КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3(15), 2022
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2022.15.93109
УДК 35.088.6:[004:007:351.86] (477)

Арсенович Леонід Антонович
доктор філософії з галузі публічне управління та адміністрування,
заступник начальника управління – начальник відділу Департаменту кадрової роботи та управління персоналом,
Адміністрація Державної служби спеціального зв'язку та захисту інформації України, м. Київ, Україна
ORCID ID: 0000-0001-7081-2838
arsen-leon@ukr.net

ІНСТРУМЕНТАРІЙ ПІДВИЩЕННЯ РІВНЯ ЦИФРОВОЇ КОМПЕТЕНТНОСТІ ФАХІВЦІВ ІЗ КІБЕРБЕЗПЕКИ В ОСВІТНЬОМУ ПРОЦЕСІ

Анотація. У статті проаналізовано вітчизняні та зарубіжні напрацювання щодо проблем формування цифрової компетентності та ефективного використання інформаційних технологій у навчанні. Розглянуто складові цифрової компетентності, які передбачають впевнену, критичну і відповідальну взаємодію з цифровими технологіями для навчання, роботи та участі у житті суспільства. Наведено результати глобального дослідження з інформаційної безпеки, а також опитування працівників провідних кіберкомпаній у всьому світі, у тому числі в Україні, які вказують на подальшу необхідність застосування та впровадження комплексного підходу у сфері освіти, із використанням організаційних заходів, програмно-технічних засобів і процесів управління на всіх рівнях діяльності будь якої організації, а також відповідного інструментарію задля підвищення рівня цифрової компетентності. Сформульовано сутність значення цифрових інструментів сфери кібербезпеки, яке має на увазі сукупність інтернет-засобів (ресурсів) для захищеності суб'єктів мережевого середовища від різних видів інформаційних та кіберзагроз, забезпечення належної організації протидії їхньому впливу, формування, функціонування й еволюції кіберпростору, а також розвитку освітніх кібертехнологій та інформаційного суспільства в цілому. Проаналізовано, виділено та запропоновано три основні групи цифрових інструментів сфери кібербезпеки (професійні кіберінструменти, інструменти кіберосвіти та комунікативні кіберінструменти), які надають можливість використовувати, доступатись, фільтрувати, оцінювати, створювати, програмувати та поширювати цифровий контент, керувати та захищати інформацію, вміст, дані та цифрові ідентичності, а також ефективно працювати з програмами, пристроями, штучним інтелектом та роботами тощо. Доведено, що на сьогодні робота з цифровими кіберінструментами та їх вмістом вимагає рефлексивного та критичного і водночас допитливого, відкритого та перспективного ставлення до їх розвитку, а також етичного, безпечного, ефективного та відповідального підходу до їх використання.

Ключові слова: фахівці із кібербезпеки; цифрова грамотність; цифрова компетентність; цифрові інструменти; цифрові технології.

ВСТУП

Сучасна безпекова ситуація як у державі, так і світі в цілому кардинально змінюється, що є поштовхом для появи якісно нових регуляторів, які у своєму арсеналі матимуть ефективні важелі впливу на суспільні і соціальні відносини в кібернетичній сфері. Ключовим завданням державної кібербезпекової політики дедалі виразніше виступає створення гарантованих умов реалізації національних інтересів у сфері освіти.

Стрімке поширення цифрових технологій в усіх сферах сучасного суспільства потребує якісної підготовки професійних ІТ-фахівців, які формують нову генерацію представників високотехнологічного соціуму, здатну зберігати та обробляти інформацію у кіберпросторі та протистояти несанкціонованому втручанню в інформаційне

середовище. Важливість збереження конфіденційності інформації, гострий дефіцит у кадровому забезпеченні ІТ-сфери України, а також нещодавнє запровадження нової спеціальності «Кібербезпека» галузі знань «Інформаційні технології» актуалізують необхідність створення ефективної та дієвої системи підготовки фахівців у сфері кібербезпеки, і перш за все в органах державної влади України.

Постановка проблеми. В умовах розбудови цифрового світу та розвитку інформаційних технологій особливого значення набувають питання професійної підготовки спеціалістів ІТ-сфери, і перш за все фахівців із кібербезпеки органів державної влади України.

Зовнішні та внутрішні загрози у безпековому середовищі України актуалізують потребу підвищення рівня професійної компетенції фахівців, які в умовах протидії збройній агресії Російської Федерації опікуються питаннями кібербезпеки та кіберзахисту державних інформаційних ресурсів.

Аналіз останніх досліджень і публікацій. Наукові напрацювання вчених і практиків засвідчують, що професійна підготовка фахівців у сфері кібербезпеки є одним із напрямів державної політики у сферах національної безпеки і оборони, без якого є неможливими захищене передавання інформації і відповідно – науково-технічний та соціально-економічний розвиток країни. На основі вивчення академічних праць з'ясовано, що в умовах інформаційних війн, замахів на цілісність і суверенітет української держави питання підготовки фахівців із кібербезпеки вміщають в себе проблеми педагогічного, системного і міждисциплінарного характеру.

Як свідчать останні дослідження і публікації, проблеми професійного розвитку фахівців з кібербезпеки є малодослідженими. Так, І. Діордіца у своїх статтях досліджує питання стандартизації підготовки фахівців із кібербезпеки та здійснює аналіз стану підготовки фахівців у сфері кібернетичної безпеки станом на 2015–2016 роки [1]. С. Мельник у науковій роботі визначає концептуальні основи організації професійної підготовки майбутніх фахівців із кібербезпеки у вищих навчальних закладах. А група науковців у складі В. Бурячка, І. Пархомея, М. Степанова та В. Толубка у своїй статті вивчає проблемні питання та актуальні завдання підготовки фахівців з кібернетичної безпеки галузі знань «Інформаційні технології».

На теперішній час підготовка висококваліфікованих кадрів залишається ключовим елементом повноцінної життєдіяльності держави. Цей процес характеризується поєднанням потреб суспільства з сучасними інформаційними технологіями із подальшим закріпленням на рівні нормативно-правових актів.

Процес професійної підготовки фахівців кібербезпеки в Україні проходить період становлення та потребує досліджень і стандартизації. На наш погляд, аналіз чинних нормативно-правових актів і напрацювань сучасних науковців у сфері кібербезпеки, враховуючи деякі прогалини у законодавстві, надасть змогу розкрити дефініцію «цифрові інструменти сфери кібербезпеки», що у подальшому дозволить визначити основні шляхи удосконалення підготовки професіоналів обраного профілю.

Метою дослідження є здійснення систематизації та групування цифрових інструментів підвищення рівня професійної компетентності фахівців із кібербезпеки в освітньому процесі.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Питання кібербезпеки актуалізуються з розвитком глобальних мереж, оскільки сучасним трендом стають цифрові технології, а соціальні мережі формують нове суспільне середовище. Шлях розвитку України у розбудові власної системи кібербезпеки

потребує ґрунтовних й невідкладних змін на основі застосування науково-обґрунтованих управлінських рішень. Така необхідність сучасних змін у системі кіберзахисту органів публічної влади спричинена збільшенням кількості кібератак та багатьма іншими інцидентами, які протягом останніх п’яти років перетворили Україну на кіберполігон геополітичного протистояння [2, с. 95].

Забезпечення безпеки інформаційного простору є одним із найбільш важливих чинників стимулювання економічного зростання та розвитку громадянського суспільства, зайнятості населення, розширення конкуренції і, як наслідок, сприяння подоланню так званого «цифрового розриву». З огляду на міжнародний досвід розвиток цифровізації суспільного життя є одним з основних факторів забезпечення успішності реформування та підвищення конкурентоспроможності країни. Реформа будь-якої галузі в сучасних умовах спрямована на широке використання сучасних інформаційно-комунікаційних технологій для досягнення необхідного рівня ефективності та результативності. Адже саме цифрові технології здатні забезпечити значне покращення якості обслуговування фізичних і юридичних осіб та підвищення відкритості, прозорості та ефективності діяльності органів державної влади та органів місцевого самоврядування. Крім того, запровадження цифрових технологій публічного управління є базовою передумовою для розбудови в Україні ефективних цифрової економіки і цифрового ринку та її подальшої інтеграції до єдиного цифрового ринку ЄС.

Наскрізним викликом для України є збільшення темпів розвитку цифрових технологій, прискорення інновацій шляхом використання цих технологій, а також величезна потреба у висококваліфікованих кадрах для перетворення економіки країни в умовах цифрової нерівності. Ключовим викликом є неготовність українського суспільства до «цифрового виклику», а саме недостатність фахових цифрових компетенцій для більшої частини працездатного населення. Потребує врегулювання питання щодо великої кількості вакансій для працівників із цифровими навичками та не працевлаштованих соціально активних громадян, у яких відсутні ці навички. Під час переходу в режим онлайн економічної діяльності, освіти, медичного обслуговування, ІТ-сфери, державних і фінансових послуг перед значними прошарками громадян постають цифрові бар’єри для повноцінного життя.

Цифрові та мережеві технології постійно розвиваються, але не завжди користувачі мають належну спроможність використовувати їх. Останнім часом зростальна чисельність кібератак на пересічних користувачів мережі Інтернет свідчить про нестачу кваліфікованих фахівців у сфері кібербезпеки. За прогнозами фахівців, «дефіцит» спеціалістів у сфері кібербезпеки у 2022 році досягне приблизно 1,8 мільйона робочих місць. Є безліч концепцій та пропозицій щодо ліквідації подібних ризиків, наприклад, завдяки підвищенню кваліфікації наявних співробітників органів публічної влади, недержавних організацій та бізнес структур або ж через застосування алгоритмів штучного інтелекту. Однак, на нашу думку, лише довгострокова стратегія, орієнтована на підготовку та спеціалізацію наступного покоління українських користувачів цифрових технологій допоможе забезпечити в майбутньому достатню кількість кваліфікованих кадрів, які професійно володітимуть необхідними цифровими компетенціями (навичками) [2, с. 96–97].

Важливою складовою професійної компетентності фахівців із кібербезпеки є цифрова компетентність, яка передбачає здатність та вміння логічно та системно використовувати інформаційні технології. Цифрова компетентність дозволяє людині бути успішною в сучасному інформаційному просторі, керувати інформацією, оперативно приймати рішення, формувати важливі життєві компетенції. Фахівець із кібербезпеки повинен вільно володіти сучасними технологіями та використовувати їх у

своїй професійній діяльності, тим самим забезпечувати життєво важливі інтереси людини і громадянина, суспільства та держави під час використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

Аналіз зарубіжного досвіду свідчить про існування різних означень цифрової компетентності. Учені Фінляндії визначають цифрову компетентність більш широко, ніж концепцію ІКТ-компетентності, яка складається з базових навичок використання ІКТ, а також розуміння процесу використання цифрових пристроїв та додатків у нових та складних ситуаціях. Науковці Іспанії розуміють під цифровими компетентностями використання комп'ютерів для отримання, оцінки, зберігання, створення, подання та обміну інформацією, а також для спілкування та участі в спільних віртуальних мережах. Це вимагає критичного та рефлексивного ставлення до наявної інформації та відповідального використання інтерактивних медіа [3, с. 31].

Науковець С. Скотт [4] розглядає цифрову компетентність як здатність використовувати цифрові ресурси та інформаційні технології, розуміти та вміти критично оцінювати цифрові ресурси та контент, ефективно комунікувати. Науковець виокремлює такі складові цифрової компетентності: інформаційна і медіаграмотність, онлайн комунікація, технічний та споживацький компоненти. Дослідник А. Феррарі на основі ґрунтовного аналізу різних проєктів та ініціатив трактує цифрову компетентність як набір знань, умінь, які необхідні для використання інформаційних технологій та цифрових медіа для виконання завдань, розв'язання проблем, керування інформацією, співробітництва, спілкування, створення і поширення контенту, спільної діяльності та задоволення потреб [5].

Своєю чергою вчений А. Мартін [6] вважає цифрову компетентність першим рівнем розвитку цифрової грамотності, тобто вибудовує протилежну підпорядкованість понять. А дослідниця К. Ала-Мутка, вивчаючи офіційні документи ЄС з питань освіти та наукові розвідки вчених, побудувала узагальнювальну модель цифрової компетентності [7], складниками якої стали:

– інструментальні вміння та знання (instrumental skills and knowledge), а саме технічні уміння роботи з цифровими пристроями, а також знання і вміння безпечного використання медіа середовищ;

– поглиблені уміння та знання (advanced skills and knowledge), що передбачають ефективну взаємодію та комунікацію, управління інформацією, навчання в мережі, участь у цифровій діяльності;

– ставлення (attitudes), зокрема розуміння й прийняття міжкультурної взаємодії, критичне ставлення до якості інформації, відкритість до цифрової творчості й навчання з використанням цифрових інструментів, розуміння й урахування проблем інтернет-безпеки, дотримання етики цифрового середовища.

Проблеми формування цифрової компетентності та ефективного використання інформаційних технологій у навчанні досліджували також і українські науковці. Так, викладач Житомирського державного університету імені Івана Франка С. М. Прохорова на прикладі вчителя іноземної мови визначає цифрову компетентність як здатність ефективно та результативно використовувати ІКТ у своїй діяльності та для свого професійного розвитку. На думку викладачки, до складових елементів цифрової компетентності також входять додаткові знання, уміння, здатності та ставлення, серед яких: технічні навички роботи з ІКТ, здатність застосовувати вказані ресурси у навчально-виховному процесі та здатність планувати, аналізувати та керувати освітнім та виховним процесом за допомогою ІКТ.

Група науковців Кам'янець-Подільського національного університету імені Івана Огієнка (А. М. Кух та О. М. Кух), описуючи цифрові компетентності в ознаках професійних вимог, визначили їх здатність до лідерства, здійснення інноваційної діяльності, інтегрованого використання засобів цифрових технологій для розв'язання професійних задач, здійснення експертизи даних і результатів діяльності та натуралізації – удосконалення власних умінь з використанням цифрових технологій у повсякденному та громадському житті та інтерналізації.

Ще одна група сучасних науковців (І. Бородкіна та Г. Бородкін) у процесі обґрунтування моделі цифрової грамотності студентів, яку розроблено на основі пірамідальної моделі з урахуванням концепції цифрової компетенції, також запропонувала своє визначення поняття, що нами досліджується. Так, на думку вчених, цифрова компетенція – це здатність користувача впевнено, ефективно та безпечно вибирати і застосовувати інформаційні та комунікаційні технології в різних сферах життя, заснована на безперервному оволодінні новими знаннями та уміннями.

Більш широку дефініцію поняття «цифрова компетентність» запропонувала група докторів наук (В. С. Куйбіда, О. В. Карпенко, О. М. Петроє, Л. І. Федулова, О. С. Марченко та Г. О. Андрощук) у 2019 році у рамках підготовки аналітичної записки «Цифрові компетенції як умова формування якості людського капіталу», яка розкриває сутність та передумови формування цифрових компетенцій у контексті розвитку глобального тренду цифрової трансформації суспільства. Науковці вважають, що цифрові компетенції – це сукупність знань, здібностей, особливостей характеру і поведінки, які необхідні для того, щоб людина могла використовувати ІКТ та цифрові технології для досягнення цілей у своєму особистому або професійному житті. На їхню думку, цифрова компетентність – багатогранний еволюційний процес, що постійно змінюється при появі нових технологій. При цьому компетенція у сфері цифрових технологій повинна сприйматися не лише як знання, що мають відношення до технічних навичок, а і як знання, більшою мірою зосереджені на когнітивних, соціальних та емоційних аспектах роботи і життя в цифровому середовищі.

Необхідно зазначити, що наукові дослідження торкнулися також й іншої складової процесу цифровізації – поняття цифрового інструментарію, який за своєю суттю нерозривно пов'язаний із цифровою компетентністю. І одну з перших розвідок у цьому напрямі здійснили науковці Київського університету імені Бориса Грінченка (Н. В. Морзе, В. П. Вембер, М. А. Гладун), які розглянули актуальні освітні тренди, інноваційні педагогічні технології та провели порівняння щодо ставлення викладачів, учителів та студентів до оволодіння цифровими інструментами і вміння їх ефективно використовувати в освітньому процесі [3, с. 37–38].

Більш широко дані питання висвітлив завідувач кафедри інформаційної політики та цифрових технологій Національної академії державного управління при Президентові України О. В. Карпенко, який, крім питань розвитку населення України з питань кібербезпеки, розглянув інструменти підвищення рівня цифрової грамотності і компетентності населення України в умовах сьогодення, сформулював потреби населення у освоєнні елементарних навичок з питань кібербезпеки, визначив необхідні види навчання, розкрив механізм їх подальшого впровадження, а також означив подальші кроки розвитку цифрової компетентності громадян України [2].

В Україні до початку 2018 року терміни «цифрова компетентність» та «цифрові інструменти» взагалі не згадувалися в офіційно прийнятих нормативно-правових актах. Певний прорив у даному контексті відбувся після розпорядження Кабінету Міністрів України від 17 січня 2018 року № 67-р «Про схвалення Концепції розвитку цифрової

економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації», яке окреслило більш конкретні кроки у напрямі розбудови системи для підвищення цифрової грамотності населення України. Так, розвиток цифрових компетенцій визнано напрямом цифрового розвитку України, а створення та виконання національної програми навчання загальним і професійним цифровим компетенціям та знанням, створення сприятливих умов та пошук відповідних моделей державно-приватного партнерства з операторами неформальної освіти, а також оновлення державного класифікатора професій, тобто розроблення та затвердження переліку цифрових професій на основі вимог ринку праці, цифрових трендів тощо, з подальшим розробленням відповідної програми їх запровадження у профільних навчальних закладах, визнано Концепцією важливими та пріоритетними завданнями на шляху до прискореного розвитку цифрової економіки. Крім цього, Концепція передбачає здійснення заходів щодо впровадження відповідних стимулів для цифровізації економіки, суспільної та соціальної сфер, усвідомлення наявних викликів та інструментів розвитку цифрових інфраструктур, впровадження яких надасть змогу реалізувати прискорений сценарій цифрового розвитку як найбільш релевантний для України з точки зору викликів, потреб та можливостей.

На сьогодні у нормативно-правових актах країни досі відсутні офіційні визначення термінів «цифрова компетентність» та «цифрові інструменти», що своєю чергою ще раз підкреслює негайну потребу розроблення стратегічного бачення та затвердження відповідних правових документів державного рівня, спрямованих на створення комплексної національної політики розвитку цифрової грамотності як населення України, так і фахівців у сфері кібербезпеки.

На теперішній час цифрова компетентність як в Україні [8], так і в країнах ЄС визнана однією з восьми ключових компетенцій для повноцінного життя та діяльності. 2016 року ЄС представив оновлений фреймворк Digital Competence (DigComp 2.0), що складається з основних п’яти блоків компетенцій та 21 компетенції (рис. 1).

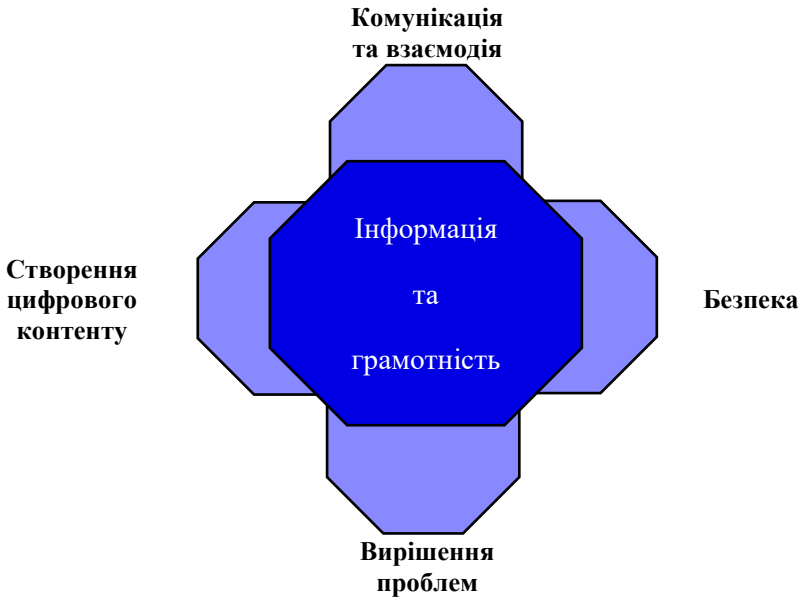

Рис. 1. Складові цифрової компетентності

Інформаційна грамотність та грамотність щодо роботи з даними (Інформація та грамотність) включає в себе вміння: шукати, фільтрувати дані, інформацію та цифровий контент; оцінювати дані, інформацію та цифровий контент; використовувати та

управляти даними, інформацією та цифровим контентом.

Зміст поняття «комунікація» змінюється одночасно з розвитком та ускладненням технічних засобів передачі повідомлень, глобалізацією і дедалі більшою інформатизацією світового суспільства. Комунікація та взаємодія передбачає вміння: спілкуватися через використання цифрових технологій; ділитися інформацією завдяки використанню цифрових технологій; контактувати із суспільством, користуватися державними та приватними послугами завдяки використанню цифрових технологій; взаємодіяти завдяки використанню цифрових технологій. Крім цього, до зазначеної складової відносяться знання «нетикету» (від англ. network та etiquette), тобто володіння правилами поведінки та етикету в цифровому середовищі, та управління цифровою ідентичністю, тобто вміння створювати та управляти акаунтами.

Цифровий контент складається зі: створення цифрового контенту; вміння змінювати, покращувати, використовувати цифровий контент задля створення нового контенту; обізнаності щодо авторських прав та політики ліцензування відносно даних, інформації та цифрового контенту; програмування, тобто вміння писати програмний код.

Своєю чергою така складова, як безпека визначає: вміння захистити пристрої та контент, знання заходів безпеки, розуміння ризиків та загроз; захист персональних даних та приватності; охорону здоров'я, тобто знання та навички для збереження свого здоров'я та інших з точки зору як екології використання цифрових технологій, так і ризиків, загроз безпеці громадян; захист навколишнього середовища, тобто розуміння впливу цифрових технологій на екологію, довкілля з точки зору утилізації, а також їх використання, що може завдати шкоди, наприклад, об'єктам критичної інфраструктури тощо.

П'ята і одночасно остання складова (Вирішення проблем) конструктивно формується із вміння: вирішувати технічні проблеми, що виникають із комп'ютерною технікою, програмним забезпеченням, мережами тощо; визначати потреби та знаходити відповідні технічні рішення або кастимізувати цифрові технології до власних потреб; самостійно визначати потребу в отриманні додаткових нових цифрових навичок. До цієї складової можна віднести також креативне користування або вміння завдяки цифровим технологіям створювати знання, процеси та продукти, індивідуально або колективно, з метою вирішення повсякденних життєвих та професійних проблем тощо [8].

Сьогодні цифрова компетентність є ключовою в умовах четвертої промислової революції. Сучасні IT-організації володіють складною, територіально розподіленою корпоративною структурою, великою кількістю інформаційних ресурсів, працюють в умовах зростальних репутаційних ризиків і безупинно мінливих зовнішніх вимог. Високий рівень збитку для бізнесу від кіберзлочинності у всьому світі, у тому числі в Україні, стимулює кіберкомпанії шукати можливості управляти цими ризиками як ззовні, так і зсередини. Опитування показує, що найбільшою загрозою для кібербезпеки компанії є необачні або необізнані співробітники (34%), застарілі засоби контролю безпеки (26%), несанкціонований доступ до інформації (13%) та ризики від використання хмарних обчислень (10%) [9].

Результати глобального дослідження EY з інформаційної безпеки показують, що кібербезпека залишається важливим питанням порядку денного організацій. 87% організацій стверджують, що не мають достатньо ресурсів для реалізації заходів із забезпечення кібербезпеки, 82% керівників не розглядають кібербезпеку як стратегічний пріоритет розвитку організації, а 77% респондентів наразі мають базовий рівень (тобто найнижчий) інструментів із забезпечення кібербезпеки [9]. Опитування показало, що 78% великих і 65% малих організацій вважають, що функція кібербезпеки принаймні

частково задовольняє їхні потреби, і лише 8% респондентів вважають, що функція повністю відповідає потребам компанії. Опитані організації продовжують працювати над впровадженням базових елементів кібербезпеки, а також перебувають у пошуку нових підходів та інструментів підвищення рівня цифрової компетентності для своїх фахівців. У такій ситуації забезпечити безпеку інформації при адекватних витратах можливо лише, якщо фахівці з кібербезпеки застосовуватимуть комплексний підхід з використанням організаційних заходів, програмно-технічних засобів і процесів управління на всіх рівнях діяльності організації, а також відповідного інструментарію задля підвищення рівня цифрової компетентності.

Цифрові інструменти – це потужні та ефективні важелі, які здатні забезпечити сфері кібербезпеки прорив на новий рівень розвитку та піднесення. Цифрові інструменти уможливлюють децентралізовану і пов'язану роботу (навчання) та підтримують компанії (органи, підрозділи) на різних стадіях процесу. Вони роблять робочий процес зрозумілим, дозволяють спілкуватися в індивідуальних або групових чатах, збирають і пріоритезують ідеї, структурують повсякденну роботу. Впровадження цифрових інструментів є шансом, нагодою та можливістю відкрити нові горизонти для будь-якого підрозділу або компанії.

Цифрові інструменти та активності, які використовуються в цифровій роботі, можна поєднати у такі основні групи, як цифрові медіа, STEAM-освіта, соціальні мережі і онлайн контент, 3-D та віртуальна реальність, які включають певний набір компонентів. Іншими словами, інструменти цифрової роботи – це засоби (інтернет-ресурси, онлайн ресурси), які застосовуються населенням будь-якої країни, усіма фахівцями та працівниками, які працюють у різноманітних сферах діяльності, для доступу до інформації, її обміну, передачі тощо. Із цифровими інструментами з'являється можливість полегшити ефективне керування різноманітними процесами, спростити операційну роботу та вивільнити ресурси на розвиток підрозділу, зміцнити довірчі відносини з партнерами та клієнтами.

Враховуючи положення Стратегії кібербезпеки України, Закону України «Про основні засади забезпечення кібербезпеки України», наукові напрацювання закладів вищої освіти, а також думки інших сучасних науковців, що досліджують засади цифрової трансформації публічного управління, пропонуємо сформулювати сутність такого поняття, як «цифрові інструменти сфери кібербезпеки». Отже, *цифрові інструменти сфери кібербезпеки – це сукупність інтернет-засобів (ресурсів), які використовують фахівці з кібербезпеки для захищеності суб'єктів мережевого середовища від різних видів інформаційних та кіберзагроз, забезпечення належної організації протидії їхньому впливу, формування, функціонування й еволюції кіберпростору, а також розвитку освітніх кібертехнологій та інформаційного суспільства в цілому.*

ІКТ швидко та постійно змінюються і розвиваються. Перелік сучасних ІТ-інструментів, які можуть собі дозволити українські органи і підрозділи державної і приватної кібербезпеки, доволі широкий, тому постає завдання щодо використання сферою кібербезпеки найефективніших і найдієвіших цифрових інструментів, що нададуть змогу управляти службовими процесами (за допомогою груп професійних кіберінструментів), розвивати освітню сферу (використовуючи групи інструментів кіберосвіти) та забезпечувати комунікацію на всіх її рівнях (застосовуючи групи комунікативних кіберінструментів), що в підсумку буде забезпечувати розвиток та підвищення рівня цифрової компетентності фахівців із кібербезпеки у публічному управлінні в цілому.

У цьому контексті варто навести досвід деяких світових кіберкомпаній, які для більш продуктивної роботи використовують кілька інструментів або ті, які включають у

себе безліч функцій. Так, міжнародна консалтингова компанія RW3 CultureWizard вп'яте опитала менеджерів у рамках Глобального опитування з віртуальної командної роботи. У дослідженні взяли участь 1620 менеджерів з 90 країн світу. 84% опитаних, відповідаючи, який тип спілкування вони вважають найкращим, заявили, що віртуальне спілкування складніше, ніж наживо. Оскільки безпосереднє спілкування не завжди можливе, на допомогу приходить програмне забезпечення, таке як Slack, Microsoft Teams і Yammer. Ці інструменти дозволяють співробітникам підключатися та обмінюватися повідомленнями і файлами.

У рамках опитування було досліджено також цифрові інструменти спільної роботи, які покращують організацію проєктів. Так, наприклад з таким інструментом, як Trello є можливість призначати завдання, коментувати і планувати їх виконання, а Redbooth показує користувачеві поточний список справ, а також дозволяє вести графік проєкту та відстежувати його прогрес. Своєю чергою Libre Plan підтримує планування ресурсів і дозволяє краще розподіляти завдання та координувати проєкти, а Wunderlist здійснює організацію та пріоритезацію окремих завдань.

Зарубіжний досвід підкреслює, що службові процеси потребують використовувати різні цифрові інструменти у сфері кібербезпеки. Багато провайдерів пропонують безкоштовну базову версію або пробний тестовий період. Коли він закінчується, саме команда кіберфахівців вирішує, чи зарекомендував себе новий інструмент і чи варто його купувати.

Здійснивши аналіз даних вітчизняних ресурсів, виділимо основні групи цифрових інструментів сфери кібербезпеки, які доцільно використовувати компаніям (органам, підрозділам) державної, приватної та академічної кібербезпеки під час організації та забезпечення службової діяльності (рис. 2).

ЦИФРОВІ ІНСТРУМЕНТИ

СФЕРИ КІБЕРБЕЗПЕКИ

ГРУПА ПРОФЕСІЙНИХ КІБЕРІНСТРУМЕНТІВ	
Шифрування даних	Соціальної медіабезпеки
Цілодобового моніторингу	Безпечного перегляду
Управління аутентифікацією	Інструменти для відновлення
ГРУПА ІНСТРУМЕНТІВ КІБЕРОСВІТИ	
Соціально-освітні інструменти	Планувально-навчальні інструменти
Практично-освітні інструменти	Інструменти онлайн користування
ГРУПА КОМУНІКАТИВНИХ КІБЕРІНСТРУМЕНТІВ	
Інструменти спілкування	Інструменти спільної візуалізації
Інструменти управління проєктами	Інструменти інтерактивних вправ

Рис. 2. Групи цифрових інструментів сфери кібербезпеки

Шифрування даних – один із найважливіших інструментів для захисту корпоративних файлів. Порушення безпеки даних має ряд ризиків, починаючи від втрати інтелектуальної власності до витоку конфіденційної інформації. До цієї підгрупи входять програми та інші інструменти для шифрування та приховування важливих даних. Для безпечного збереження цих даних використовуються складні алгоритми кодування.

Зашифрувати можна не тільки текст, а й іншу інформацію – від файлів баз даних до зображень. Найбільш відомими інструментами є TrueCrypt – програма для шифрування даних «на льоту», VeraCrypt – потужна програма для шифрування файлів, папок і цілих дисків на комп'ютері користувача, AxCrypt – утиліта з відкритим вихідним кодом, що призначена для захисту користувацьких даних методом шифрування, SafeNotes – інструмент для створення і зберігання паролів, який використовує 272-бітове шифрування і програмний захист військового стандарту, а також PicaSafe – віртуальний сейф, який надає можливість безпечного збереження і перегляду фотографій. Використовуючи це програмне забезпечення, можна надійно сховати від неавторизованих осіб свої секретні дані – банківські документи, особисті фотографії, персональні записи, пошту тощо.

Групи цілодобового моніторингу дозволяють спостерігати, зберігати дані та проводити аналіз поточної роботи інфраструктури в режимі реального часу згідно з даними, зібраними з десятків тисяч серверів, віртуальних машин і мережевих пристроїв. До завдань, які вирішує система моніторингу IT-інфраструктури, можна віднести: моніторинг працездатності широкого спектра програмного та апаратного забезпечення; виявлення потенційних проблем до того, як вони стануть реальними; інтегроване, сумісне рішення, яке підвищує ефективність управління IT-середовищем; рольовий підхід до управління, поліпшену масштабованість; підтримку великих неоднорідних IT-інфраструктур.

Сьогодні у сфері кібербезпеки виокремлюють ряд рішень, які допомагають забезпечити додаткові рівні безпеки корпоративної мережі. Проте важливо захищати не тільки IT-системи, а й конфіденційні дані, які є головним ресурсом будь-якого підприємства. Зокрема набуває популярності група цифрових інструментів для управління аутентифікацією, які є ідеальним рішенням для захисту різних онлайн сервісів від несанкціонованого доступу. Наприклад: Active Directory – поширена технологія від компанії Microsoft, на базі якої працюють служби аутентифікації і авторизації для бізнес-додатків та мережевих ресурсів; утиліта Health Profiler від компанії Ossisto, яка являє собою надійну підсистему виконання, призначену для повноцінного аналізу ризиків та безпеки; Netwrix Auditor – що дозволяє спостерігати, що відбувається всередині домену через відстеження авторизацій і змін у налаштуваннях користувачів, груп, організаційних одиниць, групової політики тощо; інструмент Account Lockout Examiner, який цілком заслуговує бути в цьому списку (ця утиліта сповіщає про блокування облікових записів, допомагає вирішувати проблеми і виявляти основні причини щодо кожної події і швидко відновлювати справжність критичних служб). Група інструментів для управління аутентифікацією може істотно зменшити імовірність викрадення особистих даних в Інтернеті та додати ще один рівень безпеки, щоб запобігти крадіжці чи витоку конфіденційних даних.

Засоби масової інформації є важливим інструментом в умовах формування інформаційного суспільства та поширення новітніх комунікаційних технологій. При цьому соціальні медіа (вебсайти, блоги, RSS-агрегатори, Wiki, Twitter, Facebook, ВКонтакте тощо) слід розглядати як засіб для надання послуг соціальної взаємодії, де користувачі створюють та обмінюються контентом, а також спілкуються один з одним. Серед основних видів кіберзагроз соціальних медіа можна виокремити крадіжку персональних даних, захоплення контролю над медіа, крадіжку інформації, фішинг (інтернет шахрайство) для отримання «компромату» тощо. І першочерговими інструментами захисту від таких загроз є використання першоджерела, надання інформаційного запиту, використання та перевірка інформації у мережі Інтернет – Google і допоміжних сайтів та онлайн-ресурсів, перевірка у соціальних мережах та

використання навичок критичного мислення. Крім того, дієвими кіберінструментами безпеки соціальних медіа є ряд технічних рішень, які мають можливість захистити інформацію в режимі онлайн, а саме: Disconnect – єдиний додаток VPN, який блокує відстеження у всіх додатках, а також цифрові інструменти бостонської компанії Abine, які захищають паролі, електронну пошту та платежі, та Ghostery Midnight, які допомагають користувачам зрозуміти, які дані збирають про них та хто їх збирає [10].

Група інструментів для безпечного перегляду захищає користувачів від зловмисного програмного забезпечення та спроб фішингу, сповіщаючи про перехід на небезпечні вебсайти та про слабкі місця в системі захисту. Наприклад, інструмент Google Cloud Security Scanner дає змогу сканувати й аналізувати вебдодатки на наявність загроз безпеці в App Engine, а Project Shield захищає вебсайти з новинами від блокування його роботи.

Персональні комп'ютери і ноутбуки, смартфони і планшети, а також інші цифрові пристрої сьогодні використовуються для зберігання важливих і особистих даних. І хоча надійність кожного із зазначених пристроїв на сьогоднішній день не викликає ніяких сумнівів – питання збереження і безпеки даних все ще дуже важливе для користувача. Відновити видалений чи втрачений файл можна за допомогою інструментів для відновлення даних: Recuva, Hetman Partition Recovery, EaseUS Data Recovery Wizard, UndeletePlus, R-Studio, Ontrack EasyRecovery, які на сьогодні є актуальними у спеціалістів IT-сфери.

Застосування IT-спеціалістами зазначених професійних кіберінструментів у службовій діяльності, в першу чергу, сприяє беззаперечному професійному і особистому розвитку та підвищенню рівня цифрової компетентності, є дієвим знаряддям забезпечення ефективності діяльності будь-якого підприємства (органу, підрозділу) і реалізації його потенціалу в майбутньому, сприяє збільшенню прибутку, зростанню продуктивності, зниженню витрат, поліпшенню якості цифрових продуктів та послуг.

Продовжуючи дослідження, слід розглянути групу цифрових інструментів управління кіберосвітою, які сприяють ефективності освітнього процесу на всіх його рівнях, формують цифрові компетентності майбутніх та нинішніх кіберфахівців, забезпечують розвиток інноваційних засобів навчання. У наш час цифрові технології та освіта у сфері кібербезпеки сплетені досить тісно, у багатьох викладачів (кібертренерів) є свої улюблені цифрові інструменти, які вони використовують у роботі і які дозволяють їм приділяти необхідну увагу з боку слухачів. При цьому цифрові інструменти безперервно оновлюються, а старі стверджуються, розширюючи сферу застосування або просто додаючи нові функції, більш актуальні для сучасної освіти і затребувані найбільш технологічно підкованими фахівцями освіти.

Соціально-освітні інструменти сфери кіберосвіти, використовуючи потужності соціальних медіа, допомагають як слухачам у процесі навчання, так і викладацькому складу вести плідну взаємодію. Наприклад, ресурс Wikispaces дозволяє ділитися онлайн завданнями, медіа та іншими матеріалами, а також надає можливість об'єднатися для подальшої співпраці. А інструмент Quora, незважаючи на те, що може використовуватися для широкого спектра різних цілей, слугує відмінним інструментом для співпраці і спілкування з іншими професіоналами сфери кібербезпеки або для залучення слухацької аудиторії до дискусії після занять. Крім цього, такі ресурси, як Edmodo, Grockit, EduBlogs, Skype, Pinterest, Schoology, Ning, OpenStudy, ePals дають широку можливість активно спілкуватися учасникам освітнього процесу, підтримувати зв'язок у режимі онлайн, а також співпрацювати з освітніми колективами інших країн.

Практично-освітні інструменти призначені для вмотивування слухачів, урізноманітнення навчального процесу та творчої самореалізації дозволяють

використовувати при цьому сучасні інтерактивні заходи. Так, StudySync – це освітня платформа з повнофункціональним інструментарієм для викладання та навчання, включаючи цифрову бібліотеку, щотижневі публікації практичного призначення, онлайн твори і експертні оцінки, а Educreations – онлайн-інструмент для iPad, який дозволяє створювати навчальне відео відповідно до заданої теми та демонструвати свої знання. До цієї групи доцільно також віднести новітню техніку презентації скрайбінг, яка за допомогою простих малюнків допомагає доступно пояснити складні теми, що дозволяє довго тримати увагу аудиторії та сприяти запам'ятовуванню ключових моментів.

Планувально-навчальні інструменти, які призначені переважно для викладачів (кібертренерів), дозволяють створювати зручний інтерактивний графік реалізації будь-якого проєкту по хвилинах. Це може бути Planboard – онлайн інструмент, створений спеціально для оцінювання успішності присутніх у освітній аудиторії, або Glogster – який дозволяє створювати мультимедійні постери, плакати тощо та є відмінним засобом для створення навчальних матеріалів і зручних інструментів для творчих проєктів.

Інструменти онлайн користування (Evernote, Dropbox, Diigo, Aviary, Jing, Popplet, SlideShare, LiveBinders тощо) являють собою набір цифрових застосунків, які дозволяють легко редагувати зображення, додавати ефекти, зразки, музику та аудіо або ж створювати і змінювати скрини, підключати до роботи інтерактивні дошки, створювати інтелектуальні карти, зберігати, обмінюватися інформацією, та мати доступ до неї з будь-якої точки світу.

Сьогодні в умовах швидких цифрових трансформацій впровадження відповідних освітніх кіберінструментів у систему підготовки кадрів у сфері кібербезпеки органів державної влади України є одним із пріоритетних напрямів розвитку всього кібернетичного суспільства. Безумовно, зростають вимоги і до особистості сучасного кібервикладача, який, крім вільного володіння сучасними цифровими технологіями, повинен також вільно використовувати їх у своїй професійній діяльності і тим самим забезпечувати ефективність всього навчального процесу.

Третьою групою цифрових інструментів, яку широко застосовують фахівці з кібербезпеки як у службовий, так і в позаслужбовий час, є так звана група комунікативних кіберінструментів, динаміка розвитку яких помітна неозброєним оком і виявляється в активній автоматизації всіх процесів та доступності інформації 24 години на добу в будь-якій точці світу. Такі кіберінструменти, крім підвищення рівня цифрової компетентності фахівців із кібербезпеки, вже зараз закладають основи до оновлення системи підготовки та підвищення кваліфікації різних категорій працівників із цифрової грамотності, зміни вимог до цифрових компетентностей при наймі персоналу, внесення змін до чинних професійних стандартів, вимог до посадових обов'язків тощо.

Мета групи інструментів спілкування – об'єднати розмови, робочі елементи і інструменти в одному місці, розставити пріоритети в роботі (або вирішити службові проблеми), поєднати потрібних людей, інформацію та інструменти для виконання певної роботи. Так, цифрові продукти компанії LogMeIn визначають категорії, розкривають потенціал сучасної робочої сили, дозволяючи мільйонам людей і компаній по всьому світу легко і безпечно виконувати роботу якнайкраще – на будь-якому пристрої, з будь-якого місця і в будь-який час. Своєю чергою Webex – універсальний магазин цифрових інструментів, який допомагає зустрічатися, спілкуватися і співпрацювати з віддалених місць, а також надає можливість працювати віддалено і не втрачати з уваги особисте життя або важливу зустріч з продажу. А компанія Appear зі штаб-квартирою в Осло (Норвегія) займається розробкою і виробництвом цифрових рішень світового класу для надання професійних послуг відео. Місія Appear – створювати унікальні цифрові продукти, що відкривають нові можливості для візуальної комунікації по всьому світу.

Інструменти управління проєктами – комплексне програмне забезпечення, що включає в себе програми для планування завдань, складання розкладу, контролю ціни і управління бюджетом, розподілу ресурсів, спільної роботи, спілкування, швидкого управління, документування та адміністрування системи, яка використовується спільно для управління великими проєктами. Найбільш популярними цифровими інструментами у цій групі є Asana (розробка мобільних і вебдодатків для управління проєктами в командах), Jira (відстеження помилок, організація взаємодії з користувачами) та Trello (управління проєктами невеликих груп).

У сучасному світі великих даних актуальним стає не тільки доступ до інформації, а й уміння правильно використовувати її, аналізувати та презентувати. Саме тут можуть стати у пригоді цифрові інструменти для візуалізації даних, завдяки яким креативно та ефективно можна і виокремити головне, і з різних сторін висвітлити весь контекст. Наприклад, Visme – платформа для створення презентацій, анімацій, банерів, інфографіки, звітів, форм і іншого візуального контенту, Easel.ly – цифровий інструмент, який використовує інтерфейс перетягування, що максимально спрощує його використання і робить процес створення інфографіки інтуїтивно зрозумілим і зручним, а Piktochart – ефективний інструмент для створення інфографіки, який призначений для використання у освітніх проєктах сфери кібербезпеки.

Інструменти інтерактивних вправ – це онлайн сервіси, за допомогою яких можна створювати та зберігати різноманітні медійні дидактичні вправи. Це конструктор інтерактивних завдань, що дає можливість перевірити та закріпити свої знання під час проведення заняття або вдома. У цьому напрямі слід виділити LearningApps.org – цифровий інструмент, створений для підтримки навчання і викладання за допомогою невеликих загальнодоступних інтерактивних модулів. Дані вправи створюються онлайн і в подальшому можуть бути використані в освітньому процесі.

Життя переходить у деякий віртуальний вимір і, щоб «бути на часі», потрібно максимально використовувати можливості сучасних інформаційних технологій, які стрімко проникають у всі сфери нашого життя. Цифрові інструменти – це новий етап еволюції цифрових процесів, сучасний механізм публічного управління, який надає змогу формувати у подальшому цифрову грамотність населення України, розвивати цифрову культуру, а також подолати цифрову нерівність та цифровий розрив.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Сьогодні економіка в Україні є ринковою, тому важливим фактором є оцінка не тільки підприємства в цілому, а й визначення відповідних процесів як фактора реалізації потенціалу. Значну роль у цьому відіграють ІТ-інструменти, які все більше застосовують в управлінні будь-яким підприємством, компанією, центром, у тому числі в органах державної влади України. Коли один інструмент засвоюється і стає звичним, з’являється новий. І це може бути проблемою для кіберфахівців – завжди встигати за розвитком технологій та засвоювати нові цифрові навички володіння цими технологіями.

У сьогоднішньому суспільстві рівень цифрових компетентностей населення здебільшого перебуває на базовому рівні – поряд із грамотністю та вмінням рахувати. Володіння цифровими інструментами, призначеними для вирішення суспільних питань, розв’язання типових та пов’язаних із професійною діяльністю завдань, вміння опановувати нові – одна з ключових компетенцій Президента України, Уряду, керівників усіх рівнів, а також кваліфікованого фахівця будь-якої галузі.

Реформа системи вищої освіти та її цифрова трансформація дуже тісно пов’язані з тими змінами, які відбуваються в соціальному житті країни, оскільки вони

безпосередньо відображають тенденції розвитку суспільства. Модернізація системи освіти у сфері кібербезпеки поетапно супроводжується певними позитивними змінами як у теоретичному аспекті, так і в практичній площині. Організація освітнього процесу у сфері кібербезпеки на сьогодні спрямована на реалізацію інноваційних підходів до викладання і навчання та забезпечує можливість інтеграції міжнародних освітніх цифрових стандартів в українську кіберосвіту на основі поетапного партнерства і співробітництва. І такі інновації у кіберосвіті відображаються в невід'ємних компонентах процесу навчання, зокрема у покроковому впровадженні цифрових кіберінструментів у публічному управлінні та більш широкому розповсюдженні таких понять, як «цифрова компетентність» та «цифрові інструменти».

Цифрові кіберінструменти – це адресні канали, що дозволяють учасникам освітньої діяльності вести постійний двосторонній інформаційно-персоніфікований діалог, тим самим даючи можливість підвищувати рівень цифрової компетентності. І на сьогодні використання розглянутих у роботі цифрових інструментів сфери кібербезпеки, безсумнівно, у подальшому будуть спрямовуватися на швидкий розвиток цифровізації суспільства, яка вимагає від того чи іншого викладача високого рівня цифрової компетентності та цифрової грамотності. Фахівці із кібербезпеки, які ведуть викладацьку діяльність, повинні бути готовими до реалізації нових ідей, використовувати можливості інформаційних технологій, підвищувати якість навчального процесу, готувати молодь до успішного життя. Цифрова компетентність є ключовою у процесі професійного розвитку, яка проявляється при вирішенні різних завдань із залученням засобів інформаційних технологій.

Цифровий інструментарій фахівців із кібербезпеки, крім підвищення рівня цифрової компетентності, забезпечує особистісно-орієнтований та диференційований підхід у кіберосвіті, забезпечує реалізацію інтерактивного підходу освітнього процесу та підвищує пізнавальну активність за рахунок різноманітної відео- та аудіоінформації. Серед недоліків впровадження цифрового інструментарію необхідно виділити зручність інтерфейсу (все нове нам здається незрозумілим та складним), необхідність постійного Інтернет доступу (це дійсно проблема, яка має позитивні тенденції до розвитку) та скорочення штату – поступова імплементація та впровадження інструментарію у сфері кібербезпеки в практичну площину призводить до деякого скорочення штату працівників муніципалітетів, що вказує на певну недосконаліть процесу цифровізації та штовхає на подальший розвиток кіберосвіти та розбудову кібербезпеки і публічного управління в цілому.

Потроху, але громадяни все більше долучаються до участі у освітньо-цифровій трансформації країни. Все більше з'являється можливостей та освітніх сервісів для взаємодії у кібернетичному просторі. І, що найбільш цікаво, всі нові сервіси створюються у вигляді доступних та зрозумілих цифрових інструментів. Такі інструменти, які дозволяють автоматизувати більшу частину своєї роботи, вивільняючи час на пошук, спілкування та самовдосконалення можуть стати у подальшому предметами подальших досліджень та наукових розвідок як серед вітчизняних так і серед зарубіжних науковців.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Diorditsa, I. (2016). State of training of cyber security specialist. *Visegrad Journal on Human Rights,* 6/1, 59-65.

2 Карпенко, О. В., Арсенович, Л. А. (2020). Державна кіберосвіта та інструменти підвищення рівня цифрової компетентності населення України. *Вісн. НАДУ. Серія «Державне управління»,* 1 (96), 95–

102.
3 Морзе, Н. В. (2019). 3D картування цифрової компетентності в системі освіти України. *Інформаційні технології і засоби навчання,* 70(2), 28-42.
4 Scott, C. (2015). The Futures of Learning 3: What kind of pedagogies for the 21st century?. *UNESCO Education Research and Foresight, Paris.* [ERF Working Papers Series, no. 15].
5 Ferrari, A. (2011). Digital Competence in Practice: An Analysis of Frameworks. *Luxemburg: IPTS-JRC.*
6 Martin, A., Grudziecki, J. (2006). Concepts and Tools for Digital Literacy Development. *Innovations in Teaching and Learning inInformation and Computer Sciences*, 5(4), 246-264.
7 Ala-Mutka, K. (2011). Mapping Digital Competence: Towards a Conceptual Understanding. *Luxemburg: IPTSJRC*.
8 Цифрова адженда України – 2020 («Цифровий порядок денний» – 2020) Концептуальні засади. Першочергові сфери, ініціативи, проєкти «цифровізації» України до 2020 року. https://ucci.org.ua/uploads/files/58e78ee3c3922.pdf.
9 Результати Глобального дослідження EY з інформаційної безпеки показують, що кібербезпека залишається важливим питанням порядку денного організацій. Сайт Європейської Бізнес Асоціації EBA. https://eba.com.ua/rezultaty-globalnogo-doslidzhennya-ey-z-informatsijnoyi-bezpeky-pokazuyut-shho-kiberbezpeka-zalyshayetsya-vazhlyvym-pytannyam-poryadku-dennogo-organizatsij/.
10 How to Improve Facebook Engagement in 2016. https://www.webhostingsecretrevealed.net/uk/blog/socialmedia-marketing/social-media-safety-5-dangers-every-influencer-needs-to-know-about/.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (15), 2022
ISSN 2663 - 4023

Arsenovych Leonid Antonovych
Doctor of Philosophy in Public Management and Administration,
deputy head – head of division at the HR Management Department of the Administration of the State Service for Special Communication and Information Protection of Ukraine, Kyiv, Ukraine
ORCID ID: 0000-0001-7081-2838
arsen-leon@ukr.net

TOOLS OF IMPROVING THE DIGITAL COMPETENCE LEVEL OF CYBER SECURITY PROFESSIONALS IN THE EDUCATIONAL PROCESS

Abstract. The article analyzes the accrued national and foreign developments regarding the problems of digital competence formation and effective use of information technology in education. The components of digital competence are considered, which provide for a confident, critical and responsible interaction with digital technology for education, work and participation in social activities. The results of a global information security research are presented along with surveys of employees of leading cyber companies around the world, including Ukraine, that testify to the necessity of further application and implementation of an integrated approach to education using organizational measures, software and hardware means and management processes at all activity levels of any organization, as well as using the appropriate tools to raise the digital competence level. The essence of the importance of digital tools in the field of cyber security is formulated, which means a set of Internet tools (resources) to protect network environment entities against various information and cyber threats, ensuring proper organization of countering their effect, formation, functioning and evolution of cyber space and development of educational cyber technology and the information society as a whole. Three main groups of digital cyber security tools were analyzed, identified and proposed (professional cyber tools, education cyber tools and communicative cyber tools) that enable the use, access, filtering, evaluating, creating, programming and communicating digital content, managing and protecting information, content, data and digital identities, as well as working effectively with software, devices, artificial intelligence, robots and more. It is proved that present-day work with digital cyber tools and their content requires a reflective, critical and at the same time inquisitive, open and promising attitude to their development, as well as an ethical, safe, effective and responsible approach to their use.

Keywords: cyber security professionals; digital literacy; digital competence; digital tools; digital technology.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1 Diorditsa, I. (2016). State of training of cyber security specialist. *Visegrad Journal on Human Rights*, 6/1, 59-65.
2 Karpenko, O. V., Arsenovych, L. A. (2020). State cyber education and tools to increase the level of digital competence of the population of Ukraine. *Visn. NADU. Seriia «Derzhavne upravlinnia»*, 1(96), 95–102.
3 Morze, N. V. (2019). 3D mapping of digital competence in the education system of Ukraine. *Informatsiini tekhnolohii i zasoby navchannia*, 70(2), 28-42.
4 Scott, C. (2015). The Futures of Learning 3: What kind of pedagogies for the 21st century?. *UNESCO Education Research and Foresight, Paris.* [ERF Working Papers Series, no. 15].
5 Ferrari, A. (2011). Digital Competence in Practice: An Analysis of Frameworks". *Luxemburg: IPTS-JRC.*
6 Martin, A., Grudziecki, J. (2006). Concepts and Tools for Digital Literacy Development. *Innovations in Teaching and Learning inInformation and Computer Sciences*, 5(4), 246-264.
7 Ala-Mutka, K. (2011). Mapping Digital Competence: Towards a Conceptual Understanding. *Luxemburg: IPTSJRC*.
8 Digital Agenda of Ukraine - 2020 ("Digital Agenda" - 2020) Conceptual principles. Priority areas, initiatives, projects of "digitalization" of Ukraine until 2020. https://ucci.org.ua/uploads/files/58e78ee3c3922.pdf.
9 The results of EY's Global Information Security Survey show that cybersecurity remains an important issue on the organizations' agenda. Website of the European Business Association EBA.

https://eba.com.ua/rezultaty-globalnogo-doslidzhennya-ey-z-informatsijnoyi-bezpeky-pokazuyut-shho-kiberbezpeka-zalyshayetsya-vazhlyvym-pytannyam-poryadku-dennogo-organizatsij/.

10 How to Improve Facebook Engagement in 2016. https://www.webhostingsecretrevealed.net/uk/blog/socialmedia-marketing/social-media-safety-5-dangers-every-influencer-needs-to-know-about/.