Труш Олександр Олегович,
к держ.упр., проф.,
професор кафедри права та європейської інтеграції,
ХарРІ НАДУ, м. Харків
ORCID 0000-0001-9578-9451;
Василенко Денис Васильович,
аспірант кафедри права та європейської інтеграції
ХарРІ НАДУ, м. Харків

УДК 35:004 **doi 10.34213/db.19.02.21**

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ПРИ ПРИЙНЯТТІ РІШЕНЬ ОРГАНАМИ ПУБЛІЧНОГО УПРАВЛІННЯ

Розглянуто підходи до організації безпечного функціонування органів публічного управління в умовах розвитку сучасних інформаційних технологій. Визначено необхідність швидкої і якісної обробки великих масивів даних, підвищення уваги до своєчасності, точності й правдивості інформації, а також до механізмів забезпечення кібербезпеки при прийнятті ними управлінських рішень. Надано авторські визначення понять "процес публічного управління", "забезпечення кібербезпеки", "механізм забезпечення кібербезпеки", "забезпечення кібербезпеки при прийнятті рішень органами публічного управління".

Ключові слова: органи публічного управління; управлінські рішення; кібербезпека.

Постановка проблеми. Ефективність діяльності органів публічного управління безпосередньо залежить від своєчасного прийняття грамотного управлінського рішення. Процес прийняття управлінських рішень завжди базується на збиранні, відборі та обробці необхідної інформації. Тільки її узагальнений аналіз надає можливість прийняти обґрунтоване рішення. Особливого значення цей процес набуває в умовах багатоваріантності та невизначеності, що призводить до складностей швидкої і якісної обробки великих масивів даних і тим самим підвищеної уваги до своєчасності, точності й правдивості інформації.

Незважаючи на очевидні плюси, стрімкий розвиток інформаційних технологій, девайсів, розумних речей, збільшенням трафіку потоків даних призвели до того, що людина, суспільство, держава почала все більше переносити в кіберпростір і в хмару (діджитал середовище) різні сторони свого життя, своєї діяльності, що породжує низку проблем, однією з яких стає не тільки захист безпосередньо інформації, а й захист всієї системи в

інформаційному полі та в полі комп'ютерних технологій в цілому.

Аналіз останніх досліджень і публікацій. Питанням інформаційно-аналітичне забезпечення процесу формування управлінських рішень присвячено роботи В. Авер'янова, О. Амосова, Л. Антонової, Г. Атаманчука, В. Бакуменка, Н. Грицяк, А. Дєгтяра, А. Додонова, Д. Ланде, В. Ємельянова, Ю. Сурміна, А. Семенченка, В. Тертички, Ю. Шарова та ін.

Забезпечення інформаційної безпеки держави, діяльності органів державного управління розглядали у своїх працях С. Гордієнко, Ю. Довгаль, О. Злагода, Ю. Саричев та інші, безпеку систем підтримки прийняття рішень – В. Ковтунець, О. Нестеренко та О. Савенков. Проблеми забезпечення кібернетичної безпеки держави та шляхи їх вирішення досліджували В. Богданович, В. Бурячок, В. Богуш, О. Довгань, Д. Дубов, Є. Живило, Є. Кубанов, В. Ліпкан, Н. Логінова, А. Марушак, В. Панченко, В. Петров, О. Черноног та ін.

Водночас залишається не розглянутим механізм забезпечення кібербезпеки управлінських рішень органів публічного управління, що обумовлює актуальність поставленої проблеми.

Метою статті є проведення системного аналізу наукових підходів до безпечного функціонування органів публічного управління, механізму забезпечення кібербезпеки при прийнятті ними управлінських рішень.

Виклад основного матеріалу. Термінологічний словник "Публічне управління", підготовлений фахівцями Національної академії державного управління при Президентові України, в якому розкривається термінологічна система публічного управління, визначає категорію публічне управління як діяльність органів державного управління, органів місцевого самоврядування, представників приватного сектору та інститутів громадянського суспільства в межах визначених законом повноважень і функціональних обов'язків (планування, організації, керівництва, координації та контролю) щодо формування та реалізації управлінських рішень суспільного значення, політики розвитку держави та її адміністративно-територіальних одиниць [1, с. 144].

З наведеного визначення витікає, що орган публічного управління – це: 1) орган виконавчої влади й орган місцевого самоврядування, які наділені владними повноваженнями, утворені й діють в установленому законом порядку в межах законодавчо визначеної компетенції та є як юридичні особи публічного права самостійними частинами системи публічної влади; 2) орган виконавчої влади, що бере участь у здійсненні функцій держави, діє від її імені і за дорученням, має державно-владні повноваження, відповідну компетенцію і структуру, застосовує властиві йому організаційно-правові форми діяльності, або орган самоврядного територіального співтовариства, яким він формується і перед яким відповідає за належне здійснення своїх повноважень, тобто орган який здійснює публічне управління [1, с. 107].

Відповідно до роботи [2, с. 103], процес публічного управління можна визначати як послідовне, цілеспрямоване, вольове здійснення взаємопов'язаних функцій публічного управління системою суб'єктів публічного управління, спрямоване на досягнення мети управління – створення найсприятливіших умов для формування публічної влади, що відповідає інтересам громадян, суспільства й держави. Процес публічного управління складається з реалізації конкретних дій і операцій, що спрямовуються на досягнення загальної мети публічного управління, виконання яких можна умовно поділити на послідовно здійснювані стадії.

У процесах публічного управління систематично виникає потреба в ухваленні рішень щодо проблем розвитку: економічного, соціального, гуманітарного, екологічного, технологічного тощо, від яких залежить культурний, освітній, науковий, технологічний рівень країни (галузі, регіону, території), її місце та роль у процесах світового розвитку [3, с. 69].

Ухваленню рішень передує обробка великих масивів різнорідних даних, часто в умовах обмеження часу і нестачі інформації.

Процес ухвалення рішення – процедура, яка передбачає вибір оптимального варіанту з низки альтернативних за допомогою постійної обробки потоків даних. Сьогодні неможливо уявити собі процес ухвалення

(прийняття) рішення без використання комп'ютерної техніки і технологій.

Одним із напрямків роботи з інформацією, яку отримують органи публічного управління, є її узагальнення шляхом використання інтелектуальних методів та технологій, зокрема за допомогою Систем підтримки прийняття рішень (СППР), які дозволяють проводити аналіз даних і за його результатами приймати мотивовані рішення та робити довготривалі прогнози [4, с. 20].

Система підтримки прийняття рішень (СППР) (англ. Decision Support System – DSS) – інтерактивна комп'ютерна автоматизована система (програмний комплекс), що призначена для допомоги та підтримки різних видів діяльності людини при прийнятті рішень стосовно розв'язання структурованих або неструктурованих проблем. Застосування СППР забезпечує виконання ґрунтовного й об'єктивного аналізу предметної області при прийнятті рішень у складних умовах. СППР шляхом збору та аналізу інформації може впливати на процес прийняття управлінських рішень [5] і вимагає постійного й якісного забезпечення інформаційної безпеки, зокрема кібербезпеки.

Кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України в кіберпросторі [6]. Звідси забезпечення кібербезпеки – це діяльність, спрямована на запобігання, своєчасне виявлення, припинення чи нейтралізацію реальних і потенційних загроз життєво важливим інтересам людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища України в кіберпросторі.

Говорячи про кібербезпеку у сфері публічного управління, не можна не погодитись з Є. Кубановим, який зазначив, що "кібербезпека системи публічного управління – це основа національної безпеки України, яка формує

захищеність держави, суспільства, системи публічного управління, населення країни в кібернетичному просторі через створення легітимних механізмів забезпечення кібербезпеки публічного управління” [7, с. 51].

Не зупиняючись докладно на загальновідомих підходах до поняття “механізм”, в нашій роботі будемо розуміти його як систему, що включає взаємодіючі між собою елементи під час її функціонування для досягнення даною системою визначених цілей. Звідси механізм забезпечення кібербезпеки можна визначити як систему правових, управлінських, адміністративних, організаційних, інженерно-технічних, технічних і програмно-технічних заходів, суб’єктів взаємодії, норм, методів, важелів, засобів, інструментів, що забезпечують захищеність життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі.

Зупинимось докладніше саме на системі заходів забезпечення кібербезпеки. Ефективність функціонування системи забезпечення кібербезпеки насамперед залежить від досконалості нормативно-правового регулювання діяльності відповідної системи державних та громадських органів, а також неурядових організацій. Система забезпечення кібернетичної безпеки України створюється й розвивається відповідно до Конституції України та інших нормативно-правових актів, що регулюють суспільні відносини у сфері управління національною безпекою в цілому та кібернетичною безпекою зокрема. Законодавчо-правову основу забезпечення національної безпеки України становлять Конституція України, закони України “Про національну безпеку України”, “Про Раду національної безпеки і оборони України”, “Про Службу безпеки України”, “Про основні засади забезпечення кібербезпеки України”, а також Стратегія національної безпеки України, Стратегія кібербезпеки України, Доктрина інформаційної безпеки України, Положення про Національний координаційний центр кібербезпеки, інші нормативно-правові акти державних органів влади та управління, міжнародні договори й угоди, укладені чи визнані Україною, які відповідають національним інтересам України.

До управлінських заходів насамперед слід віднести формування органами публічного управління політики безпеки, що визначають загальний напрям виконання робіт. Організаційно-адміністративне забезпечення кібербезпеки складається з регламентації діяльності та взаємовідносин суб'єктів використання кіберпростору на нормативно-правових засадах, що унеможливлює розголошення, витік і несанкціонований доступ до інформації або створює суттєві труднощі до її доступу за рахунок проведення організаційних заходів. (Наприклад, створення спеціальної служби інформаційної безпеки, визначення посадових інструкцій працівників, організацію режимних заходів, охорону приміщень, контроль за роботою персоналу з інформацією, визначення порядку зберігання, резервування, знищення конфіденційної інформації й т. ін.)

Інженерно-технічні (фізичні) заходи являють собою сукупність спеціальних органів, технічних засобів і заходів, що функціонують спільно для виконання певного завдання щодо захисту інформації. Рівень забезпечення кібербезпеки залежить від оточення, в якому працює система забезпечення кібернетичної безпеки. До інженерних засобів відносять екранування приміщень, організація сигналізації, охорона приміщень з персональними комп'ютерами.

Програмно-технічні засоби забезпечення кібербезпеки включають в себе апаратні, програмні, криптографічні засоби захисту, які ускладнюють можливість атаки, допомагають виявити факт її виникнення, позбутися від наслідків атаки.

Відтак, забезпечення кібербезпеки при прийнятті рішень органами публічного управління це – діяльність, спрямована на запобігання, своєчасне виявлення, припинення чи нейтралізацію реальних і потенційних загроз при прийнятті рішень органами публічного управління під час використання кіберпростору шляхом застосування легітимних механізмів забезпечення кібербезпеки.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямку. Таким чином, у статті розглянуто підходи до безпечного функціонування органів публічного управління, механізму забезпечення кібербезпеки при прийнятті ними управлінських рішень, надано авторські визначення понять процесу публічного управління, забезпечення кібербезпеки, механізму забезпечення кібербезпеки, забезпечення кібербезпеки при прийнятті рішень органами публічного управління.

У перспективі подальших розвідок передбачається проаналізувати закордонний досвід забезпечення кібербезпеки органів публічного управління та виокремити його основні механізми.

Список використаних джерел

1. Публічне управління : термінологічний словник / уклад. : В. С. Куйбіда, М. М. Білинська, М. М. Петроє. Київ : НАДУ, 2018. 224 с.

2. Бондаренко К. В. Щодо визначення процес у державного управління. Науковий вісник Ужгородського національного університету. 2015. Вип. 35. Ч. І. Т. 2. С. 101–104 (Серія: Право).

3. Коврига О. С. Процес ухвалення управлінських рішень у публічному управлінні. Вчені записки ТНУ імені В. І. Вернадського. 2018. С. 67–72. (Серія: Державне управління).

4. Косолапов В. Л., Колосов В. Є., Ковтун, В. О. та ін. Інформаційно-аналітичні технології як інструмент підтримки та забезпечення систем підтримки прийняття рішень на державному рівні. Математичні машини і системи, 2007. № 1. С. 16–26.

5. Системи підтримки прийняття рішень. URL: https://msn.khnu.km.ua/pluginfile.php/308246/mod_resource/content/4/МСШІ%20Теорія%2012%20Системи%20підтримки%20прийняття%20рішень.pdf (дата звернення: 18.12.2019).

6. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017. № 2163-VIII. Дата оновлення 08.07.2018. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 18.12.2019).

7. Кубанов Є. В. Теоретичні підходи до понятійно-категоріального апарату кібербезпеки в системі публічного управління. Аспекти публічного управління. 2018. Т. 6. № 8. С. 49–55.

References

1. Publichne upravlinnia: terminologichnyi slovnik. (2018). V.S. Kujbida, M.M. Bilynska, M.M. Petroie (Eds.). Kyiv: NADU [in Ukrainian].

2. Bondarenko, K.V. (2015). Schodo vyznachennia protses u derzhavnoho upravlinnia. *Naukovyj visnyk Uzhhorodskoho natsionalnoho universytetu, issue 35, ch. I. vol. 2,* 101–104 [in Ukrainian].

3. Kovryha, O.S. (2018). Protses ukhvalennia upravlinskykh rishen u publichnomu upravlinni. *Vcheni zapysky TNU imeni V.I. Vernadskoho,* 67–72 [in Ukrainian].

4. Kosolapov, V.L., Kolosov, V.Ye., Kovtun, V.O. et al. (2007). Informatsijno-analityni tekhnolohii iak instrument pidtrymky ta zabezpechennia system pidtrymky pryjniattia rishen na derzhavnomu rivni. *Matematychni mashyny i systemy, 1,* 16–26 [in Ukrainian].

5. Systemy pidtrymky pryjniattia rishen. URL: https://msn.khnu.km.ua/pluginfile.php/308246/mod_resource/content/4/MSShI%20Teoriia%2012%20Systemy%20pidtrym

ky%20pryjniattia%20rishen'.pdf [in Ukrainian].

6. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy vid 05.10.2017 № 2163-VIII. (2017). URL: https://zakon.rada.gov.ua/laws/show/2163-19.

7. Kubanov, Ye.V. (2018). Teoretychni pidkhody do poniatijno-katehorialnoho aparatu kiberbezpeky v systemi publichnoho upravlinnia. *Aspekty publichnoho upravlinnia, vol. 6, 8*, 49–55 [in Ukrainian].

Trush O. O.,
PhD. in Public Administration, Professor,
Professor of Department of Law and European Integration,
KRI NAPA, Kharkiv
ORCID 0000-0001-9578-9451;
Vasilenko D. V.,
Post-Graduate Student of Department of Law and European Integration,
KRI NAPA, Kharkiv

Ensuring cyber security in decision making public administration bodies

There are considered in the article the approaches to the organization of safe functioning of public administration bodies in the conditions of modern information technologies development, the necessity of fast and qualitative processing of big data sets, increased attention to timeliness, accuracy and truthfulness of information, the mechanism of providing cybersecurity in making management decisions.

Public administration is the activity of public administration bodies, local self-government bodies, representatives of the private sector and civil society institutions within the limits of the powers and functional responsibilities (planning, organization, leadership, coordination and control) defined by law to form and implement managerial decisions of public importance, development policy of the state and its administrative-territorial units.

The effectiveness of the activities of public administration depends directly on the timely adoption of a competent management decision.

Decision-making is preceded by the processing of large arrays of heterogeneous data, often under the constraints and lack of information.

Today, it is impossible to imagine a decision-making process without the use of computer hardware and technology, which requires constant and high-quality information security, including cybersecurity.

Cybersecurity is an activity aimed at preventing, timely identifying, stopping or neutralizing real and potential threats to the vital interests of the individual and the citizen, society and the state through the use of cyberspace, which ensures the sustainable development of the information society and digital communication environment in Ukraine.

Cybersecurity of public authorities is achieved through a mechanism of cybersecurity that can be defined as a system of legal, administrative, administrative, organizational, engineering, technical and software-technical measures, subjects of interaction, norms, methods, levers, tools, tools that protect the vital interests of man and citizen, society and the state in cyberspace.

Therefore, ensuring cybersecurity in public administration decision-making is an activity aimed at preventing, timely identifying, suspending or neutralizing real and potential threats to public administration decision-making when using cyberspace, through the use of legitimate cybersecurity mechanisms.

Key words: public administration; management decisions; cybersecurity.

Надійшла до редколегії 29.10.2019 р.