Петро Кузик

*аспірант кафедри державного управління Науково-навчального інституту соціальних наук ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом», м. Київ, Україна,
e-mail: iapm@iapm.edu.ua, <https://orcid.org/0000-0003-3855-2524>*

СИСТЕМА КОНТРОЛЮ ЗАГРОЗ ВИБОРЧОМУ ПРОЦЕСУ В МЕХАНІЗМІ ДЕРЖАВНОГО УПРАВЛІННЯ

Анотація. Статтю присвячено аналізу системи контролю загроз, яка допомагає державному управлінню в провідних країнах світу. Особливо гостро проблематика загроз продемонструвала себе останні кілька років, зокрема – в ході реалізації заходів протидії поширенню коронавірусної хвороби COVID-19 та заходів з кібербезпеки, орієнтованих на протидію програмам-вимагачам та іншим кібератакам.

Постійне оновлення підходів до створення систем контролю загроз для організацій різної форми власності та державного управління включає в себе критичне зрушення старої парадигми питання безпеки. Сьогодення вимагає більш активної участі з боку керівництва, в першу чергу, під час підготовчого етапу цього процесу, який пронизує всі рівні управління і вимагає постійних зусиль з проведення оцінки та попередження загроз.

Автор констатує оновлення чинного законодавства, покликане протидіяти загрозам, у тому числі – кіберзагрозам. Такі заходи стосуються і протидії кіберзагрозам виборчому процесу, що набуває особливої ваги з огляду на викриття спроб впливу на вибори президента у США та Франції.

Проаналізовано деякі заходи протидії кіберзагрозам місцевим виборам в 2020 році, з боку, зокрема заходи спрямовані на протидію фейкам стосовно COVID-19.

Окрему увагу присвячено оцінці наявного стану протидії кіберзагрозам в Україні та тенденціям стосовно його зміни. Констатовано наявність негативної динаміки та акцентовано увагу на потребі не лише розробки освітніх для фахівців з кібербезпеки, але й налагодження підготовки фахівців за рядом спеціалізацій, зокрема: фахівців по роботі з великими масивами даних, фахівців із цифрової трансформації, фахівців з навчання цифровим компетентностям та інших професій.

Ключові слова: державне управління, виборчий процес, безпека, загрози безпеці, інформаційна безпека, кібератака, COVID-19.

Petro Kuzyk

*Postgraduate student of the Department of Public Administration of the Research and Training Institute of Social Sciences of PJSC "Higher Educational Institution" Interregional Academy of Personnel Management ", Kyiv, Ukraine,
e-mail: iapm@iapm.edu.ua, <https://orcid.org/0000-0003-3855-2524>*

THE SYSTEM OF CONTROL OVER THREATS TO THE ELECTORAL PROCESS IN THE MECHANISM OF PUBLIC ADMINISTRATION

Abstract. The article is devoted to the analysis of the threat control system, which helps public administration in the leading countries of the world. The issue of threats has been especially acute in the past few years, in particular, during the implementation of measures to counter the spread of the coronavirus disease COVID-19 and cybersecurity measures aimed at countering ransomware and other cyber attacks.

Constantly updating approaches to creating threat control systems for organizations of various forms of ownership and government administration includes a critical shift in the old paradigm in the issue of security. Modernity requires more active participation on the part of the leadership of the state, first of all, during the preparatory stage of this process, which permeates all levels of government and requires constant efforts to assess and prevent threats.

The author states that the current legislation has been updated to counter threats, including cyber threats. Such measures also relate to countering cyber threats to the electoral process, which is of particular importance in view of the exposure of attempts to influence the presidential elections in the United States and France.

Some measures to counter cyber threats to local elections in 2020 were analyzed, in particular, measures aimed at countering fakes regarding COVID-19.

Special attention is devoted to assessing the current situation in countering cyber threats in Ukraine and trends regarding its change. The presence of negative dynamics was stated and attention was focused on the need not only to develop educational programs for cybersecurity specialists, but also to establish training of specialists in a number of specializations, in particular: specialists in working with large amounts of data, specialists in digital transformation, specialists in teaching digital competencies, and other professions.

Keywords: public administration, electoral process, security, security threats, information security, cyberattack, COVID-19.

Постановка проблеми. Тотальна інформатизація суспільства, що супроводжує перехід виробничих процесів до нового, четвертого етапу науково-технічної революції, настільки сильно видозмінює архітектуру викликів та загроз державі, національній безпеці та громадському порядку,

що незмінними лишаються тільки базові принципи та основні постулати теорії безпеки. Особливе місце серед сучасних загроз, посідає категорія, яка не має історичних аналогів (а отже – і відомих раніше заходів протидії) – кіберзагрози. При цьому, важливою якістю кіберзагроз, є їх дуальна природа. З одного боку, вони проявляють себе в якості негативного впливу на системи комунікації, обробки й зберігання інформації, з іншого ж – як канал для реалізації інших загроз – впровадження дезінформації, поширення панічних настроїв, здійснення негативного впливу на моральний стан мільйонів людей.

Особливо гостро проблематика загроз продемонструвала себе останні кілька років, зокрема – в ході реалізації заходів протидії поширенню коронавірусної хвороби COVID-19. Кількість спотвореної інформації та дезінформації стосовно подолання COVID-19 стала своєрідним феноменом. Все це, своєю чергою, не могло не позначитися на підходах до контролю загроз виборчому процесу в механізмі державного управління, що й обумовлює актуальність даного дослідження.

Аналіз попередніх досліджень даної тематики. Проблематика оцінки й прогнозування загроз, а також механізмів протидії їм, зокрема – в межах виборчого процесу є доволі опрацьованою у західному науковому просторі. Зокрема, значної уваги вона набула у працях таких західних дослідників як А. Clayton, Е. Nakashima, Р. Sonne, Н. Taleb, Л. Tilman. У вітчизняному науковому просторі цю проблематику, у контексті державного управління, досліджували А. Савков, І. Баришев, Р. Кравець, І. Кірнос, С. Кукушкіна, С. Лисенко, Е. Мамедова, Н. Нижник, С. Серьогіна В. Цимбалюк та інші.

Водночас, з огляду на невпинне розширення палітри загроз, проблематика контролю загроз виборчому процесу в механізмі державного управління й надалі лишається малодослідженою та потребує уваги науковців, які представляють різні галузі знань.

Метою статті є висвітлення нового погляду на контроль за загрозами виборчому процесу в механізмі державного управління.

Виклад основного матеріалу. Прийнята у провідних країнах світу система контролю загроз допомагає державному управлінню пройти процес оцінки та авторизації для підтвердження безпеки їх державних систем стосовно наявності у них адекватних алгоритмів для виявлення і подальшого усунення чи бодай – зниження ризиків для безпеки.

Національний інститут стандартів і технологій (NIST) Сполучених Штатів Америки завершив роботу над оновленням спеціальної публікації 800-37 «Система управління ризиками для інформаційних систем і організацій: Системний підхід протягом усього експлуатаційного періоду для забезпечення безпеки і конфіденційності» в 2020 році [1]. Причина активізації уваги до цих концепцій аж ніяк не в тому, що вони не були сформульовані раніше. Справа в іншому – тактика інформаційних агресорів висвітлила слабкість системи поставок і вразливість підрядників.

Ще у 2018 році видання Washington Post розповіло широкому загалу про те, як китайські хакери отримали понад 600 ГБ даних, що стосувалися проекту, відомого як «Морський дракон», зокрема сигналів та даних датчиків, а також інформації про підводні човни, що стосувалася криптографічних систем, та бібліотеки електронної боротьби з підводними човнами ВМС, що містила сигнали підводних човнів ВМС США, сенсорних, криптосистем, також інших конфіденційних тактичних і проектних даних. Що характерно, хакери не зламали ВМС – вони зламали їх підрядника [2]. Звісно ж, уряд США почав присвячувати більше уваги проблемі безпеки своєї системи поставок і відтепер просить підрядників вживати всіх можливих заходів інформаційної безпеки, щоб уникнути потрапляння інформації до своїх геополітичних суперників.

Відтак, метою запровадження державного управління безпекою є надання організаціям більшої мобільності в адаптації засобів управління для задоволення їх особливих потреб. Створення надійної системи внутрішнього аудиту, в межах державного управління, починається з першого кроку: підготовки. При цьому, основна увага зосереджена на чотирьох елементах державного управління: виборі елементів управління, впровадженні елементів управління, оцінці елементів управління, моніторингу елементів управління.

Ключова роль державного управління в межах системи контролю ризиками пов'язана із відповідальністю за розподіл зазначених ролей між окремими особами або групами осіб, які підпорядковані відповідному контролюючому органу або підрозділу безпеки. І оскільки на перший погляд складається враження, що за такої організації державного управління потрібно тільки схвалити систему контролю, варто звернути більш детальну увагу на ролі учасників системи, зупинившись, зокрема, на їх функціях. Це допоможе зрозуміти, чому система має бути такою надійною для державного управління і застосуватися на всіх рівнях організації [3].

Відповідно до своєї ролі, учасники системи контролю розподіляються на дві групи, урядову та корпоративну, саме в першій і криється сенс державного управління в системі контролю загрозами.

Урядова (службовець, підрядник або цивільна особа) група:

- Уповноважена посадова особа - це посадова особа керівного складу, яка візьме на себе відповідальність за загрози, пов'язані з системою безпеки. Повноваження мають бути визначені у контракті такої особи.
- Уповноважений офіційний представник (для конкретних завдань), має певні навички та призначається урядом у разі потреби.
- Аудитор (або ціле агентство з аудиту), з яким організація працює за контрактом. Цю роль також може відігравати інша державна аудиторська організація.
- Головний технічний інструмент (по впровадженню технологічних рішень з урахуванням питань безпеки та конфіденційності) – входить до

складу системи, і є частиною функції державного управління системою контролю за загрозами.

- Власник інформації (оскільки організація не володіє інформацією у системі, це робить уряд). Державне управління забезпечує співпрацю з організаціями (власниками інформації) для забезпечення безпеки їх даних.

- Ризик-менеджер (функціональний) – дана роль зарезервована тільки за державними службовцями і в кінцевому підсумку передбачає відповідальність за всі загрози, пов'язані з виконанням завдань або веденням діяльності.

- Старша посадова особа, відповідальна за управління ризиками – очолює функцію управління ризиками. Як і на попередніх аналогічних посадах, це державний службовець, відповідальний за питання конфіденційності.

Корпоративна група:

- Співробітник з питань інформації (на якому лежить повна відповідальність за систему і процес з боку підрядника).

- Постачальник загального контролю (переважно це особа або група осіб, що визначає політику безпеки організації стосовно системи контролю загроз).

- Модель безпеки або конфіденційності – це роль високого рівня, яка визначає стратегії зниження загроз і розподіл контролю, відповідає за інтеграцію вимог безпеки і конфіденційності під всю систему.

- Власник системи – менеджер, який відповідає за ухвалення рішень.

- Співробітник системи безпеки або конфіденційності – це корпоративний відділ внутрішнього аудиту, який проводить ревізію та звітує.

- Користувач, співробітник організації та інші.

На практиці, одна і та ж особа або команда виконуватиме кілька функцій, і в якості підрядника державного підприємства існує можливість взаємодіяти тільки з контролером і власником об'єкта протягом усього процесу. Причина для необхідності перерахування всіх ролей полягає в тому, щоб продемонструвати, наскільки складним може стати механізм державного управління і як швидко маленький персонал перевантажиться через великий обсяг передбачених обов'язків. Натомість, належне планування може допомогти пом'якшити цю ситуацію.

Звісно ж, держава, в особі уряду, бере на себе основні ризики, але організаціям потрібно буде продемонструвати не лише розуміння ситуації, але й реалізацію комплексу заходів, що свідчитиме про їх готовність до стихійних лих, шпionажу, інших зовнішніх або внутрішніх загроз.

Визначення організаційних базових рівнів контролю та профілів добре виконується завдяки вищевикладеним умовам. Вони дозволяють заздалегідь передбачити оптимальний варіант адаптації, орієнтований на виникнення тих чи інших загроз.

Окремої уваги заслуговує необхідність частого оновлювання власних

правил і частоти перевірок на предмет підвищення привілеїв. Але не менш важливою лишається гнучкість самої системи.

Характер функції забезпечення кібербезпеки вимагає виявлення загроз у цій сфері національної безпеки. В останні роки Україна неодноразово стикалася з актуалізацією таких загроз. Серед таких можна згадати недавнє поширення шкідливого програмного забезпечення «Petya», вимагача «WannaCry», атаки 2015-2016 років на енергетичний сектор, атака на президентські вибори у 2014 році, різні інциденти, пов'язані з інформаційними системами та мережами державних органів і держкомпаній у 2016 році, інциденти, пов'язані з Євромайданом у 2013-2014 роках, а також низка профільних кіберзлочинів, що відбуваються день у день і є не такими відомими широкому загалу [4, с. 70].

При цьому, за останні 4-5 років було ухвалено значну кількість документів, присвячених відображенню принципів формування та реалізації державної інформаційної політики, у тому числі – пов'язаних з протидією деструктивному зовнішньому інформаційному впливу. Такими можна вважати Концепцію розвитку цифрової економіки та суспільства України на 2018-2020 роки та план заходів щодо її реалізації, затверджені Розпорядженнями Кабінету Міністрів України від 20.09.2017 № 649-р, від 8 листопада 2017 р. № 797-р та від 17 січня 2018 р. № 67-р. [5], а також Укази Президента України від 15 березня 2016 року № 96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» і від 14.09.2020 р. № 392/2020 «Про Стратегію національної безпеки України» [6; 7].

Отож, не варто вважати, що держава повністю ігнорує кіберзагрози функціонуванню своїх інститутів, зокрема, кіберзагрози виборчому процесу. 19 грудня 2019 було ухвалено Виборчий кодекс України. На відміну від попередніх регуляторних документів, в його редакції було (бодай – поверхнево) враховано особливості сучасних підходів до втручання у виборчий процес. Так, зокрема, відповідно до ст. 36 «В приміщеннях виборчої комісії, в яких встановлено елементи автоматизованої інформаційно-аналітичної системи, мають право знаходитися особи, визначені рішенням Центральної виборчої комісії або відповідної комісії, які забезпечують кіберзахист, кібербезпеку системи та каналів зв'язку, задіяних для забезпечення її функціонування, та є співробітниками органів, перелік яких визначено відповідним рішенням Центральної виборчої комісії» [8]. Крім Центральної виборчої комісії проблематикою безпеки (у тому числі – кібербезпеки) переймаються й інші структури.

Так, зокрема, напередодні місцевих виборів 2020 року представники Комітету виборців України зазначали, що є ризик застосування маніпуляцій через COVID-19. Зокрема, передбачалося поширення фейків про спалахи хвороби на дільницях, задля залякування людей та усунення їх від участі в голосуванні. Як результат, це може вплинути на, і без того невисоку, явку виборців на місцевих виборах [9]. Не лишилася осторонь виборчих процесів і

СБУ, яка закликала громадян проявляти пильність та повідомляти правоохоронців про:

- підготовку до скоєння терористичних актів, посягання на життя державного чи громадського діяча;
- підготовку та факти посягань на суб'єктів виборчого процесу, виборчі штаби, територіальні виборчі комісії;
- злочини проти виборчих прав і свобод громадян тощо [10].

Однак попри всі заходи наразі рівень кібербезпеки в Україні є доволі низьким. При цьому, значно гіршими є не статичні, а динамічні оцінки, адже останніми роками спостерігаються тенденції до подальшого послаблення рівня кібербезпеки, що обумовлено рядом суб'єктивних і об'єктивних факторів. Відсутність належної уваги з боку держави та соціально-відповідальної підтримки з боку великого бізнесу, створює умови для зниження цифрової грамотності як пересічних громадян, так і представників бізнес-кіл та державного сектору. Значний відсоток від фахівців, які все ж здобули належну професійну підготовку у сфері інформаційних технологій, у тому числі – інформаційної безпеки, виїздить за кордон, або переходить на аутсорсингову роботу за кордоном, фізично лишаючись на території України. В будь-якому разі, здібності та навички цих людей не використовуються для зміцнення кібербезпеки на державному чи корпоративному рівні.

Тому не дивно, що інформаційне середовище України сповнене численними фейками, дезінформацією та іншими формами інформаційної агресії, спрямованими як на завдання збитків державі в цілому, так і на порушення роботи окремих державних інститутів, як то – порушення виборчого процесу. І якщо навіть вибори в таких розвинених країнах як США та Франція зазнають впливу з боку загроз інформаційного характеру (зокрема – кіберзагроз), то Україні, з її сьогодишнім станом забезпечення сфери протидії інформаційним загрозам годі сподіватися на безпеку виборчого процесу.

Висновки. Наявний в Україні рівень кібербезпеки є не просто низьким, адже спостерігаються тенденції до його подальшого послаблення, в першу чергу, з огляду на недостатню цифрову грамотність населення, а також представників бізнес-кіл та державного сектору.

Тому не дивно, що інформаційне середовище України сповнене численними фейками, дезінформацією та іншими формами інформаційної агресії, спрямованими як на завдання збитків державі в цілому, так і на порушення роботи окремих державних інститутів, як то – порушення виборчого процесу. Якщо навіть вибори в таких розвинених країнах як США та Франція зазнають впливу з боку загроз інформаційного характеру (зокрема – кіберзагроз), Україні з її сьогодишнім станом забезпечення сфери протидії інформаційним загрозам годі сподіватися на безпеку виборчого процесу.

З огляду на це, вкрай нагальним є виведення на належний для захисту державних інтересів рівень систем кібербезпеки та захисту від потенційних

небезпек у цифровому середовищі, особливо тих, які відбуваються завдяки людському фактору. Серед іншого, це потребує не лише розробки освітніх для фахівців з кібербезпеки, але й налагодження підготовки фахівців за рядом спеціалізацій, як то – для роботи з великими масивами даних, фахівців із цифрової трансформації, фахівців з навчання цифровим компетентностям та інших професій.

Література:

1. Tilman L. (2013). Risk Intelligence: A Bedrock of Dynamism and Lasting Value Creation. URL: <https://www.europeanfinancialreview.com/risk-intelligence-a-bedrock-of-dynamism-and-lasting-value-creation/>.
2. Ellen Nakashima and Paul Sonne. China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare. June 8, 2018. The Washington Post. URL: https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html
3. Лисенко С. О. Створення системи аналізу інформаційних загроз за найкращими практиками та стандартами. *Європейські перспективи*, №3. 2020. с. 81-88.
4. Мамедова Е.А. Теоретично-правові аспекти кібербезпеки України. *Сучасні проблеми забезпечення національної безпеки держави: Матеріали III Міжнародної науково-практичної конференції (26 листопада 2020 року) Київ. 2020. с. 69-71.*
5. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації: Розпорядження Кабінету Міністрів України від 17.01.2018 р. № 67-р. *Урядовий кур'єр*. 2018. № 88.
6. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15 березня 2016 року № 96/2016. *Урядовий кур'єр* від 18.03.2016. № 52.
7. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»: Указ Президента України від 14 вересня 2020 року № 392/2020. *Урядовий кур'єр* від 16.09.2020. № 179.
8. Виборчий кодекс України: Закон України № 396-IX від 19 грудня 2019 р. URL: <https://zakon.rada.gov.ua/laws/show/396-20#Text>
9. Місцеві вибори 2020 і COVID: що варто знати про правила безпеки. 07.10.2020. URL : <https://decentralization.gov.ua/news/12858>
10. СБУ звертається до громадян із закликом повідомляти про порушення виборчого процесу. 23 жовтня 2020. Офіційний веб-сайт Служби безпеки України. URL: <https://ssu.gov.ua/novyny/sbu-zvertaietsia-do-hromadian-iz-zaklykom-povidomliaty-pro-porushennia-vyborchoho-protsesu>

References:

1. Tilman, L. (2013). Risk Intelligence: A Bedrock of Dynamism and Lasting Value Creation. *www.europeanfinancialreview.com*. Retrieved from <https://www.europeanfinancialreview.com/risk-intelligence-a-bedrock-of-dynamism-and-lasting-value-creation/> [in English].
2. Nakashima, E., Sonne, P. (2018). China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare. *www.washingtonpost.com*. Retrieved from https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html [in English].

3. Lysenko, S.O. (2020). Stvorennia systemy analizu informatsiinykh zahroz za naikrashchymy praktykamy ta standartamy [Creation of a system of analysis of information threats according to the best practices and standards]. *Yevropeiski perspektyvy – European perspectives*, 3, 81-88 [in Ukrainian].

4. Mamedova, E.A. (2020). Teoretychno-pravovi aspekty kiberbezpeky Ukrainy [Theoretical and legal aspects of cybersecurity in Ukraine]. *Suchasni problemy zabezpechennia natsionalnoi bezpeky derzhavy – Modern problems of ensuring the national security of the state: Proceedings of the 3rd International Scientific and Practical Conference*. (pp. 69-71). Kyiv [in Ukrainian].

5. Rozporiadzhennia Kabinetu Ministriv Ukrainy “Pro skhvalennia Kontseptsii rozvytku tsyfrovoi ekonomiky ta suspilstva Ukrainy na 2018-2020 roky ta zatverdzhennia planu zakhodiv shchodo yii realizatsii” : vid 17.01.2018 r., № 67-r [Order of the Cabinet of Ministers of Ukraine On approval of the Concept of development of the digital economy and society of Ukraine for 2018-2020 and approval of the action plan for its implementation dated January 17, 2018 № 67-r]. (2018). *Uriadovyi kurier – Government courier*, 88 [in Ukrainian].

6. Ukaz Prezydenta Ukrainy “Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 27 sichnia 2016 roku «Pro Stratehiiu kiberbezpeky Ukrainy» : vid 15 bereznia 2016 roku № 96/2016 [Decree of the President of Ukraine “On the decision of the National Security and Defense Council of Ukraine of January 27, 2016 "On the Cyber Security Strategy of Ukraine" from March 15, 2016, № 96/2016]. (2016). *Uriadovyi kurier – Government courier*, 52 [in Ukrainian].

7. Ukaz Prezydenta Ukrainy “Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 veresnia 2020 roku «Pro Stratehiiu natsionalnoi bezpeky Ukrainy» : vid 14 veresnia 2020 roku № 392/2020 [Decree of the President of Ukraine “On the decision of the National Security and Defense Council of Ukraine of September 14, 2020 "On the National Security Strategy of Ukraine" from September 14, 2020, № 392/2020]. (2020). *Uriadovyi kurier – Government courier*, 179 [in Ukrainian].

8. Zakon Ukrainy “Vyborchyi kodeks Ukrainy” : vid 19 hrudnia 2019 r., № 396-IX [Law of Ukraine “Electoral Code of Ukraine” from December 19, 2019 № 396-IX]. *zakon.rada.gov.ua*. Retrieved from <https://zakon.rada.gov.ua/laws/show/396-20#Text> [in Ukrainian].

9. Mistsevi vybory 2020 i COVID: shcho varto znaty pro pravyla bezpeky [Local elections 2020 and COVID: what you need to know about security rules]. (2020). *decentralization.gov.ua*. Retrieved from <https://decentralization.gov.ua/news/12858> [in Ukrainian].

10. SBU zvertaietsia do hromadian iz zaklykom povidomliaty pro porushennia vyborchoho protsesu [The SBU appeals to citizens to report violations of the election process]. (2020). *ssu.gov.ua*. Retrieved from <https://ssu.gov.ua/novyny/sbu-zvertaietsia-do-hromadian-iz-zaklykom-povidomliaty-pro-porushennia-vyborchoho-protsesu> [in Ukrainian].