при обстеженні великих площ, так і на об'єктовому рівні з забезпеченням максимальної достовірності [7, 8].

Другим напрямком підвищеної уваги є кібербезпека, яка вже на сучасному етапі набуває виключне значення.

Основа підходу державних структур до розвитку системи кібербезпеки полягає в тому, щоб сформувати систему захисту від небажаних впливів в кіберпросторі. Система кібербезпеки держави розглядається як самостійне доповнення до загальної системи безпеки держави.

Базові позиції такого підходу дещо помилкові. Транспорт, енергетика та охорона здоров'я, телекомунікації, фінанси, безпека, демократичні процеси, космос та оборона значною мірою залежать від мережевих та інформаційних систем, зв'язки між якими стають дедалі тіснішими [1]. Стрімке розгортання кіберпростору та його інтеграція у всі сфери діяльності країни та кожної особи вже формує систему безпеки, в якій безпека всіх складових пов'язана з кібербезпекою. Тому відмінною особливістю розвитку системи кібербезпеки сьогодення, і тим більше в перспективі, є охоплення кіберпростором всіх сфер діяльності функціонально, територіально і фактичне об'єднання систем безпеки техногенної діяльності з системою кібербезпеки. Система кібербезпеки вже стала невід'ємною складовою системи безпеки. Саме тому систему кібербезпеки доцільно описувати за схемою трьох груп потенціалів, а побудова системи кібербезпеки має базуватися на принципах побудови загальної системи безпеки держави з інтегруванням в відповідний методичний та понятійний апарат.

Останній, але не менш важливий, приклад з сегменту розробки законодавчої бази, пов'язаний з об'єктами критичної інфраструктури.

Відповідно Проекту Закону [11], під критичною інфраструктурою розуміється сукупність виключно важливих об'єктів. І, оскільки таких об'єктів багато, критична інфраструктура охоплює практично всі сфери діяльності держави.

Як наслідок, постає питання про створення надвідомчого органу, керуючого к-інфраструктурою.

Незважаючи на високий рівень розробки Проекту Закону, головне посилання при використанні трьох груп потенціалів стає, вочевидь, помилковим.

Які б об'єкти не включили в критичну інфраструктуру, це не стане достатнім і не гарантує повноти переліку на весь час. У якийсь момент часу незначна і не включена в критичну інфраструктуру складова може стати стратегічно важливою.

Тому критичну інфраструктуру необхідно визначати не як окрему особливо важливу структуру, а як сукупність елементів звичайної системи управління, які в поточний момент пов'язані з високими ризиками для держави.

Причому, принциповим є той факт, що в критичну інфраструктуру може потрапити будь-який елемент, яким керує держава. В іншому випадку, якщо елемент настільки неважливий, що його деградація не викликає ніякої загрози, то не зрозуміло, навіщо і для чого він взагалі потрапляє в структуру управління країною.

Тобто, режим для об'єктів критичної інфраструктури – це режим звичайних об'єктів управління, які створюють підвищені ризики. У критичну інфраструктуру може потрапити будь-який об'єкт будь-якого міністерства. Об'єкти, які в поточний момент створюють підвищену потенційну загрозу, і становитимуть критичну інфраструктуру.

В зв'язку з зазначеним створення додаткового надвідомчого органу втрачає будь-який сенс.

Необхідна регламентація діяльності всіх міністерств з об'єктами, пов'язаними з підвищеним ризиком для держави.

Висновки

Напрямок удосконалення управління системою безпеки за рахунок підвищення значимості об'єктивної інформації і поширення області формальних процедур прийняття рішень можливий та перспективний. За цим напрямком, вже на початковому етапі, можливий ефективний аналіз стану безпеки.

Пропонується в якості перспективних визначити напрямки досліджень:

- ІЧ-спектроскопію в якості технології збору об'єктивної інформації високої ефективності;
- створення системи реагування на надзвичайні ситуації в кіберпросторі в якості складової загальної системи безпеки країни з потенційними нестандартними загрозами виключно високого рівня небезпеки.

ЛІТЕРАТУРА

1. Joint Communication to the European Parliament and the Council. The EU's Cybersecurity Strategy for the Digital Decade. Join (2020) 18 final. European Commission of the Union for Foreign Affairs and Security Policy. Brussels, 16.12.2020.
2. Національний класифікатор України Класифікатор надзвичайних ситуацій ДК 019:2010. Затв. Наказом Держспоживстандарту України від 11.10.2010 р. № 457. Чинний від 01.01.2011 р.
3. Клепиков В.Ф. Тепловізорний метод оцінки зсувонебезпеки в зоні розташування гідротехнічних споруд енергетичного комплексу / В.Ф. Клепиков, В.В. Литвиненко, Б.Б. Бандурян, М.І. Базалес, О.Г. Лисиченко, І.Б. Воробйов // Техногенно-екологічна безпека та цивільний захист. – 2013. – Вип. 5. – С. 84-94.
4. Пат. 40608 Україна, E02B 1/00, E04C 2/04 (2006.01), E04B 1/02 (2006.01). Спосіб діагностики стану бетонних гідротехнічних споруджень, які знаходяться під впливом напірної фільтрації / В.Ф. Клепиков, Ю.Л. Забулонов, В.В. Литвиненко, Б.Б. Бандурян, М.І. Базалес, О.Г. Лисиченко; (Україна), заявник та патентовласник Інститут електрофізики і радіаційних технологій НАН України. – № u200806435, заяв. 14.05.2008; опубл. 27.04.2009, бюл. № 8.
5. Пат. 115934 Україна, G01J 5/20 (2006.01), G01J 3/28 (2006.01), G01N 21/35 (2014.01), G01C 11/02 (2006.01). Спосіб реєстрації спектра інфрачервоного проміння / В.Ф. Клепиков, В.В. Литвиненко, Б.Б. Бандурян, О.Й. Волчок, В.І. Соколенко, А.В. Пахомов; (Україна), заявник та патентовласник Національний науковий центр «Харківський фізико-технічний інститут» НАН України; Інститут електрофізики і радіаційних технологій НАН України. – № a201605738, заяв. 27.05.2016; опубл. 10.01.2018, бюл. № 1.
6. Заключний звіт зі здійснення інфрачервоного сканування поверхні в місці аварії на виконання природоохоронного заходу «Моніторинг довкілля у місці техногенної аварії біля смт. Ожидів». – Львів, Київ: НВО ЕТН. – 2008.
7. Ітоговий звіт «Польові контрольно-вимірвальні роботи, ландшафтно-геохімічна характеристика території колишнього Виробничого об'єднання Придніпровський хімічний завод» з виконанням експертизи та контролю робіт з паспортизації хвостосховищ та об'єктів уранового виробництва». Етап 2». – Київ: ІГНС. – 2009.
8. Звіт «Проведення комплексного обстеження та оцінка геодинамічних умов в зоні розташування греблі Дніпровської ГЕС з урахуванням тектонічної активності та сейсмічних впливів». Етап 2: «Польове інструментальне обстеження району розташування Дніпровської ГЕС». – Київ: Державне підприємство «Екоінформ» НАН України. – 2009.
9. Kovalevskyi V.V. Radiological control and monitoring on the military installation sites in Ukraine. General approaches. / V.V. Kovalevskyi // SCOPE-RADSITE. "Radioactivity from Military Installationsites and Effectson Population Health", 12-14.11.1998, Belgium.
10. Забулонов Ю.Л. Принципи удосконалення системи антитерористичного моніторингу і контролю САТМ / Ю.Л. Забулонов, В.В. Ковалевський, Г.В. Лисиченко // Збірник праць Інституту геохімії НАН України, Київ. – 2008.
11. Федієнко О.П. Проект Закону України «Про критичну інфраструктуру народних депутатів України». / О.П. Федієнко та ін, рукопис станом на 05.02.2021 р.

Bandurian B., Kovalevskij V., Tsvaigov D.
FORMALIZATION OF SAFETY ASSESSMENT AND MANAGEMENT

The article is the first in a series of articles, united by a single theme of improving the organization of the country's security management system. The article is limited to the general principles of the organization of security management of the country. It is proposed to divide all activities and values of the country into three types of potentials, which are characterized by quantitative or objective formal parameters and provide for different types of management influences; describe with potentials the current, target, forecast state of the country and allowable limitations of potentials.

It is proposed to divide the components of complex parameters into three groups: positive potentials, which should be increased, negative potentials, which should be reduced, and passive potentials, which are not formalized or the relation to which is not defined. Of these components, positive and negative components have an impact on decision-making. The passive component can eventually be transformed into a positive or negative component.

Examples of application of the offered approach are resulted.

Key words: security, security assessment, security system organization, infrared scanning.

REFERENCES

1. Joint Communication to the European Parliament and the Council. The EU's Cybersecurity Strategy for the Digital Decade. Join (2020) 18 final. European Commission of the Union for Foreign Affairs and Security Policy. Brussels, 16.12.2020.
2. Nacional'nyj klasyfikator Ukrainy Klasyfikator nadzvychajnyh situacij DK 019:2010. Zatv. Nakazom Derzhspozhyvstandartu Ukrainy vid 11.10.2010 r. № 457. Chynnyj vid 01.01.2011 r.
3. Klepikov V.F., Lytvynenko V.V., Bandurjan B.B., Bazaljejev M.I., Lysychenko O.G., Vorobjov I.B. (2013). Teplovizornyj metod ocinky zsvonebezpeky v zoni roztashuvannja gidrotehnyh sporud energetychnogo kompleksu. *Tehnogenno-ekologichna bezpeka ta cyvil'nyj zahyst*, 5: 84-94.
4. Klepikov V.F., Zabulonov Ju.L., Lytvynenko V.V., Bandurjan B.B., Bazaljejev M.I., Lysychenko O.G. (2009). Patent 40608 Ukraine, E02B 1/00, E04C 2/04 (2006.01), E04B 1/02 (2006.01). Sposib diagnostyky stanu betonnyh gidrotehnyh sporudzen', jaki znahodjat'sja pid vplyvom napirnoi fil'tracii'.
5. Klepikov V.F., Lytvynenko V.V., Bandurjan B.B., Volchok O.J., Sokolenko V.I., Pahomov A.V. (2018). Patent 115934 Ukraine, G01J 5/20 (2006.01), G01J 3/28 (2006.01), G01N 21/35 (2014.01), G01C 11/02 (2006.01). Sposib rejestracii' spektra infrachervonogo prominnja.
6. Zakljuchnyj zvit zi zdijsnennja infrachervonogo skanuvannja poverhni v misci avarii' na vykonannja pryrodohoronnoho zahodu «Monitoryng dovkillja u misci tehnogennoi' avarii' bilja smt. Ozhydiv». L'viv, Kyi'v: NVO ETN, 2008.
7. Itogovyj zvit «Pol'ovi kontrol'no-vymirjuval'ni roboty, landshaftno-geohimichna harakterystyka terytorii' kolyshn'ogo Vyrobnyc'hogo ob'jednannja Prydniprov's'kyj himichnyj zavod» z vykonannjam ekspertyzy ta kontrolju robiz z pasportyzacii' hvostoshovyshh ta ob'ektiv uranovogo vyrobnyc'tva». Etap 2». Kyi'v: IGNS, 2009.
8. Zvit «Provedennja kompleksnogo obstezhennja ta ocinka geodynamichnyh umov v zoni roztashuvannja grebli Dniprov's'koi' GES z urahuvannjam tektonichnoi' aktyvnosti ta sejsmichnyh vplyviv». Etap 2: «Pol'ove instrumental'ne obstezhennja rajonu roztashuvannja Dniprov's'koi' GES». Kyi'v: Derzhavne pidpryjemstvo «Ekoinform» NAN Ukrainy, 2009.
9. Kovalevskij V.V. (1998). Radiological control and monitoring on the military installation sites in Ukraine. General approaches. *SCOPE-RADSITE. "Radioactivity from Military Installationsites and Effectson Population Health"*, 12-14.11.1998, Belgium.
10. Zabulonov Ju.L., Kovalevskij V.V., Lysychenko G.V. (2008). Pryncypy udoskonalennja systemy antyterorystychnogo monitoryngu i kontrolju SATM / Zabulonov Ju.L. *Zbirnyk prac' Instytutu geohimii' NAN Ukrainy*, Kyi'v, 2008.
11. Fedijenko O.P. Proekt Zakonu Ukrainy «Pro krytychnu infrastrukturu narodnyh deputativ Ukrainy». / O.P. Fedijenko ta in, rukopys stanom na 05.02.2021 r.