Котух Євген Володимирович,
к.т.н., доцент кафедри комп'ютерних наук,
Сумський державний університет,
м. Суми
ORCID 0000-0003-4997-620X

УДК 351.865 **doi: 10.34213/tp.21.01.05**

ОЦІНКА РІВНЯ ЗАХИСТУ КІБЕРПРОСТОРУ В ПУБЛІЧНОМУ УПРАВЛІННІ: НАЦІОНАЛЬНИЙ ТА ОРГАНІЗАЦІЙНИЙ ВИМІРИ

Досліджено особливості та основні напрями забезпечення кібербезпеки в публічному управлінні. Встановлено, що держава в цілому і органи публічного управління зокрема не готові сьогодні до адекватного реагування на головні кіберзагрози, пов'язані з крадіжкою інформації, фінансовим шахрайством і хакерськими атаками. Проаналізовано сучасний стан та шляхи покращання кібербезпеки у сфері публічного управління на національному та організаційному рівнях, зокрема: збільшення бюджетного фінансування відповідної сфери, стратегічне інвестування в кібераналітику і хмарні технології, створення в організаціях спеціальних підрозділів з кіберзахисту, встановлення сучасного програмного забезпечення та його постійне оновлення, регулярне підвищення кваліфікації працівників, задіяних у питаннях захисту організаційної та персональної інформації.

Ключові слова: рівень захисту кіберпростору, забезпечення кібербезпеки, фінансування, публічне управління, хакерські атаки.

Постановка проблеми. Головними кіберзагрозами для сучасної України є крадіжка інформації, фінансове шахрайство і хакерські атаки. При цьому держава в цілому і органи публічного управління зокрема є неготовими сьогодні до адекватного реагування на ці загрози. Рівень кіберзахисту в публічному секторі значно поступається приватному. Державний сектор узагалі виявився найбільш незахищеним з точки зору протистояння кібератакам та витоку даних в Україні. Це зумовлено як недостатньою захищеністю інформаційних мереж, недосконалістю обладнання і програмного забезпечення, що існує, так і відсутністю кваліфікованих фахівців у сфері кіберзахисту. Ураховуючи це, держава не виступає суб'єктом, якому громадяни довіряють у питаннях кіберзахисту та, зокрема, захисту персональної інформації. У такому разі більшість людей покладається на себе. При цьому найбільш захищеними від кібератак та витоку даних є ІТ-компанії та банківський сектор.

Як показує практика, публічний сектор має сьогодні неабиякі проблеми з фінансуванням сфери кібербезпеки і в цьому питання значно поступається приватному. Це зумовлено як недосконалістю державної політики в цій сфері (недостатньою увагою до цих проблем, низькому рівнем фінансування, відсутністю ефективного моніторингу, тестувань, спеціальних підрозділів тощо), так і високою вартістю відповідного обладнання і програм.

Аналіз останніх досліджень і публікацій. Загальні науково-практичні основи кібербезпеки, напрями забезпеченні національної безпеки знайшли своє відображення в численних дослідженнях вітчизняних і зарубіжних науковців, зокрема таких, як С. Андреєв, С. Домбровська, І. Діордіца, Є. Живило, З. Коваль, В. Куцаєв, В. Ліпкан, С. Срібний, В. Ткаченко, В. Шеломенцев та ін. Серед іноземних дослідників своїми працями особливо виділяються Р. Азмі, К. Андреассон, Е. Камарк, П. Кеніс, К. Прован та ін. Але успіх упроваджуваних стратегій кіберзахисту залежить від чіткого обґрунтування до-

цільності заходів на основі виокремлення ключових проблем у цій сфері. У таких умовах необхідним є перманентне оцінювання рівня захисту кіберпростору в публічному управлінні.

Метою статті є оцінювання сучасного рівня захисту кіберпростору в публічному секторі в національному та організаційному вимірах, а також обґрунтування шляхів підвищення кіберзахисту у сфері публічного управління.

Виклад основного матеріалу дослідження. Перш ніж перейти до викладу основних результатів проведеного дослідження, визначимо, що оцінка рівня захисту кіберпростору в публічному управлінні вкрай важлива в сучасних умовах, оскільки вона дозволяє обґрунтовано підходити до формування стратегії кіберзахисту.

З метою з'ясування інформації щодо стану кібербезпеки в Україні в сучасних умовах у період з 24 жовтня по 3 листопада 2020 р. автором за сприяння кафедри політології та філософії Харківського регіонального інституту державного управління було проведене всеукраїнське експертне соціологічне опитування. До складу експертної групи входили: керівники державних та комунальних підприємств; представники великого і середнього бізнесу, банківських структур; керівники громадських організацій, депутати різних рівнів, працівники органів виконавчої влади та місцевого самоврядування, політичні аналітики; журналісти; експерти з питань кібербезпеки.

З урахуванням мети дослідження серед основних його завдань були:

— оцінювання нинішнього стану кібербезпеки в Україні, зокрема на рівні окремих організацій і установ;

— визначення основних кіберзагроз для сфери публічного управління;

— встановлення основних шляхів підвищення рівня кібербезпеки в Україні, зокрема у сфері публічного управління.

Слід зазначити, що під кібербезпекою в дослідженні розумілася 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, своєчасні виявлення й нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі та запобігання їм [1, ст. 1]).

Як з'ясувалося, переважна більшість опитаних не вважає кіберпростір в Україні захищеним. При цьому рівень захисту кіберпростору своїх організацій порівняно із загальнодержавним рівнем опитані вважають набагато вищим (рис. 1).

Цікавим є порівняння рівня захисту "публічних" і "непублічних" організацій. В останніх, згідно з результатами проведеного дослідження, систему захисту від кібератак налагоджено набагато краще. Наприклад, лише 35 % працівників органів публічного управління назвали кіберпростір своїх організацій захищеним порівнянні з 56 % працівниками інших організацій. Привертає увагу те, що трохи більш "захищеними" свої організації вважають мешканці обласних центрів порівняно з мешканцями інших адміністративно-територіальних одиниць (40 проти 35 %).

Відповідно і рівень загроз для країни в цілому експерти вважать вищим, ніж для організацій, у яких вони працюють. Тож не викликає здивування, що "публічний сектор" виявився, за оцінками опитаних, більш незахищеним. Лише 15 % опитаних працівників органів публічного управління оцінили рівень кіберзагроз своїм організаціям як низький.

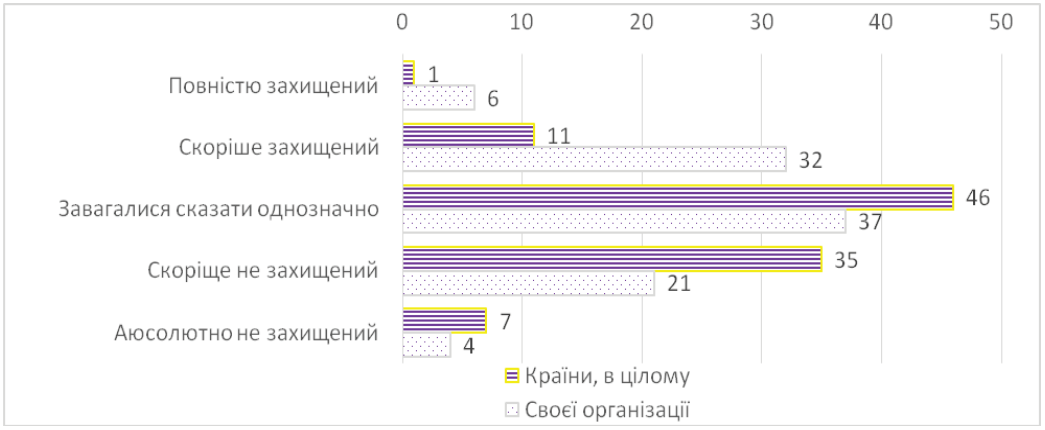

Рис. 1. Оцінка захисту кіберпростору країни та організацій, у яких працюють опитані

З огляду на дані, які наведено, цілком закономірно, що, за результатами опитування, більшість респондентів визнали рівень кібербезпеки в України низьким. До речі, найгірше його оцінили опитані, які обіймають керівні посади в своїх організаціях (58 % із них заявили про низький рівень кібербезпеки країни). Серед головних кіберзагроз, які сьогодні є найбільш актуальними для України, експерти виділили такі, як крадіжка інформації (67 %); фінансове шахрайство (63); хакерські атаки (59); вірусні програми (52 %). Найбільше на крадіжці інформації (73 % у цій групі) та фінансовому шахрайстві (72 %) акцентують особи, які не працюють у "публічному секторі".

На думку опитаних, найбільш успішними з точки зору протистояння кібератакам в Україні є ІТ-компанії (64 %) і банківський сектор (47 %). Лише шоста частина опитаних (17 %) віднесли до успішних державний сектор. Майже ніхто (3 %) не бачить позитивного досвіду протистояння кібератакам в органів місцевого самоврядування (рис. 2).

При цьому державний сектор, за оцінками респондентів, є найменш захищеним від кібератак та ризиків витоку баз даних. Поряд із ним за рівнем кіберзагроз знаходяться лише соціальні мережі. Цікаво, що про незахищеність державного сектору більше говорять ті опитані, які не працюють у публічній сфері (52 %).

Таким чином, можна констатувати, що публічний сектор у цілому є найменш підготовленим до кібератак і немає успішного досвіду протистояння їм. Утім така ситуація має свої причини. Як показало дослідження, фінансування організацій, у яких працюють опитані, знаходиться на вкрай низькому рівні (рис. 3).

Як свідчать результати опитування, лише 8 % респондентів вважають, що їхня організація виділяє абсолютно достатню кількість ресурсів, для того щоб інформацію організації було повністю захищено. При цьому у 4 рази більше опитаних (34 %) зазначають, що таких ресурсів виділяється недостатньо.

Показовим є порівняння відповідей опитаних, які працюють у публічному секторі, та інших. Наприклад, рівень фінансування кібербезпеки в "публічному секторі" є удвічі гіршим порівняно з іншими сферами.

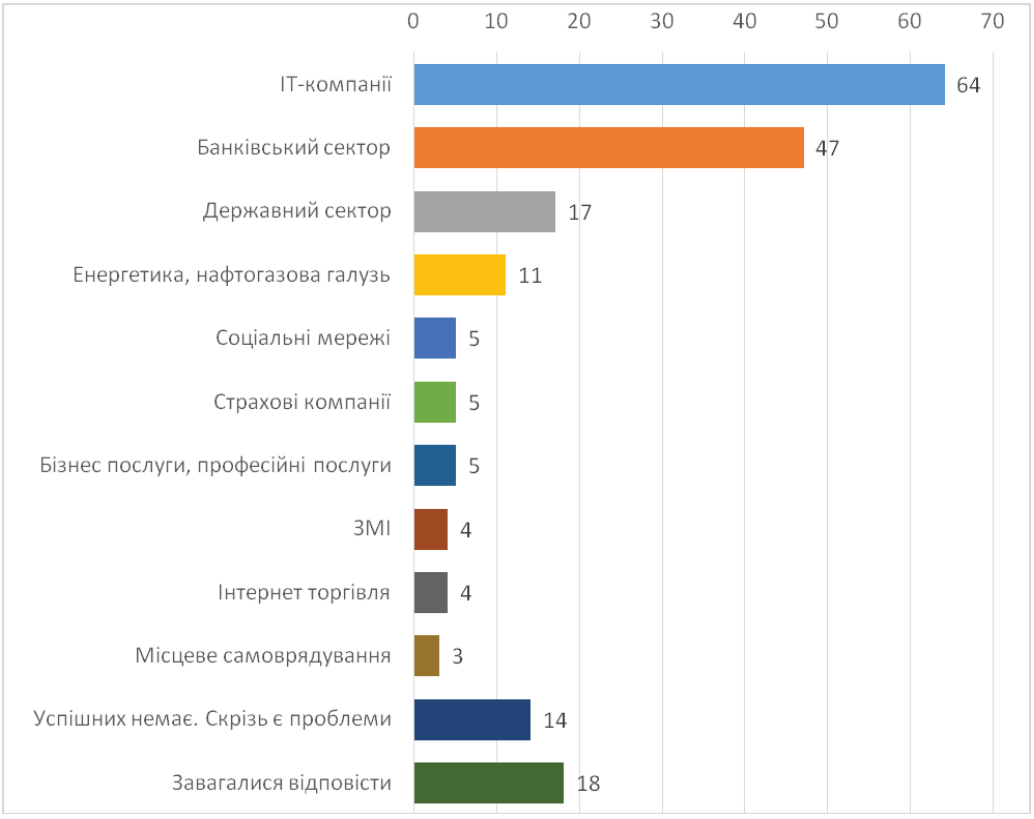

Рис. 2. Розподіл відповідей опитаних щодо галузі найбільш успішного протистояння кібератакам та витоку даних в Україні

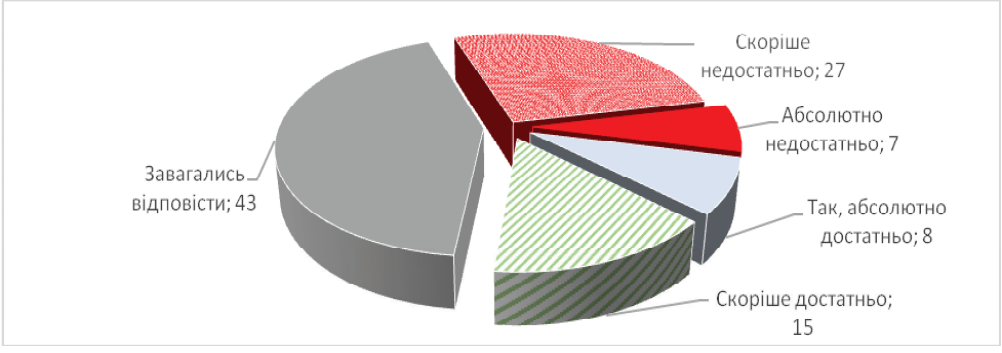

Рис. 3. Розподіл відповідей опитаних на запитання: "Чи достатньо фінансових ресурсів виділяє Ваша організація для забезпечення кібербезпеки?"

Серед причин такої ситуації опитані працівники органів публічного управління називають насамперед залежність їхнього бюджету від "головної організації". Позитивним моментом є той факт, що лише 5 % опитаних пра-

цівників "публічного сектору" вважають, що керівництво не приділяє цим питанням достатньої уваги. Узагальнюючи результати відповідей респондентів, можна зазначити перевагу об'єктивних чинників недофінансування над суб'єктивними.

Утім негативним моментом є те, що бюджети органів публічного управління щодо забезпечення кібербезпеки останніми роками не збільшилися. Така ситуація є гіршою порівняно з непублічною сферою, де майже чверть опитаних вказали на зростання витрат за цією статтею.

Ще одним недоліком у роботі органів публічного управління у сфері кібербезпеки є фактична відсутність профілактичної діяльності щодо кіберзахисту своїх підприємств. Лише 12 % працівників органів публічного управління вказали, що в їхніх організаціях проводяться регулярні тести щодо проникнення до баз даних інформаційних ресурсів. У недержавних установах цей показник понад удвічі вищий (27 %). При цьому більше половини опитаних у "публічному секторі" (61 %)взагалі не володіють інформацією з цього питання.

Також звернімо увагу на різницю у відповідях опитаних, які працюють у різних за чисельністю працівників організаціях. У "маленьких" (з чисельністю до 40 співробітників) на проведення тестування вказали 22 % опитаних. У "великих" (з чисельністю більше 40 співробітників) на реалізацію таких заходів вказали лише 14 % опитаних.

При цьому недостатньо поінформованими респонденти є про кіберінциденти на місці своєї роботи. Більшості опитаних (70 %) на момент проведення дослідження не було відомо про кібератаки на організації, у яких вони працюють (рис. 4).

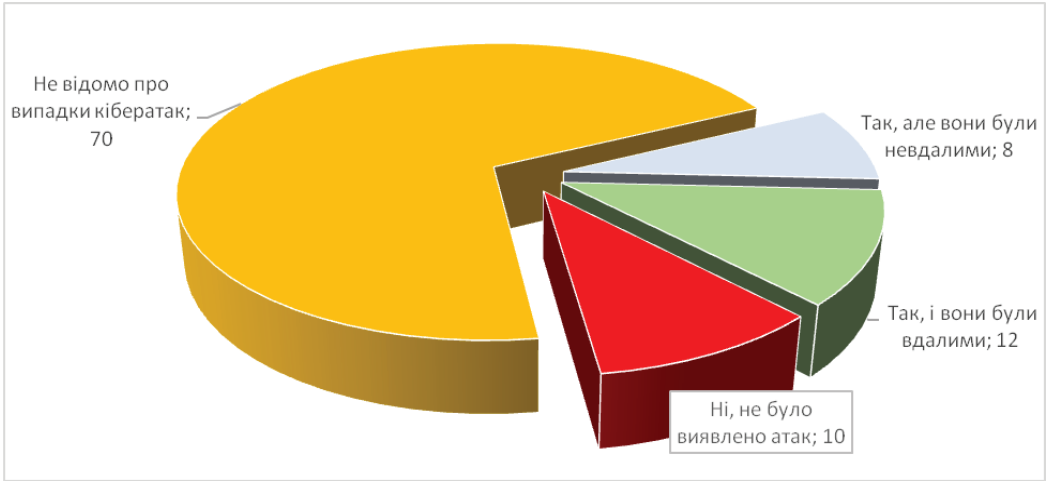

Рис. 4. Розподіл відповідей на запитання: "Чи можливим є здійснення кібератаки для отримання інформації, яку має право знати громадськість?"

Однак (з цього ж рис. 4) привертає увагу той факт, що 20 % організацій все ж таки зазнавали таких атак. Судячи з результатів опитування, більше загроз відчуває на собі "непублічний сектор".

За результатами опитування, можна визначити, що найбільшу цінність для здійснення кібератак у публічному секторі являють собою персональні дані працівників, а також дані, пов'язані з державною таємницею, у непублічному – дані фінансового характеру, а також матеріали, пов'язані з комерційною таємницею.

При цьому відносна більшість опитаних, які працюють і в публічній, і в непублічній сферах, погодилася з тим, що основні ризики, пов'язані з витоком інформації з їхньої організації, ідуть від особистої недбалості працівників організації. Хоча в цьому випадку на недбалості співробітників більше наголошують працівники "непублічного сектора".

Цікаво, що про особисту недбалість працівників також більше стверджують особи, які обіймають керівні посади (47 проти 32 % у рядових працівників).

Цікавим є і розподіл відповідей опитаних на запитання щодо чинників, які сприяють успішності проведення кібератак у публічному секторі. Більшість опитаних визначили, що це недосвідченість персоналу в питаннях кібербезпеки (54 %). Також значущими факторами є недостатня кількість інструментів для виявлення кібератак (61 %), недостатня захищеність інформаційних даних, мереж (58 %) і відсутність кваліфікованих фахівців з інформаційної безпеки (50 %). Привертають увагу певні відмінності у відповідях із цього питання працівників органів публічного управління та інших респондентів. Перші більше акцентують на відсутності в публічному секторі належних інструментів для виявлення кібератак та запобігання їм (об'єктивні чинники), другі – на відсутності підготовлених фахівців та недосвідченості персоналу у сфері кібербезпеки (суб'єктивні чинники).

Різними в державних та недержавних установах є і рівень володіння інформацією про реакції на такі атаки, а також способи реагування на кіберзагрози. Відмінним є і розуміння в різних організаціях політики щодо інцидентів у сфері кібербезпеки. Зокрема, 71 % працівників органів публічного управління невідомо про таку політику в своїх організаціях взагалі. На цьому тлі близько половини опитаних працівників "непублічної сфери" зазначили, що в їхніх організаціях такі інциденти фіксуються, класифікуються, а також вживається заходів щодо реагування на них.

З огляду на це не дивує й оцінка опитаними заходів, які проводить їхня організація щодо захисту своїх інформаційних ресурсів.

Лише 10 % опитаних працівників органів публічного управління визнали, що таких заходів достатньо. Це практично в три рази менше, ніж у "непублічному секторі". Привертає в черговий раз увагу і низький рівень обізнаності опитаних працівників органів публічного управління щодо кіберполітики своїх організацій (більше ніж половина респондентів не змогли оцінити заходи щодо кіберзахисту на своєму місці роботи).

Говорячи про шляхи підвищення рівня кібербезпеки своїх організацій, відносна більшість опитаних (47 %) погодилася з тим, що це має бути регулярне проведення контролю щодо встановлення оновлень програмного забезпечення. Також важливим опитані визнали регулярне проведення навчання працівників (38 %) і створення власного підрозділу із захисту інформаційних ресурсів (33 %).

Однак і в цьому підходи працівників "публічного сектору" і "непублічної сфери" істотно відрізняються. Працівники недержавних організацій порів-

няно більше акцентують на необхідності створення власного підрозділу щодо захисту інформаційних ресурсів, а також на перевірці ефективності заходів, які застосовувалося раніше для усунення виявлених недоліків.

Також думки опитаних розділилися у відповіді на запитання "Яку частину бюджету сучасна організація має витрачати для забезпечення ефективного захисту свого інформаційного простору?" (рис. 5). Відносна більшість опитаних вважає, що на це повинно йти до 30 % наявних коштів. Між тим серед працівників органів публічного управління є порівняно більшим усвідомлення необхідності збільшення фінансування заходів у сфері кібербезпеки.

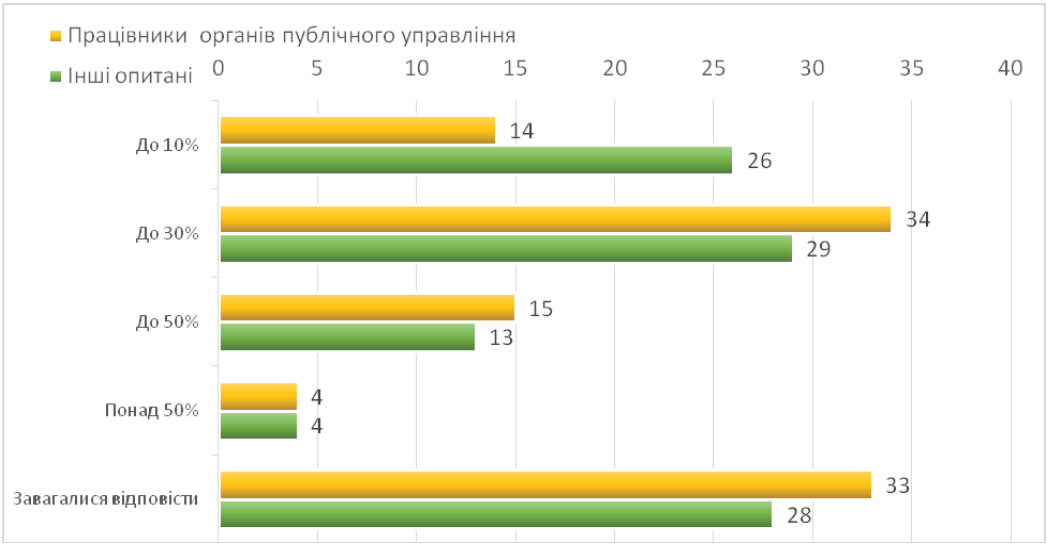

Рис. 5. Порівняльний розподіл відповідей респондентів на запитання "Яку частину бюджету сучасна організація має витрачати для забезпечення ефективного захисту свого інформаційного простору?" (у % до опитаних)

При цьому головними напрямами, на які необхідно спрямовувати кошти, респонденти назвали: сучасне ліцензоване програмне забезпечення, техніку й устаткування, навчання всіх працівників, а також оплату праці фахівців у сфері кібербезпеки.

Говорячи про пріоритетні напрями щодо інвестування (фінансування) для підвищення рівня кібербезпеки в країні в цілому, опитані звернули увагу насамперед на кібераналітику (69 %) і хмарні технології (50 %). У публічному секторі важливими було визнано інвестування в хмарні технології та машинне навчання (по 52% відповідно), на рівні окремих організаій – у кібераналітику (66 %) і хмарні технології (63 %).

Висновки з цього дослідження і перспективи подальших розвідок у цьому напрямі. Вищенаведене дозволяє дійти висновку про те, що публічний сектор має сьогодні неабиякі проблеми з фінансуванням сфери кібербезпеки і в цьому питанні значно поступається приватному. Це зумовлено як недосконалістю державної політики в цій сфері, так і високою вартістю відповідного обладнання і програм. Дослідження довело низький рівень кваліфікації працівників органів публічного управління щодо в цілому кіберпи-

тань та зокрема використання технологій організаційного і особистого кіберзахисту. Спільною для всіх осіб, які працюють в органах публічного управління, є також потреба в опануванні технологій електронного документообігу та онлайн-комунікацій, що пов'язано зі специфікою їхньої роботи.

Шляхами підвищення рівня кібербезпеки в публічному секторі є збільшення бюджетного фінансування відповідної сфери, стратегічне інвестування в кібераналітику і хмарні технології, створення в організаціях спеціальних підрозділів з кіберзахисту, встановлення сучасного програмного забезпечення та його постійне оновлення, регулярне підвищення кваліфікації всіх працівників із питань захисту організаційної та персональної інформації.

Список використаних джерел

1. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовт. 2017 р. № 2163-VIII. *ВВР України*. 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

Kotukh Ye. V.,
Phd of Technical Sciences, Associate Professor of Computer Science Department, Sumy State University, Sumy
ORCID 0000-0003-4997-620X

ASSESSMENT OF THE CYBER SPACE PROTECTION LEVEL IN PUBLIC GOVERNANCE: NATIONAL AND ORGANIZATIONAL DIMENSION

The article examines the features and main directions of cybersecurity in public administration. It is established that the state in general and public administration authorities, in particular, are not ready today to adequately respond to the main cyber threats related to information theft, financial fraud and hacker attacks.

The success of the implemented cybersecurity strategies depends on a clear justification of the feasibility of measures based on the identification of key issues in this area. In such conditions, a permanent assessment of the cyberspace protection level in public administration is necessary. In this regard, the aim of the article was to assess the current level of cyberspace protection in the public sector in the national and organizational dimensions, as well as to justify ways to increase cyber protection in the field of public administration.

In order to clarify the information about cybersecurity state in Ukraine in modern conditions, an all-Ukrainian expert sociological survey was conducted. The current cybersecurity state is analyzed, as well as ways to increase its level in the field of public administration at the national and organizational levels. The identified problems are due to the imperfection of public policy in this area, as well as the high cost of relevant equipment and programs. It is determined that common to all persons working in public administration is the need to master the technologies of electronic document management and online communications, which are related to the specifics of their work.

The priority ways to increase the level of cybersecurity in the public sector in modern conditions should be to increase budget funding, strategic investment in cyber analytics and cloud technologies, the creation of special units for cybersecurity, installation of modern software and its constant updating, regular training of employees involved in matters of organizational and personal information protection.

Keywords: level of cyberspace protection, cybersecurity, financing, public administration, hacker attacks.

References

1. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy vid 05.10.2017 r. № 2163-VIII. (2017). *VVR Ukrainy. 45, art. 403.* URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

Надійшла до редколегії 12.01.2021 р.