

**Довбиш Анатолій Степанович,**

*д.т.н., проф.,*

*завідувач кафедри комп'ютерних наук, завідувач лабораторії інтелектуальних систем,*

*Сумський державний університет,*

*м. Суми*

*ORCID 0000-0003-1829-3318;*

**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/ap.20.02.03

## СУЧАСНИЙ СТАН ТА ПРОБЛЕМИ “ЦИФРОВІЗАЦІЇ” В УКРАЇНІ

У статті досліджено особливості цифровізації в публічному управлінні, сформульовано основні напрями забезпечення кібербезпеки при цьому. З урахуванням комплексного науково-методологічного аналізу висвітлені окремі особливості організації комунікації суб'єктів публічного управління залежно від рівня та розміру організації. Проаналізовано сучасний стан кібербезпеки, а також визначено шляхи підвищення її рівня в сфері публічного управління та в цілому в Україні. Пріоритетним шляхами підвищення рівня кібербезпеки в публічному секторі в сучасних умовах має стати збільшення бюджетного фінансування відповідної сфери, стратегічне інвестування в кібераналітику і хмарні технології, створення в організаціях спеціальних підрозділів з кіберзахисту, установка сучасного програмного забезпечення та його постійне оновлення, регулярне підвищення кваліфікації всіх працівників з питань захисту організаційної та персональної інформації.

**Ключові слова:** цифровізація; забезпечення кібербезпеки; електронний уряд; організації публічного сектора; кіберзахист.

**Постановка проблеми.** Органи влади в Україні та багатьох країнах світу за останні десятиліття стали активними учасниками так званого “цифрового руху”. Це означає впровадження у сфері публічного управління різних способів цифровізації, які характеризуються певними інноваціями з боку органів влади, прозорістю процесів в них, співпрацею між ними і участю громадян. Однак у міру того, як все більше публічних організацій намагаються виправдати ці зростаючі очікування перетворення публічного управління, вони повинні вирішувати важливі питання своєї внутрішньої політики, особливо ті, що стосуються забезпечення безпеки загальнодоступних онлайн-даних й інформації, і все частіше організовувати тісну взаємодію між різними посадовими особами і співробітниками, а також з представниками громадськості.

**Аналіз останніх досліджень і публікацій.** Загальні науково-практичні засади кібербезпеки, її ролі у забезпеченні національної безпеки та цифровізації підлягали дослідженню у численних працях вітчизняних і зарубіжних науковців, зокрема, таких, як: С. Андреев, С. Домбровська, І. Діордіца, Є. Живило, З. Коваль, В. Куцаєв, В. Ліпкан, С. Срібний, В. Ткаченко, В. Шеломенцев та ін. Серед закордонних дослідників хотілося б окремо виділити праці Р. Азмі, К. Андреассона, Е. Камарка, П. Кеніса, К. Прована та ін.

**Метою статті** є оцінка сучасного стану кібербезпеки, а також шляхів підвищення її рівня в сфері публічного управління та в цілому в Україні.

**Виклад основного матеріалу дослідження.** Перш ніж перейти до викладу основних результатів проведеного дослідження, визначимо, що під нею цифровізацією розумілося насичення фізичного світу електронно-цифровими пристроями, засобами, системами та налагодження електронно-комунікаційного обміну між ними, що фактично уможливило інтегральну взаємодію віртуального та фізичного, тобто створює кіберфізичний простір [2].

З метою з'ясування інформації щодо стану кібербезпеки в Україні в сучасних умовах та пошуку шляхів підвищення рівня захисту кіберпростору в Україні у період з 24 жовтня по 3 листопада 2020 р. автором за сприяння кафедри політології та філософії Харківського регіонального інституту державного управління було проведено 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.

Виходячи з мети, було сформульовано такі основні завдання дослідження:

- оцінка нинішнього стану кібербезпеки (під якою 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, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [1, ст. 1]) в Україні в цілому, та на рівні окремих організацій і установ;

- визначення основних кіберзагроз для України в цілому, та для сфери публічного управління, зокрема,

- визначення рівня цифровізації публічного управління в Україні;

- з'ясування рівня “цифрової грамотності” працівників різних сфер;

- визначення основних чинників, що негативно впливають на рівень кібербезпеки України в цілому, та сфери публічного управління, зокрема;

- встановлення основних шляхів підвищення рівня кібербезпеки в Україні в цілому та у сфері публічного управління зокрема.

Загальна кількість респондентів на цьому етапі дослідження складала 1007 осіб. Відповідно до результатів опитування експерти розподілилися (у % до тих, які відповіли) за різними ознаками, зокрема за статтю (чоловіків – 30; жінок – 70); за віком (від 18 до 35 років – 27; від 36 до 45 років – 38; понад 46 років – 35) та іншими. Слід відмітити, що 81 % опитаних працюють в органах публічного управління. Далі всі цифри у наводяться у % до тих опитаних, які відповіли на запитання.

Оцінюючи ступінь розвитку цифровізації в Україні, відносна більшість експертів визначили його як середній (рис. 1).

Найнижче серед усіх категорій опитаних рівень “цифровізації” в Україні оцінили опитані, які працюють в приватному секторі економіки. Серед них 43 % визначили його як низький (у середньому по масиву 27 %) і лише 32 % як середній (відповідно 42 %).

Говорячи про відповідний рівень “цифровізації” у своєму місті /районі, експерти висловили схожі із попередніми оцінки. Однак у цьому разі привертає увагу відсутність істотної різниці в оцінках між мешканцями обласного центру і “провінції”.

Таким чином, можна стверджувати, що в межах всієї країни рівень “цифровізації” є приблизно однаковим.

Схожими є й думки респондентів щодо рівня розвитку електронного урядування в Україні (рис. 2). Відносна більшість опитаних визнає його середнім. При цьому оцінки експертів, що працюють в органах публічного управління, є більш високими у порівнянні з іншими опитаними (рис. 3).

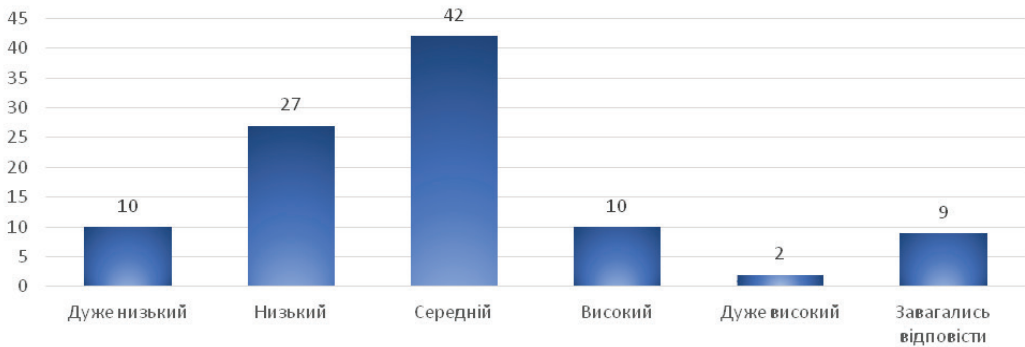


Рис. 1. Загальна оцінка рівня цифровізації в Україні

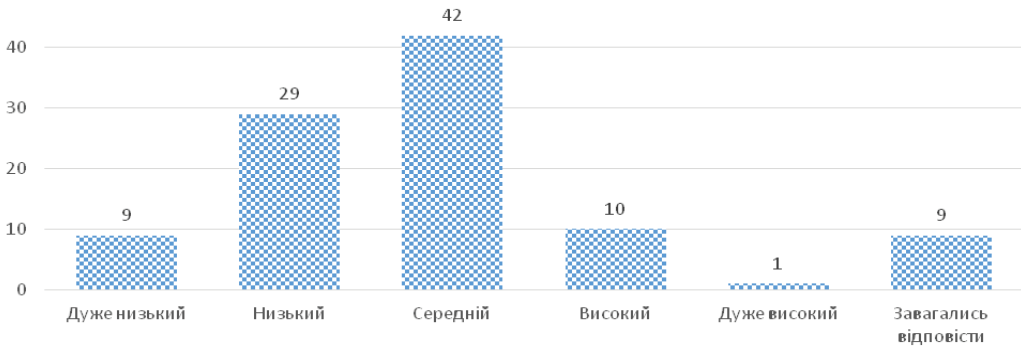


Рис. 2. Оцінка рівня розвитку електронного урядування в Україні

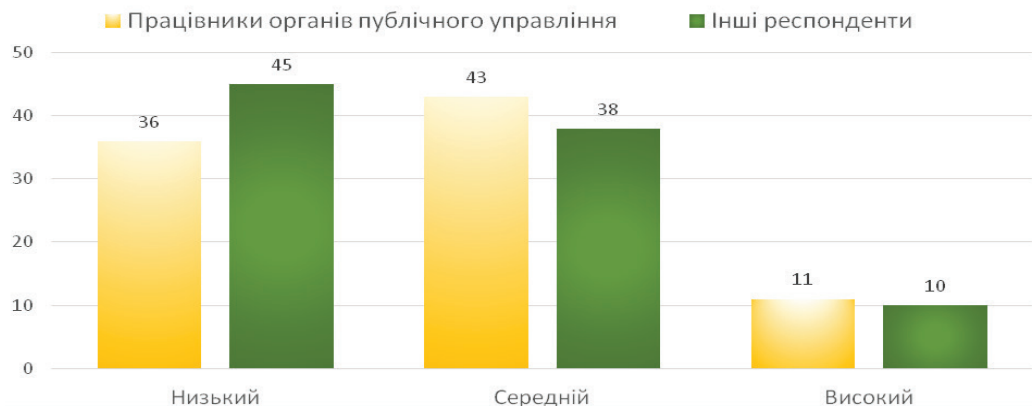


Рис. 3. Порівняльні оцінки рівня розвитку електронного урядування в Україні працівниками органів публічного управління та іншими експертами (у % до опитаних у кожній групі)

Середнім відносна більшість опитаних визнає і рівень розвитку електронного урядування у їхніх містах та районах.

Говорячи про окремі складові “цифровізації” та розвитку електронного урядування, привертають увагу як позитивні, так і негативні моменти.

Серед позитивного: переважна більшість опитаних (99 %), і зокрема, працівників органів публічного управління (99 %), мають на своєму робочому місці персональний комп’ютер. Однак рівень продуктивності комп’ютерів в “публічному секторі” значно поступається “приватному сектору”. Так, якщо в публічному секторі 36 % оцінили свій комп’ютер як продуктивний, то в приватному – 50 %.

Таким чином, можна констатувати перший негативний момент – рівень продуктивності комп’ютерів, що використовуються в роботі, в публічному секторі є нижчим, ніж у приватному.

Наступна проблема – це рівень забезпечення робочих місць організаційною технікою. В органах виконавчої влади та органах місцевого самоврядування він є значно гіршим порівняно з іншими організаціями та установами. Так, в органах публічного управління лише третина опитаних (33 %) зазначила, що у них є вся необхідна організаційна техніка. Серед інших експертів – таких більше половини (52 %).

Ще більш показовим є розрив в рівні продуктивності організаційної техніки між “публічним” та “приватним” сектором: рівень продуктивності комп’ютерної та організаційної техніки, якою користуються працівники органів публічного управління, є порівняно невисоким. А це, як наслідок, негативно впливає на якість їх праці.

Між тим, рівень вимог до працівників органів публічного управління останнім часом значно виріс. Як показало проведене дослідження, сучасні працівники органів публічного управління для ефективного виконання своїх функціональних обов’язків повинні володіти:

- технологіями електронного документообігу (90 %);
- електронним листуванням (74 %);
- технологіями он-лайн комунікації (65 %);
- інтернет-месенджерами (53 %).

Між тим, порівняння необхідного та наявного, тобто такого, що безпосередньо використовують працівники органів публічного управління в своїй роботі, визначає високий рівень їх потреб в удосконаленні вмінь щодо використання технологій електронного документообігу та онлайн комунікацій. Позитивним моментом і наслідком “цифровізації” та інформатизації суспільства стало майже повсюдне поширення інтернету. І у публічному, і у приватному секторі 92 % опитаних мають можливість виходу до всесвітньої мережі на своєму робочому місці. У той же час швидкість інтернету не скрізь є однаковою. Як доводять результати дослідження, в “публічному секторі” вона є порівняно низькою. При цьому у працівників, які займають керівні посади в своїх організаціях, швидкість інтернету є трохи вищою, ніж у рядових працівників.

Таким чином, за результатами проведеного дослідження, можна спостерігати цілу низку “цифрових нерівностей”, пов’язаних з різним рівнем забезпечення опитаних комп’ютерною та організаційною технікою, швидкістю інтернету та ін. Найбільш вразливою у цьому аспекті є категорія працівників органів публічного управління, які не займають керівні посади і працюють

невеличких містах, селищах і селах. При цьому спільною для всіх працівників органів публічного управління є потреба в опануванні технологій електронного документообігу та он-лайн комунікацій, а також в підвищенні рівня особистої захищеності в кіберпросторі (під яким в опитуванні розумілося середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних) [1, ст. 1].

Останню тезу підтверджують відповіді опитаних на запитання “Чи відчуваєте Ви себе безпечно в сучасному кіберпросторі?” (рис. 4).

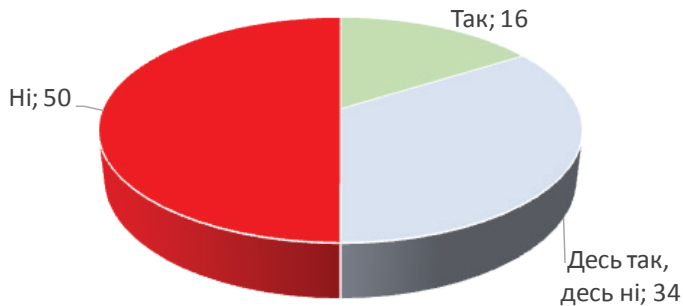


Рис. 4. Оцінка рівня особистої захищеності експертів в сучасному кіберпросторі

Цікаво, що найбільш захищеними себе почувають експерти віком до 35 років (21 % серед них відзначили цей факт).

Як наслідок, у всіх опитаних є достатньо високими потреби у знаннях і вміннях з кіберпитань (не вистачає – 16 % та важко сказати однозначно – 40 %). Більшими при цьому є потреби у таких знаннях, вміннях і навичках у працівників органів публічного управління (разом 47 %). Серед вікових категорій опитаних порівняно високий рівень потреб відзначається у опитаних віком понад 35 років (60 %). Як наслідок, не дивно, що значна кількість опитаних хотіли б підвищити свій рівень обізнаності з кіберпитань (83 %). Найбільше серед усіх категорій опитаних у цьому зацікавлені експерти віком понад 45 років (88 % у цій групі).

Серед знань, вмінь і навичок, найбільш затребуваними у опитаних виявилися у сфері технологій електронного документообігу (81 %). Серед працівників органів публічного управління, порівняно високими виявилися потреби у оволодінні технологіями он-лайн комунікацій (37 %). Що в цілому відповідає наведеним вище результатам і об'єктивно виявленим потребам.

При цьому опитані також дуже низько оцінюють рівень своїх знань, вмінь та навичок щодо захисту інформації своєї організації від кіберзагроз. Так, лише 21 % опитаних визнали його високим. У той же час більше третини опитаних (37 %) вважають його низьким або констатують повну відсутність таких знань. При цьому у працівників органів публічного управління рівень знань з питань протистояння організаційним кіберзагрозам є більш низьким порівняно з іншими респондентами.

Привертає увагу і низький рівень обізнаності з питань протидії організаційним кіберзагрозам у опитаних віком понад 35 років (рис. 5).

Негативно опитані оцінюють і рівень знань своїх колег з цього питання. Лише 16 % визнали його високим.

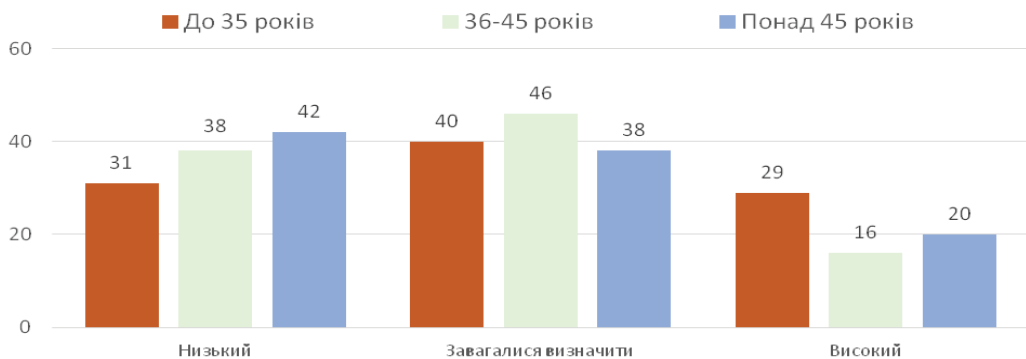


Рис. 5. Порівняльний розподіл відповідей на запитання “Яким є рівень Ваших знань, вмінь та навичок із захисту інформації Вашої організації від кіберзагроз” (у % до тих, які відповіли у кожній групі)

**Висновки з даного дослідження і перспективи подальших розвідок у даному напрямку.** За результатами проведеного опитування можна зробити висновки щодо оцінки сучасного стану кібербезпеки в Україні. Рівень цифровізації та інформатизації, а, відповідно, і розвитку електронного урядування є невисоким. Причинами цього виступають:

- незадовільне матеріально-технічне забезпечення органів публічного управління, зокрема, застарілість комп’ютерної та організаційної техніки;
- відсутність швидкісного інтернету, особливо невеличких містах, селищах і селах;
- недостатній рівень знань, вмінь і навичок, найбільш затребуваних у сфері технологій електронного документообігу та технологіях безпечних онлайн комунікацій, що обумовлено низьким рівнем обізнаності щодо сучасних засобів забезпечення кібербезпеки.

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, установка сучасного програмного забезпечення та його постійне оновлення, регулярне підвищення кваліфікації всіх працівників з питань захисту організаційної та персональної інформації.

#### Список використаних джерел

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення: 10.10.2020).
2. 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. URL: <https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text> (дата звернення: 14.10.2020).

**Dovbysh A. S.,**

*Doctor of Technical Science, Professor, Head of Computer Science Department,  
Head of Intellectual System Laboratory, Sumy State University, Sumy  
ORCID 0000-0003-1829-3318;*

**Kotukh Ye. V.,**

*PhD in Technical Sciences, Associate Professor of Computer Science Department,  
Sumy State University, Sumy  
ORCID 0000-0003-4997-620X*

## **CURRENT SITUATION AND PROBLEMS OF “DIGITALIZATION” IN UKRAINE**

The article examines the features of digitalization in public administration, formulates the main cybersecurity directions.

Modern “digital movement” means the introduction in the field of public administration of various methods of digitization, which are characterized by certain innovations by the authorities, the transparency processes inside the authorities, cooperation between last ones and citizens. More and more public organizations need to address important issues of their domestic policy, especially those related to the security of publicly available online data and information, and increasingly organize close cooperation between various officials and employees, as well as with members of the community.

Taking into account the complex scientific and methodological analysis, some features of the organization of communication of public administration bodies depending on the level and size of the organization are highlighted. The current situation with cybersecurity is analyzed, as well as ways to increase its level in the field of public administration in Ukraine. It is proved that the level of digitalization and informatization, and, accordingly, the development of e-government is low. The reasons for this are:

- unsatisfactory material and technical support of public administration bodies, in particular, obsolescence of computer and organizational equipment;
- lack of high-speed Internet, especially in small towns, villages and hamlets;
- insufficient level of knowledge, skills and abilities most in demand in the field of electronic document management technologies and secure online communication technologies, due to the low level of awareness of cybersecurity modern means.

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

**Keywords:** digitalization; providing cybersecurity; e-government; public sector organizations; cybersecurity.

### **References**

1. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy vid 05.10.2017 r. № 2163-VIII. (2017). *Vidomosti Verkhovnoi Rady Ukrainy*, 45, art. 403. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> [in Ukrainian].
2. Pro skhvalennia Konceptsii rozvytku tsifrovoi ekonomiky ta suspilstva Ukrainy na 2018-2020 roky ta zatverdzhennia planu zahodiv shodo ii realizacii: Rozporiadzhennia Kabinetu Ministriv Ukrainy vid 17.01.2018 r. № 67-r. (2018). URL: <https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text>.

*Надійшла до редколегії 14.10.2020 р.*