

ДЕРЖАВНА КІБЕРОСВІТА ТА ІНСТРУМЕНТИ ПІДВИЩЕННЯ РІВНЯ ЦИФРОВОЇ КОМПЕТЕНТНОСТІ НАСЕЛЕННЯ УКРАЇНИ

О. В. Карпенко,
Національна академія державного управління при Президентові України
Л. А. Арсенович,
Національна академія державного управління при Президентові України

У статті обґрунтовано необхідність формування системи державної кіберосвіти в Україні. Сформульовано потреби в опануванні базових цифрових компетенцій, визначено складові навчання у сфері кібербезпеки, запропоновано механізми підвищення загального рівня цифрової компетентності населення, а також визначено пріоритетні шляхи розвитку системи державної кіберосвіти. Запропоновано практичні рекомендації профільним (зацікавленим) центральним органам виконавчої влади щодо підвищення рівня цифрової компетентності населення України.

Ключові слова: кібербезпека; кіберзахист; кіберосвіта; цифрова компетентність; цифрові компетенції; цифрова гігієна; цифрові трансформації.

STATE CYBER EDUCATION AND TOOLS FOR THE UKRAINE POPULATION' DIGITAL COMPETENCE LEVEL INCREASING

O. V. Karpenko,
National Academy for Public Administration under the President of Ukraine
L. A. Arsenovych,
National Academy for Public Administration under the President of Ukraine

The article substantiates the necessity of forming a state cyber education system in Ukraine. The requirements for mastering basic digital competences have been formulated, the components of cybersecurity training have been identified, the mechanisms for increasing the general level of the population digital competence have been proposed, as well as the priority ways of state cyber education system development. Practical recommendations are offered to specialized (interested) central executive authorities on improving the population digital competence level in Ukraine.

Keywords: cyber security; cyber defence; cyber education; digital competence; digital competencies; digital hygiene; digital transformations.

Постановка проблеми у загальному вигляді та її зв'язок з важливими науковими та практичними завданнями. Питання кібербезпеки актуалізуються з розвитком глобальних мереж, оскільки сучасним трендом стають цифрові технології, а соціальні мережі формують нове суспільне середовище.

Шлях розвитку України в розбудові власної системи кібербезпеки потребує ґрунтовних й невідкладних змін на основі застосування науково обґрунтованих управлінських рішень. Така необхідність сучасних трансформацій у системі кіберзахисту органів публічної влади спричинена збільшенням кількості кібератак та багатьма іншими інцидентами, які упродовж останніх п'яти років перетворили Україну на кіберполігон геополітичного протистояння.

Діапазон небезпек кіберпростору постійно розширюється. Якщо на початку ХХІ ст. інформаційні небезпеки можна було типологізувати за кількома складовими, то на сьогодні розмаїття

усіляких кіберзагроз неухильно збільшується, зачіпаючи при цьому права людини в інтернеті. Особливо гострою ця проблема стає при використанні соціальних мереж. Крім того, потребує вирішення проблема розвитку та впровадження цифрових технологій як в освіті, так і в побуті для громадян, на чому акцентується увага наукової спільноти як в Україні, так і за її межами.

У кіберзагрозливому середовищі визначальним стає навчання всіх учасників мережевої взаємодії для опанування навичок кібергігієни. Різноманітну інформацію щодо кіберзагроз і можливих негативних наслідків їх впливу на діяльність будь-якої людини необхідно підкріплювати моделюванням тих чи інших ситуацій, що можуть виникати в процесі мережевої взаємодії.

Рівень обізнаності населення щодо питань кібербезпеки повинен не лише відповідати сучасним потребам у розвитку цифрового суспільства, а й підвищувати довіру кожного користувача до інформації в мережі, забезпечувати належними

© Карпенко О. В., Арсенович Л. А., 2020

знаннями про кібербезпеку та цифрову гігієну (культуру) у соцмережах, здатність належним чином використовувати сучасні цифрові технології, сервіси та програми.

Зазначене потребує вдосконалення, передусім, нормативно-правового забезпечення цієї сфери. Зміни в законодавстві є однією з передумов підвищення ефективності процесу навчання населення основам кібербезпеки та створення відповідних напрямів для набуття професійних компетенцій (практичних знань і навичок) у світі цифрових технологій.

Рівень цифрової компетентності (грамотності) населення є проблемним питанням пов'язаним, з провадженням системи кібербезпеки в Україні. У контексті проведення реформ публічного управління, навчання (підготовка, спеціалізація та підвищення кваліфікації) основам і технологіям кібербезпеки, безпечної роботі з інформацією (даними) під час виникнення інцидентів кібербезпеки це питання набуває особливої актуальності та потребує окремого ґрунтовного дослідження.

Аналіз останніх публікацій за проблематикою та визначення невирішених раніше частин загальної проблеми. З охопленням цифровими технологіями майже всіх сфер життєдіяльності суспільства опанування навичок цифрової гігієни та кібербезпеки стало визначальною ознакою професійної компетентності у сфері безпеки життєдіяльності людини.

За останні п'ять років в Україні кількість злочинів у сфері персональних даних зросла більш ніж у 2,5 рази. Серед найпоширеніших кіберзлочинів є незаконне отримання доступу до персональних даних та банківських рахунків, викрадення паролів та іншої цифрової інформації користувачів мережі «Інтернет». Потерпілими можуть стати як юридичні особи, державний сектор, бізнес, так і пересічні громадяни. Встановлено, що різке підвищення рівня кіберзлочинності починається з 2017 р., коли за ст. 361 Кримінального кодексу України (несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електров'язку) було зафіксовано 1795 відкритих кримінальних справ, у 2018 р. – 1023, а в 2019 р. – понад 2000 (Хакери в ударі, 2019). З метою запобігання підвищенню рівня кіберзлочинів у країнах ЄС приймаються національні та регіональні програми, створюються відповідні центри, реалізуються заходи щодо спільних дій, затверджуються стандарти тощо.

Так, за останні роки у Польщі формується та реалізується послідовна державна політика запо-

бігання кіберзагрозам, де важливим здобутком є ухвалення відповідних змін до законодавства. Зокрема, 5 липня 2018 р. Президент Польщі підписав Закон про національну систему кібербезпеки (O krajowym systemie, 2018), положення якого в тому числі регулюють діяльність, пов'язану з освітніми програмами, проведення національного навчання у сфері кібербезпеки, наукових досліджень і розробок у сфері цифрових трансформацій та підвищення рівня обізнаності населення з питань кібергігієни.

У Швеції 17 листопада 2017 р. ухвалено Стратегію кібербезпеки (A national cyber, 2016), яка передбачає навчання як публічних службовців, так і пересічних громадян.

Для забезпечення належного рівня кіберзахисту громадян необхідно підвищувати рівень їх обізнаності та грамотності у сфері цифрової безпеки, однак ця проблематика й надалі залишається малодослідженою в галузі публічного управління. У контексті нашого дослідження необхідно виділити публікації В. Бурячка (2013), І. Діордіці (2016), О. Корченка (Ознаковий принцип, 2010), С. Мельника (2016), Г. Почепцова (2013), М. Погорецького (Погорецький, Шеломенцев, 2009), які розглядають питання цифрових трансформацій суспільства та окремі аспекти професійної підготовки фахівців у сфері кібербезпеки. Водночас слід констатувати, що питання підготовки, спеціалізації та підвищення кваліфікації публічних службовців у сфері кібербезпеки України залишилося не охопленим комплексними науковими дослідженнями галузі науки державного управління. На практиці це може призвести до недооцінення ролі цифрових трансформацій у суспільстві, які є одним із сучасних трендів діяльності української влади у процесі провадження національної безпеки України.

Формулювання цілей (мети) статті. Метою статті є визначення механізмів підвищення рівня цифрової компетентності населення в рамках реалізації системи державної кіберосвіти в Україні.

Виклад основних результатів та їх обґрунтування. Цифрові та мережеві технології постійно трансформуються, але не завжди користувачі мають належну спроможність щодо їх ефективного використання. Останнім часом зростаюча кількість кібератак на пересічних користувачів у мережі «Інтернет» свідчить про низький загальний рівень їх цифрової грамотності, а також про нестачу кваліфікованих фахівців у сфері кібербезпеки.

За прогнозами фахівців (Разрыв в навыках, 2017), «дефіцит» спеціалістів у сфері кібербезпеки у 2022 р. досягне рівня 1,8 млн осіб. Є різні

концепції та пропозиції щодо запобігання виникненню цієї проблеми, наприклад через підвищення кваліфікації вже працюючих співробітників органів публічної влади, недержавних організацій та бізнес-структур або через застосування алгоритмів штучного інтелекту. Однак, на нашу думку, лише довгострокова стратегія розвитку кіберосвіти, яка буде зорієнтована на підготовку та спеціалізацію майбутніх поколінь українських користувачів мережевих технологій, дасть змогу забезпечити достатню кількість кваліфікованих кадрів, які професійно володітимуть необхідними цифровими компетенціями (навичками).

На сьогодні в Україні впровадження кіберосвіти для широких верств населення фактично перебуває лише на початковому етапі. Приватні компанії вже друге десятиріччя організують та проводять навчання своїх співробітників навичкам кібербезпеки, безпечній роботі з інформацією в інтернеті та правилам поведінки під час виникнення інцидентів кібербезпеки за аналогією з навчанням правилам протипожежної безпеки чи цивільного захисту, яке проводиться у всіх державних закладах України. Лише за ініціативою деякої невеликої кількості українських та міжнародних громадських організацій, що опікуються питаннями кіберосвіти українців (наприклад громадська організація «Українська академія кібербезпеки», Київське відділення міжнародної громадської організації «ISACA»), комерційних тренінгових центрів (наприклад Академія CISCO, IT Education Academy), в останні роки започатковані та ефективно проводяться відповідні навчальні курси, але більшість з них розрахована на студентів та фахівців з вищою технічною освітою. Наразі важливим є запровадження такого навчання для всього населення, оскільки рівень цифрової грамотності (компетентності) українців на сьогодні недостатній.

Так, 24 грудня 2019 р. у своїй промові Прем'єр-міністр України О. Гончарук під час презентації проекту «Дія. Цифрова освіта» зазначив, що за результатами досліджень, 53 % українців володіють цифровими навичками нижче від середнього (базового) рівня (Мінцифри запустило, 2019). При цьому цифрові нововведення освоює переважно молодь, а громадяни літнього віку неохоче сприймають гаджети та важко адаптуються до цифрового світу. Однак і вони поступово розуміють, що державні послуги цифровізуються, а за допомогою мережевих технологій простіше комунікувати в суспільстві.

Нормативно-правовою основою підвищення рівня цифрових компетенцій населення стали: Стратегія кібербезпеки України, затверджена Ука-

зом Президента України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року “Про Стратегію кібербезпеки України”» від 15 березня 2016 р. № 96 (Про рішення Ради, 2016), Концепція розвитку цифрової економіки та суспільства України на 2018–2020 роки, схвалена розпорядженням Кабінету Міністрів України від 17 січня 2018 р. № 67-р, в якій зазначено, що створення та виконання національної програми навчання загальним і професійним цифровим компетенціям та знанням є пріоритетним завданням на шляху до прискореного розвитку цифрової економіки (Про схвалення Концепції, 2018).

І хоча окремої державної програми (стратегії) щодо запровадження державної кіберосвіти в Україні не існує, в Програмі діяльності Кабінету Міністрів України, затвердженій 29 вересня 2019 р., заплановано, що 70 % із 6 млн українців, які будуть охоплені програмою розвитку цифрових навичок, володітимуть ними на базовому рівні. Так, у п. 14.3 міститься проєкт Концепції державної політики щодо досягнення цілі «Українець, який хоче мати цифрові навички, може їх вільно набути», згідно з якою подальшими запланованими діями стане:

- створення повної екосистеми з реалізації політики цифрової освіти – онлайн-платформи з доступними курсами цифрової грамотності в п'яти різних категоріях, що завжди будуть доступними (безкоштовними) для українців;
- здійснення підготовки персоналу, який працюватиме з населенням в офлайн та надаватиме онлайн-підтримку;
- проведення на місцевому рівні тижнів цифрової грамотності та відповідних регіональних форумів із зазначеного питання;
- створення великої власної, партнерської та волонтерської мережі;
- проведення першої масштабної інформаційної кампанії із залученням національного та регіонального телебачення тощо (Програма діяльності, 2019).

Залежність суспільства від цифрових технологій стає все відчутнішою, а тому й рівень технологічності кібератак підвищується з такою швидкістю, що марно сподіватися на ефективний захист з допомогою лише наявних антивірусних програм. На сьогодні збільшується кількість атак, пов'язаних з уведенням людини в оману шляхом захоплення її персональних даних. Передусім громадян потрібно навчати розпізнавати кібератаки зловмисників і не реагувати на листи, дзвінки та SMS-повідомлення від шахраїв, які намагаються різними хитрощами заволодіти па-

ролями до мережевих чи банківських акаунтів. Крім того, в більшості користувачів існує потреба в освоєнні базових навичок цифрової гігієни, таких, як: безпечне налаштування мобільного телефону, домашнього інтернету та смартпристроїв, які до нього підключені, користування WI-FI, розпізнавання небезпечних сайтів, використання паролів високого рівня складності тощо. Зазначимо, що таке масове навчання основам цифрової гігієни може проводитися тільки на добровільних засадах, оскільки сучасний темп життя не дає змоги розраховувати на те, що звичайна людина витратить на це більше ніж 10–15 хв на добу. Тому людей необхідно зацікавити, передусім пояснивши на простих прикладах, чому правильне застосування у повсякденній діяльності цифрових технологій є серйозним питанням та стосується кожного з них. Для цього з 21 січня 2019 р. Міністерство цифрової трансформації України (далі – Мінцифра) започаткувало курси з цифровізації населення, які будуть реалізовуватись у форматі серій токшоу, де запрошеним у студію експертам українці зможуть поставити актуальні запитання щодо кібербезпеки та цифровізації (Мінцифра запустило, 2019). На нашу думку, Мінцифра повинна поширювати навчальні матеріали у форматі коротких відео, інтерактивних цифрових курсів, що оздоблені анімаціями, які повинні проходити в ігровій формі, динамічно, мати сучасний, привабливий вигляд. Звичайно, це повинна бути не «пам'ятка» з безпеки, а, наприклад, трихвилинний відеоролик (мініфільм), або навіть ще коротший за тривалістю одноквилинний «вайн» (від англ. vine), де висвітлюється історія звичайної людини, яка стала жертвою кібершахраїв. У такому візуалізованому навчальному матеріалі на простих, взятих з життя прикладах, повинні роз'яснюватися правила цифрової гігієни із зазначенням інформації про те, яким чином можна запобігти кібершахрайству та кібератакам. Навчання має бути доступним у будь-який час, будь-де, з мобільних пристроїв та стаціонарних комп'ютерів.

На сучасному етапі цифрових трансформацій в Україні для популяризації основних засад кібергігієни та підвищення рівня кіберграмотності корисним було б створення окремого інформаційного ресурсу у вигляді порталу з навчання базовим навичкам кібербезпеки населення, де будуть поширюватися навчальні матеріали і в разі необхідності можна отримати як онлайн-консультацію фахівця, так і можливість комунікувати користувачам між собою з актуальних питань протидії хакерам та злочинцям завдяки його представленню у со-

ціальних мережах «Фейсбук» та «Твітер». Українською важливо, щоб державна програма кіберосвіти була максимально ефективною для забезпечення навчання якомога більшої кількості громадян. Це має бути не тільки портал з навчальними матеріалами, а саме освітня програма, яка буде побудована за всіма сучасними трендами, включаючи цікавий та сучасний контент, інтерактивні онлайн-курси, сучасні методики просування кібертехнологій та використання різноманітних каналів і методів навчання для різних категорій населення.

Подібні програми існують у США та інших країнах. Наприклад, за допомогою загальнонаціональної кампанії з підвищення обізнаності громадськості «Stop.Think.Connect», серед користувачів проводиться відповідна робота щодо розуміння кіберзагроз, що дає можливість американській громадськості почуватися безпечніше в мережі «Інтернет». Як зазначено на державному порталі www.dhs.gov, вказана кампанія спонукає американців розглядати безпеку інтернету як «спільну відповідальність вдома, на роботі та в інших інформаційних спільнотах» (CISA).

Підвищення рівня цифрової компетентності (грамотності) громадян та кіберкультури, набуття комплексних знань, навичок щодо поведінки в кіберпросторі, впровадження державних і громадських проєктів з підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту є пріоритетами провадження кібербезпеки України, затвердженими Стратегією кібербезпеки України (Про рішення Ради, 2016).

Першим кроком має бути розробка структури програми кіберосвіти, в якій будуть визначені базові цифрові навички, канали і методи навчання для різних цільових аудиторій («профілів» громадян). Наприклад, для цільової аудиторії віком понад 60 років навчання може проводитися не тільки через інтернет, а й через телерадіомовлення та друковані засоби масової інформації. Ці канали інформування наразі залишаються популярними серед людей поважного віку, які тільки нещодавно почали використовувати сервіси мережі «Інтернет» та мобільних телефонів.

Іншою важливою цільовою аудиторією стають діти та підлітки, для яких необхідно створювати мобільні ігри, що в розважальній формі навчатимуть їх необхідним навичкам цифрової гігієни. Знайомство з цифровими технологіями та передовими смартметодами в ранньому віці сприятиме поглибленому опануванню громадянами віком від 6 до 14 років тих компетенцій, які в майбутньому стануть необхідними для поповнення професіоналами (людськими ресурсами) кіберіндустрії.

Однак не менш важливим є й формування кіберкультури дітей та підлітків. Сучасне молоде покоління формує свій світогляд в епоху цифрових трансформацій, а тому перебуває в ідеальних умовах розвитку, оскільки має більше можливостей для отримання знань та обґрунтування варіантів вирішення проблем, пов'язаних з кібербезпекою, які в майбутньому позитивно позначаться на їх працевлаштуванні. З правилами кібергігієни молодь потрібно знайомити ще в початковій школі, як, наприклад, зараз це відбувається з правилами безпечної поведінки на дорозі. Недосконалість сучасних навчальних програм має місце й у викладанні шкільного курсу інформатики, оскільки даються взнаки відсутність серед учителів відповідних фахівців, незадовільна технічна організація навчального процесу (скажімо, як розглядати тему «Електронне листування» в сільській школі за відсутності звичайного комп'ютера або підключення до мережі «Інтернет») та громіздка програма навчання (навіть «розвантажена» програма шкільної інформатики, кілька офіційних предметних олімпіад та неофіційних учнівських конкурсів не зможуть охопити обсяг шкільного курсу інформатики) (Сучасна освіта).

Опанування цифрових технологій учителями відкриє для них нові можливості у викладанні, даючи змогу разом з учнями отримувати задоволення від процесу навчання комунікування з учнями та пізнання. Такі інноваційні технології дадуть змогу вчителю цифровізувати більшу частину своєї роботи, вивільняючи час на пошук інформації, спілкування, самовдосконалення, індивідуальну роботу з учнями, забезпечать зворотний зв'язок, підвищать ефективність управління навчальним процесом та освітою в цілому (Про схвалення Концепції, 2018). Це також дасть педагогам можливість виявляти таланти дітей на ранній стадії і вдосконалювати їхні вміння та майстерність.

В Україні необхідно сформувати не просто культуру безпечного поведіння з інформацією, а й суспільну цифрову культуру. Звичайно, це стає стратегічною метою, на реалізацію якої буде витрачено не один рік. Цифрова культура передбачає передачу знань шляхом соціального навчання – люди навчаються від інших людей або передають навички через цифрові артефакти. Так, створення українського комедійного серіалу з кібербезпеки із залученням професійних акторів, у якому би висміювалися нехтування засобами цифрової гігієни та небезпечна поведінка користувачів у кіберпросторі, стало б яскравою ілюстрацією формування цифрової культури в

Україні. Прикладом цього є британський телесеріал «Айтішники», сюжет якого розвивається навколо витівок команди з технічної підтримки вигаданої британської корпорації та який у комедійному стилі поширює знання з безпеки користування цифровими технологіями та інтернетом.

До соціального навчання слід віднести й розвиток мережі волонтерських організацій, які допомагатимуть громадянам опановувати навички кібербезпеки. Подібна програма існує у США, де таких волонтерів називають «Посланцями безпеки» (Security Ambassadors). Так, слід зазначити, що і в українському інформаційному просторі діють волонтерські організації «Українські кібервійська» та «Кіберальянс», які спеціалізуються на проведенні оборонних і наступальних операцій в інтернеті з метою протидії сепаратистам і терористам під час ведення інформаційних воєн проти України (Інформаційне агентство «Уніан»). Разом з тим зауважимо, що діяльність таких волонтерських організацій не сприяє розвитку кіберосвіти населення України.

Велике значення для формування кіберкультури, просвітницької діяльності у сфері цифрових трансформацій має практика відзначення в суспільстві професійних свят. Прикладом таких свят в Україні є «День безпечного інтернету», святкування якого започатковано за ініціативою європейських некомерційних організацій European SchoolNet та Insafe, який відзначається щороку у другий вівторок лютого. День безпечного інтернету має на меті долучити до співпраці дітей і молодь, батьків та вчителів, науковців і соціальних працівників, працівників ІТ-індустрії та публічних службовців, заохочуючи їх брати участь у забезпеченні комфортного користування інтернетом шляхом формування навичок цифрової грамотності та вивчення питань використання технологій, пов'язаних із кібербезпекою (Центр кращого інтернету). Постійними організаторами заходів для дітей та молоді до Дня безпечного інтернету в Україні є Міністерство освіти і науки України, Державна наукова установа «Інститут модернізації змісту освіти» та низка організацій і закладів освіти, які організують та проводять різноманітні освітні заходи. Звичайно, на сьогодні організація таких освітніх заходів потребує передусім проведення загальноукраїнської комунікативної кампанії та залучення більшої кількості органів влади, закладів вищої освіти, недержавних організацій та волонтерів, які пропагуватимуть у суспільстві питання розвитку сфер кібербезпеки та цифрових трансформацій.

Зрозуміло, технічні знання необхідні. Однак комунікативні навички не повинні залишатися поза увагою держави, оскільки вважаються не менш важливими в галузі кібербезпеки. Водночас, поки ця тема перебуває на стадії розгляду та впровадження, необхідно, щоб фахівці з кібербезпеки розробили відповідні етичні стандарти, потрібні для ефективної роботи в цій галузі. Рішенням для усунення цифрового розриву в навичках сфери цифрової безпеки є кіберосвіта не тільки для фахівців закладів вищої освіти, а й для всього населення України. Важливо, щоб держава масштабно здійснювала освітню та просвітницьку діяльність серед населення через започаткування національної навчальної програми кіберосвіти, яка забезпечить кожному людину базовим рівнем компетентності. Поза всякими сумнівами є те, що за умов належної побудови навчальної програми майбутні професіонали будуть залучені до продукування нових можливостей, які існують в індустрії кібербезпеки. Враховуючи зазначене, слід наголосити, що без навчання громадян основам цифрової гігієни та кібербезпеки «держава в смартфоні» може стати найбільшим розчаруванням українців.

Висновки та перспективи подальших досліджень. Унаслідок стрімкого поширення цифрових трансформацій цифрові навички стають визначальними серед інших професійних компетенцій громадян. Так, цифровізація на сьогодні є головним трендом на загальному ринку праці. Інакше кажучи, вміння працювати із цифровими технологіями поступово стає постійним та необхідним для всього населення країни.

Цифрова грамотність визнана Європейським Союзом однією з восьми ключових компетенцій для повноцінного життя та діяльності людини в умовах сьогодення. Держава має запровадити національну програму кіберосвіти й навчати населення загальним та професійним цифровим навичкам, що важливо в контексті побудови цифрової економіки та суспільства. Український політикум та зацікавлені центральні органи виконавчої влади повинні створити та в подальшому координувати відповідні ініціативи щодо реалізації кіберосвіти. Наразі сфера державної кіберосвіти в Україні фрагментарна та хаотична, застарілі методики викладання, відсутність

Список використаних джерел

Хакери в ударі: в Україні вдвічі зросла кіберзлочинність. Сайт інформаційного агентства «Сьогодні». 21 жовт. 2019 р. URL: <https://www.segodnya.ua/ua/economics/enews/hakery-v-udare-v-ukraine-vdvoevyrosla-kiberprestupnost-1348336.html> (дата звернення: 26.01.2020).

відповідної законодавчої бази та стандартів, недостатність підготовлених викладачів, а також недоступність цифрових технологій призвели до недостатнього рівня цифрової грамотності населення України.

Для реалізації основних засад Стратегії кібербезпеки України та Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки необхідно розробити практичні рекомендації (алгоритм дій) органам публічної влади з метою підвищення рівня цифрової компетентності населення України та реалізації кіберосвіти в цілому.

Ураховуючи зазначене та беручи до уваги наявність недоліків у законодавстві стосовно навчання населення цифровим навичкам, вважаємо за доцільне запропонувати Міністерству освіти і науки України, Міністерству цифрової трансформації України, Адміністрації Держспецзв'язку розглянути питання щодо розроблення відповідного нормативного акта, положеннями якого передбачатиметься:

- забезпечення умов для формування та розвитку державної кіберосвіти населення України на центральному, регіональному та місцевому рівнях;
- збільшення обсягів державного замовлення для підготовки фахівців у галузі кібербезпеки;
- упровадження програм з перекваліфікації (перепідготовки) тимчасово непрацюючих з числа колишніх військовослужбовців та учасників бойових дій;
- вжиття заходів щодо профорієнтації в закладах початкової, середньої та вищої освіти для виявлення обдарованих дітей, учнів та студентів для роботи у сфері кібербезпеки;
- розробка національного стандарту цифрової компетентності;
- оновлення державного класифікатора професій через розроблення та затвердження переліку «цифрових» професій (на основі вимог ринку праці, «цифрових» трендів), а також введення посад та підрозділів кіберзахисту в органах публічної влади.

Цифрова компетентність населення є основою побудови цифрової економіки та суспільства. Громадяни України вже перебувають у цифровому світі. Наступним кроком держави повинно стати провадження безпечного користування цифровими технологіями в кіберпросторі.

References

Khakery v udari: v Ukraini vdvichi zrosla kiberzlochynnist (2019). Sait informatsiinoho ahentstva «Sohodni». Retrieved from: <https://www.segodnya.ua/ua/economics/enews/hakery-v-udare-v-ukraine-vdvoevyrosla-kiberprestupnost-1348336.html> (Accesed: 26 January 2020).

- О krajowym systemie cyberbezpieczeństwa: USTAWA z dnia 5 lipca 2018 r. Poz. 1560. *Dziennik Ustaw Rzeczypospolitej Polskiej*. URL: <http://dziennikustaw.gov.pl/DU/2018/1560> (дата звернення: 26.01.2020).
- A national cyber security strategy. *Government Office of Sweden*. 2016. URL: <https://www.government.se/legal-documents/2017/11/skr.-201617213/> (дата звернення: 26.01.2020).
- Бурячок В. Л. Основи формування державної системи кібернетичної безпеки: монографія. Київ: НАУ, 2013. 432 с.
- Діордіца І. Стан підготовки фахівців у сфері кібербезпеки. *Visegrad Journal on Human Rights*. 2016. № 6/1. P. 59–65. URL: http://vjhr.sk/archive/2016_6/part_1/11.pdf (дата звернення: 26.01.2020).
- Ознаковий принцип формування класифікацій кібератак / О. Г. Корченко та ін. *Вісник Східноукр. нац. ун-ту імені Володимира Даля*. 2010. № 1. С. 32–38.
- Мельник С. Концептуальні основи організації професійної підготовки майбутніх фахівців із кібербезпеки. *Педагогічні науки: теорія, історія, інноваційні технології*. 2016. № 10. С. 79–88. URL: http://nbuv.gov.ua/UJRN/pednauk_2016_10_9 (дата звернення: 26.01.2020).
- Почепцов Г. Г. Смыслові та інформаційні війни. *Інформаційне сусп-во*. 2013. Вип. 18. С. 21–27. URL: http://nbuv.gov.ua/UJRN/is_2013_18_6 (дата звернення: 26.01.2020).
- Погорецький М. А., Шеломенцев В. П. Поняття кіберпростору як середовища вчинення злочину. *Інформаційна безпека людини, суспільства, держави*. 2009. № 2 (2). С. 80.
- Разрыв в навыках кибербезопасности: обучение следующего поколения. Хостинг-провайдер «King Servers». 2017. URL: <https://habr.com/ru/company/kingservers/blog/342070/> (дата звернення: 26.01.2020).
- Мінцифри запустить для українців курси з цифровізації у форматі токшоу. Електрон. інформ. ресурс ЛБ. ua. 2019. URL: https://ukr.lb.ua/society/2019/12/24/445703_mintsifri_zapustit_ukraintsiv.html (дата звернення: 26.01.2020).
- Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15.03.2016 № 96/2016. Офіц. вебсайт Верхов. Ради України. URL: <https://zakon5.rada.gov.ua/laws/show/96/2016> (дата звернення: 26.01.2020).
- Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки та затвердження плану заходів щодо її реалізації: Розпорядж. Каб. Міністрів України від 17.01.2018 № 67-р. Офіц. вебсайт Верхов. Ради України. URL: <https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80> (дата звернення: 26.01.2020).
- Програма діяльності Кабінету Міністрів України. *Урядовий портал*. 2019. URL: <https://program.kmu.gov.ua/meta/ukrainec-akij-hoce-mati-cifrovi-navicki-moze-ih-vilno-nabuti> (дата звернення: 26.01.2020).
- USTAWA (2018). O krajowym systemie cyberbezpieczeństwa: z dnia 5 lipca 2018 r. Poz. 1560. *Dziennik Ustaw Rzeczypospolitej Polskiej*. Retrieved from: <http://dziennikustaw.gov.pl/DU/2018/1560> (Accessed: 26 January 2020).
- A national cyber security strategy (2016). *Government Office of Sweden*. Retrieved from: <https://www.government.se/legal-documents/2017/11/skr.-201617213/> (Accessed: 26 January 2020).
- Buriachok, V. L. (2013). *Osnovy formuvannia derzhavnoi systemy kibernetichnoi bezpeky* [Fundamentals of formation of the state system of cyber security]. Kyiv [in Ukrainian].
- Diorditsa, I. (2016). Stan pidhotovky fakhivtsiv u sferi kiberebezpeky [Status of cybersecurity training]. *Visegrad Journal on Human Rights*. Retrieved from: http://vjhr.sk/archive/2016_6/part_1/11.pdf (Accessed: 26 January 2020).
- Korchenko, O. H., Patsira, Ye. V., Hnatiuk, S. O., Kinzeriavyy, V. M., Kazmirchuk S. V. (2010). Oznakovyi pryntsyyp formuvannia klasyfikatsii kibereatak [Essential principle of formation of cyberattack classifications]. *Visnyk Skhidnoukrainskoho natsionalnoho universytetu imeni Volodymyra Dalia*. № 1. P. 32–38 [in Ukrainian].
- Melnyk, S. (2016). Kontseptualni osnovy orhanizatsii profesiinoi pidhotovky maibutnikh fakhivtsiv iz kiberebezpeky [Conceptual bases for the organization of professional training of future cybersecurity professionals]. *Pedahohichni nauky: teoriia, istoriia, innovatsiini tekhnolohii*. N 10. P. 79–88. Retrieved from: http://nbuv.gov.ua/UJRN/pednauk_2016_10_9 (Accessed: 26 January 2020).
- Pochepstov, H. H. (2013). Smyslovi ta informatsiini viiny [Meaningful and informational wars]. *Informatsiine suspilstvo*. Vup. 18. P. 21–27. Retrieved from: http://nbuv.gov.ua/UJRN/is_2013_18_6 (Accessed: 26 January 2020).
- Pohoretskyi, M. A. & Shelomentsev, V. P. (2009). Poniattia kibereprostoru yak seredovyshcha vchynennia zlochynu [The concept of cyberspace as a medium of crime], *Informatsiina bezpeka liudyny, suspilstva, derzhavy*. N 2 (2). P. 80 [in Ukraine].
- Razryv v navykakh kiberebezopasnosti: obuchenie sleduyushhego pokoleniya (2017). *Khosting-provayder «King Servers»*. Retrieved from: <https://habr.com/ru/company/kingservers/blog/342070/> (Accessed: 26 January 2020).
- Mintsyfry zapustyt dlia ukraintsiv kursy z tsyfrovizatsii u formati tok-shou (2019). *Elektronnyi informatsiyni resurs LB. ua*. Retrieved from: https://ukr.lb.ua/society/2019/12/24/445703_mintsifri_zapustit_ukraintsiv.html (Accessed: 26 January 2020).
- Ukaz Prezydenta Ukrainy (2016). Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 27 sichnia roku «Pro Stratehiu kiberebezpeky Ukrainy». Retrieved from: <https://zakon5.rada.gov.ua/laws/show/96/2016> (Accessed: 26 January 2020).
- Rozpopriadzhennia Kabinetu Ministriv Ukrainy (2018). Pro skhvalennia Kontseptsii rozvytku tsyfrovoy ekonomiky ta suspilstva Ukrainy na 2018–2020 roky ta zatverdzhennia planu zakhodiv shchodo yii realizat-

CISA: about the Campaign. Stop.Think.Connect. Official website of the Department of Homeland Security. URL: <https://www.dhs.gov/about-stopthinkconnect> (дата звернення: 26.01.2020).

Сучасна освіта. Osvita.ua. URL: <https://osvita.ua/school/method/46851/> (дата звернення: 26.01.2020).

Інформатика в початкових класах. URL: <https://sites.google.com/site/informatikavpocatkovi/hk/pro-osoblivosti-vikladanna-informatiki-v-pocatkovij-skoli> (дата звернення: 26.01.2020).

Інформаційне агентство «Уніан». URL: <https://www.unian.ua/economics/finance/1371476-ukrajinski-it-volonteri-zablokuvali-na-rahunkah-terroristiv-13-milyoniv.html> (дата звернення: 26.01.2020).

Центр кращого інтернету. URL: <https://betterinternetcentre.org/?p=463> (дата звернення: 26.01.2020).

sii. Retrieved from: <https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80> (Accessed: 26 January 2020).

Prohrama diialnosti Kabinetu Ministriv Ukrainy (2019). *Uriadovyi portal*. Retrieved from: <https://program.kmu.gov.ua/meta/ukrainec-akij-hoce-mati-cifrovi-navicki-moze-ih-vilno-nabuti> (Accessed: 26 January 2020).

CISA: about the Campaign (2019). Stop.Think.Connect. Official website of the Department of Homeland Security. Retrieved from: <https://www.dhs.gov/about-stopthinkconnect> (Accessed: 26 January 2020).

Suchasna osvita. Osvita.ua. Retrieved from: <https://osvita.ua/school/method/46851/> (Accessed: 26 January 2020).

Informatyka v pochatkovykh klasakh. Retrieved from: <https://sites.google.com/site/informatikavpocatkovi/hk/pro-osoblivosti-vikladanna-informatiki-v-pocatkovij-skoli> (Accessed: 26 January 2020).

Informatsiine ahentstvo «Unian». Retrieved from: <https://www.unian.ua/economics/finance/1371476-ukrajinski-it-volonteri-zablokuvali-na-rahunkah-terroristiv-13-milyoniv.html> (Accessed: 26 January 2020).

Tsentr krashchoho internetu. Retrieved from: <https://betterinternetcentre.org/?p=463> (Accessed: 26 January 2020).

Карпенко Олександр Валентинович, доктор наук з державного управління, доцент, завідувач кафедри інформаційної політики та цифрових технологій, Національна академія державного управління при Президентіві України, 03057, Україна, м. Київ, вул. Антона Цедіка, 20
Арсенович Леонід Антонович, аспірант кафедри інформаційної політики та цифрових технологій, Національна академія державного управління при Президентіві України, 03057, Україна, м. Київ, вул. Антона Цедіка, 20

Цитування: Карпенко О. В., Арсенович Л. А. Державна кіберосвіта та інструменти підвищення рівня цифрової компетентності населення України. *Вісн. НАДУ. Серія «Державне управління»*. 2020. № 1 (96). С. 95–102.

Стаття надійшла: 10.02.2020

Схвалено до друку: 18.02.2020

Karpenko, Oleksandr V., Doctor of Science in Public Administration, Associate Professor, Head of Information Policy and Digital Technologies Department, National Academy for Public Administration under the President of Ukraine, 20, Anton Tsedyk St., Kyiv, 03057, Ukraine
Email: dr.karpenko@ukr.net
<http://orcid.org/0000-0002-9301-7973>
Arsenovych, Leonid A., Ph.D student of Information Policy and Digital Technologies Department, National Academy for Public Administration under the President of Ukraine, 20, Anton Tsedyk St., Kyiv, 03057, Ukraine
E-mail: arsen-leon@ukr.net
<http://orcid.org/0000-0001-7081-2838>

Citation: Karpenko, O. V., Arsenovych, L. A. (2020). Derzhavna kiberosvita ta instrumenty pidvyshchenni rivnia tsyfrovoi kompetentnosti naselennia Ukrainy [State cyber education and tools for the ukraine population' digital competence level increasing]. *Bulletin of the NAPA. Series «Public Administration»*. Is. 1 (96). P. 95–102 [in Ukrainian].

Article arrived: 10.02.2020

Accepted: 18.02.2020