УДК 004.056:351.861
DOI 10.18372/2786-823.1.17497

Городянська Лариса Володимирівна
кандидат економічних наук, доцент, член-кореспондент АЕН України,
Київський національний університет імені Тараса Шевченко,
м. Київ, Україна
gorod_lv@knu.ua

РОЛЬ ЦИФРОВОЇ КОМПЕТЕНТНОСТІ ФАХІВЦЯ У СФЕРІ КІБЕРБЕЗПЕКИ В УМОВАХ ВОЄННИХ ЗАГРОЗ

Анотація. *У статті розкрито, що загрози в інформаційному світі можуть виникнути у будь-який момент «спілкування» з Інтернетом, де кіберзлочинці можуть скористатись доступом до конфіденційної інформації через фішинг-повідомлення електронної пошти, підробку паролів, або через пошкоджене обладнання. З метою підвищення обороноздатності України у кіберпросторі вкрай необхідно навчати фахівців сучасним методам кіберзахисту та формувати в них відповідні цифрові компетентності з урахуванням інструменту підвищення рівня обізнаності людини у галузі цифрових технологій (DigComp 2.0) та рекомендацій Європейського Парламенту й Ради.*

Ключові слова: *цифрова компетентність, кібербезпека, освітній процес, воєнні загрози.*

Annotation. *The article reveals that threats in the information world can arise at any moment of «communication» with the Internet, where cybercriminals can gain access to confidential information through a phishing email message, password forgery or damaged equipment. In order to increase the defense capability of Ukraine in cyberspace, it is necessary to train specialists in modern cyber defense methods and form their appropriate digital competencies in accordance with the Digital Competence Framework for Citizens (DigComp 2.0) and the Recommendation of the*

European Parliament and the Council.

Key words: *digital competence, cyber security, education process, military threats.*

Актуальність статті. Від початку анексії Криму відповідно до даних офіційної статистики Офісу Генерального прокурора України кількість кіберзлочинів у період з 2014 по 2021 роки зросла майже у 7,5 разів [1]. Лише за перший місяць війни, від початку повномасштабного вторгнення російської федерації до України, було зафіксовано 768 000 кібератак порівняно з 21 000 за 2021 рік, з яких 70-80 % є фішингом і перебором паролів [2]. За статистикою провайдерів, навіть станом на четвертий місяць війни, кількість атак зросла у 500-1000 разів. Цілями багатьох кібератак є енергетичні, телекомунікаційні, медіа та фінансові підприємства та інші об'єкти критичної інфраструктури України. Враховуючи, що це перша кібервійна у світі, для українців кібербезпека стає такою ж важливою, як Збройні Сили України.

Постановка проблеми. В умовах збройної агресії російської федерації для ефективності боротьби з кіберзлочинністю Уряд України прийняв низку нормативно-правових документів [3; 4]. Небезпека кіберзлочину пов'язана з викраденням або руйнуванням інформації в інформаційних системах і мережах, яка призводить до дестабілізуючих та деструктивних дій, спрямованих на людину, підприємство, регіон, державу. Під час війни кіберзлочини можуть спричинити виведення з ладу критично важливих державних підприємств, техніки, завдання матеріальної шкоди. Як приклад, Держспецзв'язку у квітні 2022 року повідомляло про надходження до українських користувачів електронних листів, відкриття яких призводило до отримання хакерами контролю над комп'ютером, загроз крадіжки та пошкодження даних [5].

Масовані кібератаки на об'єкти критичної інфраструктури України, починаючи з першого місяця війни, потребували впровадження дієвих кримінально-правових механізмів протидії кіберзлочинності [3; 4].

Дослідженню проблем зростаючих кіберзагроз до початку

повномасштабного вторгнення російської федерації до України присвячено роботи багатьох вчених. У працях зазначено, що ризик наразитися на кіберзагрози, пов'язаний з витоком комерційної або конфіденційної інформації, суттєво зростає зі збільшенням кількості пристроїв в мережі, а також з поширенням в бізнесі хмарних обчислень. Разом з цим, порівняння досвіду і рівня знань українських фахівців, які займаються впровадженням сучасних технологій кіберзахисту, із рівнем знань фахівців США чи Європи показав, що за цим показником Україна знаходиться на рівні 2015 року [2], що є недостатнім з урахуванням збройної агресії російської федерації та масованих кібератак на об'єкти критичної інфраструктури України.

З метою підвищення обороноздатності України у кіберпросторі необхідно навчати фахівців сучасним методам кіберзахисту та формувати в них відповідні цифрові компетентності.

Метою статті є визначення ролі цифрової компетентності фахівця у сфері кібербезпеки в умовах воєнних загроз.

Результати дослідження. Після перших місяців збройної агресії російської федерації ворог почав здійснювати масовані фішингові атаки й змінювати тактику ведення кібервійни. Відтепер відбувається цілеспрямований фішинг як на підприємства критичної інфраструктури, так і на користувачів. Варто зазначити, що фішинг є атакою, спрямованою не на технологію, а саме на людину. Це латентні загрози проти людини, які важко стовідсотково розпізнати. В умовах сучасної війни застосовується зброя, використання якої потребує відповідних цифрових знань, умінь та навичок людини під час її взаємодії з цифровими технологіями. Отже, зростає роль людини, яка набула відповідних цифрових компетентностей після навчання, підвищення кваліфікації.

Перелік ключових компетентностей людини, які варто набувати й оновлювати в процесі навчання та/або протягом усього життя, наведені у Рамковій програмі Європейського Союзу (ЄС). Згідно з рекомендаціями ЄС ключові компетентності визначаються як комбінація знань, навичок та ставлень. Згідно із Законом України «Про освіту» компетентність – це динамічна

комбінація знань, умінь, навичок, способів мислення, поглядів, цінностей, інших особистих якостей, що визначає здатність особи успішно соціалізуватися, провадити професійну та/або подальшу навчальну діяльність [6].

Інтелектуальний потенціал людини відображає її здатність оволодіти набором ключових компетентностей, необхідних не лише для особистісного розвитку та конкурентоспроможності, а й для збереження суверенітету країни. В умовах сучасних загроз важливими є такі компетентності людини, як її обізнаність у цифрових технологіях, підприємливість, критичне мислення, вміння вирішувати проблеми та навчатися. В умовах війни критично важливу роль серед низки ключових компетентностей набуває цифрова компетентність людини, яка здатна забезпечувати власний розвиток і набувати вмінь і навичок за широким спектром складових від медіаграмотності, опрацювання та критичного оцінювання інформаційних даних, до знань у сфері кі бербезпеки з метою успішного вирішення виробничих завдань підприємства.

Цифрова компетентність фахівця – це складне динамічне цілісне інтегративне утворення особистості, яке є його багаторівневою професійно особистісною характеристикою в сфері цифрових технологій і досвіду їхнього використання, що обумовлене з одного боку потребами та вимогами цифрового суспільства, а з іншого появою цифрового освітнього простору, який змінює освітню (навчально-виховну) взаємодію всіх її учасників [7]. Цифровий освітній простір характеризується широким залученням мережі Інтернет, цифрових систем зберігання та первинної систематизації даних, а також автоматизованих цифрових аналітичних систем (на основі нейромереж та штучного інтелекту), що дозволяє ефективніше здійснювати професійну діяльність та водночас потребує постійного професійного саморозвитку.

Цифрова грамотність або цифрова компетентність визнана ЄС однією з 8 ключових компетенцій, необхідних для повноцінного життя. У 2016 році ЄС представив оновлений DigitalCompetence (DigComp 2.0). DigComp 2.0 – це європейська система цифрової компетентності, яка є інструментом підвищення рівня компетентності людини у галузі цифрових технологій [8, с. 2].

Концептуальна еталонна модель DigComp 2.0 для Системи цифрової компетентності громадян складається з 5 блоків компетенцій [8, с. 8].

Опис цифрової компетентності фахівця розроблено відповідно до Європейських рамкових документів про цифрову компетентність – DigComp 2.0: Система цифрової компетентності громадян [8], DigComp 2.1: Рамка цифрових компетенцій для громадян із вісьмома рівнями кваліфікації та прикладами використання [9]. Відповідно до рекомендацій документів [10; 11] із врахуванням особливостей [8; 9] сформовано складові цифрової компетентності:

- знання базових функцій та використання різних пристроїв, програмного забезпечення й цифрових мереж;

- здатність створювати цифровий контент (включаючи програмування) та медіаконтент;

- вміння захищати інформацію, особисті дані та забезпечувати умови, пов’язані з кібербезпекою;

- знання правових та етичних принципів, пов’язаних із використанням цифрових технологій.

В Україні ІТ-фахівців випускають більше 100 вищих навчальних закладів. Рейтинги ВНЗ за рівнем підготовки фахівців із інформаційних технологій за 2013 рік свідчать, що існуюча в Україні система ІТ-освіти не задовольняє вимоги ІТ-індустрії за необхідними обсягами та якістю підготовки ІТ-фахівців [12]. Наявні кваліфікації подані в Національному класифікаторі України ДК003:2010 «Класифікатор професій». Їх перелік відстає від поточних потреб ІТ-індустрії в ІТ-кадрах. Проблема формування комплексних знань, навичок і умінь фахівця у сфері цифрової компетентності, які є необхідними для роботи з мережею Інтернет та дотримання цілей безпеки, реалізації державних і громадських проектів з підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту є актуальною як на макро-, так і на мікрорівні та має відбуватись за активної підтримки держави.

Висновки. Визначено сучасну роль цифрової компетентності фахівця в умовах війни та масованих кібератак на критично важливі об'єкти України. Зокрема, аналіз ступеня задоволеності підприємств рівнем підготовки вітчизняних фахівців із інформаційних технологій та результати кібератак 2022 року свідчать про недостатній рівень кваліфікації та про важливість формування цифрових компетенцій людини відповідно до європейської системи цифрової компетентності (DigComp 2.0) та з урахуванням рекомендацій Європейського Парламенту й Ради [10]. Спираючись на ці документи сформовано цифрові компетентності фахівця у сфері кібербезпеки, рівень кваліфікації яких важливо підтримувати упродовж всього життя.

Список використаних джерел

1. Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування. *Офіс генерального прокурора* : веб-сайт. URL: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2 (дата звернення: 26.10.2022).

2. Осіпова В. Фахівці з кіберзахисту, чиї рішення використовує уряд України, - про «першу кібервійну у світі» та безпеку держпідприємств. *DOU* : веб-сайт. URL: https://dou.ua/lenta/interviews/first-cyber-war/ (дата звернення: 21.10.2022).

3. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану : Закон України від 24 березня 2022 р. № 2149-IX. URL: https://zakon.rada.gov.ua/laws/show/2149-20#Text (дата звернення: 26.10.2022).

4. Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування» за гарячими сдідами та протидії кібератакам : Закон України від 15 березня 2022 р. № 2137-IX. URL: https://zakon.rada.gov.ua/laws/show/2137-20#Text (дата звернення: 26.10.2022).

5. Нова кібератака групиArmageddonна державні органи України.

Державна служба спеціального зв'язку та захисту інформації: веб-сайт. URL: https://cip.gov.ua/ua/news/uvaga-nova-kiberataka-grupi-armageddon-na-derzhavni-organi-ukrayini (дата звернення: 26.10.2022).

6. Про освіту : Закон України від 05 верес. 2017 р. № 2145-VIII. URL: https://zakon.rada.gov.ua/laws/show/2145-19#Text (дата звернення: 26.10.2022).

7. Опис цифрової компетентності педагогічного працівника : *електронне наукове фахове видання «Відкрите освітнє е-середовище сучасного університету»*/ Морзе Н. та ін. URL: https://doi.org/10.28925/2414-0325.2019s39 (дата звернення: 26.10.2022).

8. DigComp 2.0: Система цифрової компетентності громадян : звіт за проектом «Наука для політики». Етап 1 оновлення: концептуальна еталонна модель / Вуорікарі Р., Пюні І., Карретеро С., Бранде Л. Європейська Комісія : Об'єднаний дослідницький центр, 2016. 41 с. URL: https://binpo.com.ua/wp-content/uploads/2021/04/DigComp-2.0-%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0-%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%BE%D1%97-%D0%BA%D0%BE%D0%BC%D0%BF%D0%B5%D1%82%D0%B5%D0%BD%D1%82%D0%BD%D0%BE%D1%81%D1%82%D1%96-%D0%B3%D1%80%D0%BE%D0%BC%D0%B0%D0%B4%D1%8F%D0%BD.pdf (дата звернення: 26.10.2022).

9. Карретеро С., Вуорікарі Р., Пюні Ю. DigComp 2.1: Рамка цифрових компетенцій для громадян із вісьмома рівнями кваліфікації та прикладами використання. Люксембург: Офіс публікацій Європейського Союзу, 2017. URL: https://publications.jrc.ec.europa.eu/repository/handle/JRC106281 (дата звернення: 26.10.2022).

10. Recommendation of the European Parliament and of the Council of 22 May 2018 on Key Competences for Lifelong Learning. Official Journal of the European Union. 2018. 4.6. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018H0604(01)&rid=7 (дата звернення: 26.10.2022).

11. Державний стандарт базової та повної загальної середньої освіти : затверджений Постановою КМУ від 23.11.2011 № 1392. URL: https://zakon.rada.gov.ua/laws/show/1392-2011-%D0%BF#Text/ (дата звернення: 26.10.2022)

12. Рейтинг вищих навчальних закладів України “Компас-2013” : звіт. Компания «Систем Кепітал Менеджмент», 2013. URL: http://bestuniversities.com.ua/sites/default/files/compas2013.pdf (дата звернення: 26.10.2022).