УДК 35.088.6:[004:007:351.86](477)
DOI https://doi.org/10.32689/2523-4625-2024-2(74)-1

Леонід АРСЕНОВИЧ
доктор філософії з публічного управління та адміністрування, заступник начальника управління, начальник відділу, Департамент кадрової роботи та управління персоналом Адміністрації Держспецзв'язку, arsen-leon@ukr.net
ORCID: 0000-0001-7081-2838

ІНСТРУМЕНТАРІЙ ПІДВИЩЕННЯ РІВНЯ ЦИФРОВОЇ КОМПЕТЕНТНОСТІ ФАХІВЦІВ НАЦІОНАЛЬНОЇ СИСТЕМИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ У ПУБЛІЧНОМУ УПРАВЛІННІ

Сучасна безпекова ситуація як в Україні, так і світі в цілому змінюється майже щодня, що є поштовхом для появи нових регуляторів, які у своєму арсеналі матимуть, у тому числі, дієві і ефективні важелі впливу на суспільні відносини в сфері захисту критичної інфраструктури. Основним завданням державної безпекової політики дедалі виразніше виступає створення гарантованих умов реалізації національних інтересів у сфері освіти.

Питання сфери захисту критичної інфраструктури актуалізуються з розвитком глобальних мереж, оскільки сучасним трендом стають цифрові технології. Шлях розвитку України у розбудові національної системи захисту критичної інфраструктури потребує корінних й негайних змін на основі застосування науково-обґрунтованих управлінських рішень. Така необхідність спричинена актуалізацією питання захисту систем, об'єктів і ресурсів, які є критично важливими для функціонування суспільства, соціально-економічного розвитку держави та забезпечення національної безпеки.

Наскрізним викликом для України є зростання темпів розвитку цифрових технологій, прискорення інновацій шляхом використання цих технологій, а також величезна потреба у кваліфікованих кадрах для трансформації 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, у тому числі сфери захисту критичної інфраструктури перед значними прошарками громадян постають цифрові бар'єри для повноцінного життя.

У статті проаналізовано питання професійної компетентності фахівців національної системи захисту критичної інфраструктури, сформульовано визначення цифровим інструментам сфери захисту критичної інфраструктури, а також виділено основні групи цифрових інструментів зазначеної сфери, що нададуть змогу управляти безпекою, керувати аутентифікацією, розвивати освітню сферу національної системи захисту критичної інфраструктури та забезпечувати попередження у сфері критичної інфраструктури, що в підсумку буде забезпечувати розвиток та підвищення рівня цифрової компетентності фахівців національної системи захисту критичної інфраструктури у публічному управлінні в цілому.

Ключові слова: *національна система захисту критичної інфраструктури, сфера захисту критичної інфраструктури, цифрова компетентність, цифрові інструменти, цифрові технології.*

Leonid Arsenovych. TOOLS FOR IMPROVING THE DIGITAL COMPETENCE OF SPECIALISTS OF THE NATIONAL SYSTEM OF CRITICAL INFRASTRUCTURE PROTECTION IN PUBLIC ADMINISTRATION

The current security situation in Ukraine and in the world as a whole is changing almost every day, which drives the emergence of new regulators that will have, among other, effective levers of influence on public relations in the area of critical infrastructure protection. The key task of the state security policy is ever more becoming to ensure guaranteed conditions for advocating the national interests in education.

The issues of critical infrastructure protection are becoming more relevant with the development of global networks, because digital technologies are becoming a modern trend. Ukraine's development path in building a national system of critical infrastructure protection needs fundamental and immediate changes based on the application of science-based management decisions. This need is caused by the emerging relevance of the issue related to protection of systems, facilities and resources that are critical for functioning of the society, for social and economic development of the state, and for safeguarding the national security.

A cross-cutting challenge for Ukraine is the increasing development of digital technologies, accelerated innovation through the use of these technologies, and the huge need for skilled workforce to transform the country's economy in the face of digital inequality. The key challenge is that the Ukrainian society is not prepared for the «digital challenge» – more specifically, most of the working population lack professional digital competencies. The issue of a large number of vacant jobs for employees with digital skills and unemployed socially active individuals who lack these skills needs to be addressed. With the transition of business operations, including the critical

infrastructure protection activities, to the online mode, numerous segments of the population face digital barriers on their way to living a full life.

The article analyzes the issues of professional competence of specialists of the national system of critical infrastructure protection, formulates a definition of digital tools in the area of critical infrastructure protection, and identifies the main groups of digital tools in this area that will allow managing security, administering authentication, developing the educational aspect of the national system of critical infrastructure protection and providing warnings in the area of critical infrastructure, which will ultimately ensure the development and improvement of digital competence of specialists of the national system of critical infrastructure protection in public administration overall.

Key words: *national system of critical infrastructure protection, critical infrastructure protection, digital competence, digital tools, digital technology.*

Постановка проблеми. Швидке поширення цифрових технологій в усіх сферах сучасного суспільства потребує також якісної підготовки фахівців національної системи захисту критичної інфраструктури, які генерують нове покоління представників технологічного соціуму, здатне зберігати і обробляти інформацію та протистояти несанкціонованому втручанню в інформаційне середовище. Необхідність збереження конфіденційності інформації, загострений дефіцит у кадровому забезпеченні сфери захисту критичної інфраструктури актуалізують необхідність створення результативної та дієвої системи підготовки фахівців у зазначеній сфері, і перш за все для суб'єктів національної системи захисту критичної інфраструктури.

Наукові напрацювання вчених та нормативно-правові акти засвідчують, що професійна підготовка фахівців національної системи захисту критичної інфраструктури є одним із напрямів національної безпеки, без якого є неможливим науково-технічний та соціально-економічний розвиток держави. На основі вивчення наукових праць з'ясовано, що в умовах повномасштабного вторгнення російської федерації на територію України питання підготовки фахівців національної системи захисту критичної інфраструктури вміщають в себе проблеми педагогічного, системного і міждисциплінарного характеру.

Аналіз останніх досліджень і публікацій. Як свідчать останні дослідження і публікації, проблеми професійного розвитку фахівців національної системи захисту критичної інфраструктури є малодослідженими. Так, науковець Дорогий Я.Ю., співробітник Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», у своїй статті розглядає питання формування вимог до нової критичної ІТ-інфраструктури, визначення параметрів для задання критерію оптимальності створення та управління критичною ІТ-інфраструктурою. Дорогий Я.Ю. зазначає, що життєвий цикл критичної ІТ-інфраструктури починається в момент появи ідеї створення такої інфраструктури і складається, у тому числі, з етапу проведення навчання персоналу [7, с. 100, 102].

Крім цього, іншими науковцями у сферах кібербезпеки та захисту критичної інфраструктури (Бурячок В.Л., Богуш В.М., Борсуковський Ю.В., Складанний П.М. та Борсуковська В.Ю.) у спільній роботі проаналізовано найбільш критичні світові загрози в інформаційній сфері, а також нові підходи до підготовки ІТ фахівців, з орієнтуванням їх передусім в практичну площину в сфері захисту критичної інфраструктури та з урахуванням найбільш актуальних умінь і навичок, які повинен отримати майбутній фахівець у зазначеній сфері. Вчені зазначають, що прикладна галузь кібербезпеки є тісно інтегрованою з поняттями інформаційної безпеки, безпекою застосувань, мережною безпекою, безпекою глобальних мереж, а також безпекою критичних інформаційних інфраструктур [4, с. 282].

Освітню складову сфери захисту критичної інфраструктури у своїй роботі розглядає також Теленик С.С., який встановлює перелік суміжних спеціальностей, які можуть бути затребувані в галузі захисту критичної інфраструктури. Вчений відводить важливе місце аналізу причин, що перешкоджають високій ефективності навчання та підвищення кваліфікації персоналу. Це, у свою чергу, дало змогу розробити пропозиції щодо вдосконалення існуючої нормативної бази та завдання для органів виконавчої влади України [14, с. 92].

Незважаючи на нещодавні дослідження вищевказаних науковців, які стосуються питань підготовки фахівців у сфері захисту критичної інфраструктури, питанням підвищення рівня цифрової компетентності фахівців національної системи захисту критичної інфраструктури у публічному управлінні приділено мало уваги, що й обумовило актуальність дослідження.

Метою статті є необхідність проведення аналізу впровадження та використання інструментарію підвищення рівня цифрової компетентності фахівців національної системи захисту критичної інфраструктури у публічному управлінні.

Виклад матеріалу. Важливою складовою професійної компетентності фахівців національної системи захисту критичної інфраструктури є цифрова компетентність, яка передбачає здібність та майстерність логічно та системно використовувати інформаційні технології. Цифрова компетентність дозволяє будь-якій людині бути вдалою в сучасному інформаційному просторі, формувати важливі повсякденні компетенції, керувати інформацією, а також оперативно приймати важливі рішення. Фахівець національної системи захисту критичної інфраструктури повинен вільно володіти сучасними цифровими інструментами та використовувати їх у своїй службовій діяльності, тим самим забезпечуючи життєво важливі інтереси людини і громадянина, суспільства та держави, а також своєчасне виявлення, запобігання і нейтралізацію реальних і потенційних загроз національній безпеці України у сфері захисту критичної інфраструктури.

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 [10, с. 31].

Проблеми формування цифрової компетентності та ефективного використання інформаційних технологій у навчанні досліджували також і українські науковці. Так, науковці А.М. Кух та О.М. Кух зазначають, що основи цифрової компетентності виявляються у розумінні суті цифрової технології, у підтримці комунікації, творчості та креативності, усвідомленні їх можливостей, обмежень, наслідків та ризиків, розумінні загальних принципів, механізмів та логіки цифрових технологій, знанні основ функціонування та використання різних пристроїв, програм та мереж [9, с. 31].

Науковець Бубній С.М. у своїй науковій роботі визначає, що цифрова компетентність – це набір знань, навичок та ставлень, необхідних для ефективного і критичного використання цифрових технологій для роботи, навчання та участі в соціальному і громадському житті. Вона включає здатність використовувати цифрові технології та інструменти для пошуку, оцінки, збереження, створення, презентації та обміну інформацією, а також для спілкування та співпраці в інтернет-просторі [3, с. 3].

У свою чергу, співробітники Криворізького фахового коледжу торгівлі та готельно-ресторанного бізнесу Наталя Боско та Лілія Бєла під поняттям «цифрової компетентності» розуміють складну цілісну структуру, до якої входять знання, навички та ставлення, необхідні для успішного використання цифрових технологій в процесі навчання та майбутньої професійної діяльності [2, с. 9].

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, у тому числі у сфері захисту критичної інфраструктури. Так, кандидат економічних наук, доцент, доцент кафедри менеджменту Київського національного економічного університету ім. В. Гетьмана Шатілова О.В. у своїй науковій статті подає характеристику таких цифрових інструментів інноваційного розвитку як: цифрове робоче місце, цифрові засоби комунікації, цифровий документообіг, цифрові інструменти накопичення та аналізу інформації. Науковиця зазначає, що основними факторами, що перешкоджають «цифровому добробуту» є необізнаність керівництва, надмірний консерватизм, надмірна бюрократизація, наявність «технологічної прірви» та брак ресурсів. Натомість, перспективними напрямками подальших досліджень у цій сфері є розробка нових цифрових інструментів, які б доповнювали перелік існуючих, а також удосконалення механізмів їх імплементації [15, с. 249].

В свою чергу, співробітниці Інституту інформаційних технологій і засобів навчання Національної академії педагогічних наук України Гриценчук О.О. та Овчарук О.В. у своїй спільній статті зазначають, що основною характеристикою цифрових інструментів, зокрема цифрових навчальних хабів є їх універсальність, доступність та гнучкість, що дозволяє налаштовувати цифрові інструменти для освітніх цілей, задач та інших потреб [5, с. 52].

Крім цього, науковці Хмельницького національного університету Красильников С.Р. та Красильникова Г.В. у своїй науковій статті зазначають, що уміння користуватися новітніми інформаційними технологіями та циф-

ровими пристроями (комп'ютери, ноутбуки, планшети, мобільні телефони тощо) і інструментами в повсякденному житті та професійній діяльності стає ключовою ознакою сучасної людини. Зокрема, при працевлаштуванні випускників закладів вищої освіти роботодавці орієнтуються на володіння ними цифровими навичками, які дають можливість швидко та ефективно виконувати поставлені завдання, бути успішними та реалізовувати потенційні можливості особистості [8, с. 2].

Слід зазначити, що до 2018 року терміни «цифрова компетентність» та «цифрові інструменти» не згадувалися в нормативно-правових актах. Прорив у даному питанні відбувся після видання 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» [12], яке стало першим кроком до:

– визначення критичних сфер та проєктів цифровізації України;

– визначення першочергових кроків щодо імплементації відповідних стимулів та створення умов для цифровізації в реальному секторі економіки, суспільстві, освіті, медицині, екології, у тому числі в сфері захисту критичної інфраструктури;

– стимулювання внутрішніх ринків споживання, впровадження та виробництва цифрових технологій;

– набуття громадянами цифрових компетенцій;

– трансформації економіки від традиційної до ефективної цифрової;

– розвитку цифрових інфраструктур, у тому числі для національної системи захисту критичної інфраструктури.

На сьогодні у нормативно-правових актах країни досі відсутні офіційні визначення термінів «цифрова компетентність фахівців національної системи захисту критичної інфраструктури» та «цифрові інструменти сфери захисту критичної інфраструктури», 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 національної системи захисту критичної інфраструктури.

Цифрові інструменти – це ефективні та потужні важелі, які здатні забезпечити сфері захисту критичної інфраструктури дієвий прорив на новий рівень розвитку та піднесення. Цифрові інструменти уможливлюють децентралізовану і пов'язану роботу (навчання) та підтримують суб'єкти національної системи захисту критичної інфраструктури на різних стадіях процесу. Вони роблять робочий процес зрозумілим, структурують повсякденну роботу, збирають і пріоритезують ідеї, а також дозволяють спілкуватися в індивідуальних або групових чатах. Впровадження цифрових інструментів у сфері захисту критичної інфраструктури є шансом, нагодою та можливістю відкрити нові горизонти для будь-якого суб'єкту національної системи захисту критичної інфраструктури.

Цифрові інструменти, які використовуються в цифровій роботі, можна поєднати у такі основні групи, як соціальні мережі, онлайн контент, 3-D та віртуальна реальність, STEAM-освіта та цифрові медіа. Іншими словами, інструменти цифрової роботи – це засоби (інтернет та онлайн ресурси), які застосовуються населенням, а також фахівцями та працівниками різноманітних сфер діяльності для доступу до інформації, її обміну, передачі тощо. Цифрові інструменти надають можливість полегшити ефективне керування різноманітними процесами, вивільнити ресурси на розвиток підрозділу, зміцнити довірчі відносини з клієнтами та партнерами, а також спростити операційну роботу.

Враховуючи положення Закону України «Про критичну інфраструктуру» [11], Концепції створення державної системи захисту критичної інфраструктури, схваленої розпорядженням Кабінету Міністрів України від 06 грудня 2017 року № 1009-р [13], наукові напрацювання закладів вищої освіти, а також думки інших сучасних науковців, що досліджують засади національної системи захисту критичної інфраструктури у публічному управлінні, пропонуємо сформулювати сутність такого поняття, як «цифрові інструменти сфери захисту критичної інфраструктури». *Отже, цифрові інструменти сфери захисту критичної інфраструктури – це сукупність інтернет-засобів (ресурсів), які використовують фахівці сфери захисту критичної інфраструктури для захищеності суб'єктів національної системи захисту критичної інфраструктури від різних видів інформаційних та кіберзагроз, забезпечення належної організації протидії їхньому впливу, формування і функціонування об'єктів критичної інфраструктури в умовах надзвичайних ситуацій, надзвичайного та воєнного стану, а також розвитку освітніх технологій у сфері захисту критичної інфраструктури та інформаційного суспільства в цілому.*

Інформаційно-комунікаційні технології постійно та швидко змінюються і розвиваються. Перелік сучасних цифрових інструментів, які можуть собі дозволити суб'єкти національної системи захисту критичної інфраструктури, доволі широкий, тому постає завдання щодо використання сферою захисту критичної інфраструктури найдієвіших і найефективніших цифрових інструментів, що нададуть змогу управляти безпекою (за допомогою групи безпеки та стійкості критичної інфраструктури), керувати аутентифікацією (через групу запобігання проявам несанкціонованого втручання на об'єкти критичної інфраструктури), розвивати освітню сферу національної системи захисту критичної інфраструктури (використовуючи групу освітніх інструментів сфери захисту критичної інфраструктури) та забезпечувати попередження у сфері критичної інфраструктури (застосовуючи групу обміну інформацією та взаємодії суб'єктів національної системи захисту критичної інфраструктури), що в підсумку буде забезпечувати розвиток та підвищення рівня цифрової компетентності фахівців національної системи захисту критичної інфраструктури у публічному управлінні в цілому.

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

Здійснивши аналіз даних вітчизняних ресурсів, виділимо основні групи цифрових інструментів сфери захисту критичної інфраструктури, які доцільно використовувати суб'єктам національної системи захисту критичної інфраструктури під час організації та забезпечення службової діяльності (рис. 1).

Шифрування інформації – важливий інструмент для захисту файлів. Порушення безпеки даних має ряд ризиків, починаючи від витоку конфіденційної інформації до втрати інтелектуальної власності. Така підгрупа включає в себе програми та інші інструменти для приховування важливих даних та шифрування. Для надійного збереження цих даних використовуються складні алгоритми кодування. Зашифрувати можна як текст, так й файли, бази даних та зображення. Найбільш відомими інструментами є:

– SafeNotes – інструмент для зберігання і створення паролів, який використовує 272-бітове шифрування і програмний захист військового стандарту. Продукт поширюється безкоштовно і включає в себе вбудований генератор сильних паролів. Програма нагадує щось на зразок блокнота з усім відповідним функціоналом, за допомогою якого користувач може створити захищений файл і внести в нього власні облікові дані. При цьому SafeNotes допоможе власнику ПЕОМ в разі необхідності вибрати пароль заданої максимальної довжини;

– AxCrypt – утиліта з відкритим вихідним кодом, що використовує метод шифрування та призначена для захисту користувацьких

ЦИФРОВІ ІНСТРУМЕНТИ СФЕРИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

ГРУПА БЕЗПЕКИ ТА СТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКТУРИ	
Шифрування інформації	Інструменти захисту
Громадської безпеки	Інструменти відновлення
ГРУПА ЗАПОБІГАННЯ ПРОЯВАМ НЕСАНКЦІОНОВАНОГО ВТРУЧАННЯ НА ОБ'ЄКТИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ	
Інструменти відстеження	Управління ідентифікацією
ГРУПА ОСВІТНІХ ІНСТРУМЕНТІВ СФЕРИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ	
Громадсько-освітні інструменти	Навчально-планувальні інструменти
Освітньо-практичні інструменти	Інструменти онлайн користування
ГРУПА ОБМІНУ ІНФОРМАЦІЄЮ ТА ВЗАЄМОДІЇ СУБ'ЄКТІВ НАЦІОНАЛЬНОЇ СИСТЕМИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ	
Інструменти комунікації	Інструменти сумісної схематизації
Інструменти керування ситуаціями	Діалогові інструменти

Рис. 1. Групи цифрових інструментів сфери захисту критичної інфраструктури

даних. Програма поширюється на безкоштовно з дещо обмеженим функціоналом. Ця утиліта об'єднує в собі менеджер зашифрованих файлів і кодувальник. Робота базується на використанні криптографічного алгоритму AES-128. Все, що потрібно користувачеві для захисту власних документів, це увійти до облікового запису AxCrypt і вказати бажаний пароль;

– TrueCrypt – програма для шифрування будь яких даних «на льоту». Одне з основних особливостей даної програми – відсутність в заголовку створеного «диска» специфічної сигнатури, характерної для інших подібних програм, що робить неможливим ідентифікувати його. Також за допомогою TrueCrypt можна повністю зашифрувати розділ жорсткого диска або іншого носія інформації. Всі збережені дані повністю шифруються, включаючи імена файлів і каталогів;

– VeraCrypt – потужна програма для шифрування як файлів, папок, так і дисків на комп'ютері користувача. Основними можливостями VeraCrypt є можливість створювати зашифровані томи з даними, приховувати зашифровані томи та використовувати надійні алгоритми шифрування;

– 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.

Засоби громадської безпеки є важливим інструментом в умовах формування інформаційного суспільства та поширення новітніх комунікаційних технологій. При цьому громадські медіа (вебсайти, блоги, RSS-агрегатори, Twitter, Wiki, Facebook тощо) слід розглядати як засіб для надання послуг громадської взаємодії, де користувачі створюють та обмінюються контентом, а також спілкуються один з одним. Дієвими інструментами зазначеної підгрупи 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 платежі, паролі і електронну пошту, та Ghostery Midnight, які допомагають користувачам зрозуміти, які дані збирають про них та хто їх збирає.

Серед основних видів загроз громадських медіа можна виокремити крадіжку інформації, отримання «компромату», захоплення контролю над медіа, крадіжку персональних даних, фішинг (інтернет шахрайство) тощо. І першочерговими інструментами захисту від таких загроз є перевірка у громадських мережах та використання навичок критичного мислення, надання інформаційного запиту, використання першоджерела та перевірка інформації у мережі Інтернет – Google і допоміжних сайтів та онлайн-ресурсів.

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

Смартфони, планшети, ноутбуки, а також інші цифрові пристрої сьогодні використовуються для зберігання особистих даних. Питання збереження і безпеки даних дуже важливе для користувачів. Серед інструментів відновлення слід виділити: EaseUS Data Recovery Wizard, UndeletePlus, Ontrack EasyRecovery, R-Studio, Recuva, Hetman Partition Recovery, які на сьогодні є актуальними у спеціалістів багатьох сфер.

Застосування спеціалістами національної системи захисту критичної інфраструктури зазначених професійних цифрових інструментів групи безпеки та стійкості критичної інфраструктури у службовій діяльності, в першу чергу, сприяє підвищенню рівня цифрової компетентності та беззаперечному професійному і особистому розвитку, є дієвим знаряддям забезпечення ефективності діяльності будь-якого суб'єкта національної системи захисту критичної інфраструктури і реалізації його потенціалу в майбутньому, сприяє зростанню продуктивності, зниженню витрат, поліпшенню якості цифрових продуктів та послуг, а також збільшенню прибутку.

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

Слід зазначити, що на сьогодні також набувають популярності цифрові інструменти для управління ідентифікацією, які є ідеальним рішенням для захисту різних сервісів від несанкціонованого доступу. Наприклад:

– Netwrix Auditor дозволяє спостерігати, що відбувається всередині домену через відстеження авторизацій і змін у налаштуваннях груп, організаційних одиниць, користувачів, групової політики тощо;

– Health Profiler, утиліта від компанії Ossisto, яка призначена для повноцінного аналізу ризиків та безпеки;

– Account Lockout Examiner, утиліта, яка допомагає вирішувати проблеми і виявляти основні причини щодо кожної події і швидко відновлювати справжність критичних служб, а також сповіщає про блокування облікових записів;

– Active Directory – поширена технологія від компанії Microsoft, на базі якої працюють служби ідентифікації і авторизації для додатків та мережевих ресурсів.

Використання у своїй службовій діяльності суб'єктами національної системи захисту критичної інфраструктури групи цифрових інструментів запобігання проявам несанкціонованого втручання на об'єкти критичної інфраструктури надасть змогу забезпечити безперервність і стійкість об'єктів критичної інфраструктури, а також унеможливити потенційні загрози для населення, суспільства, соціально-економічного стану, а також для національної безпеки і оборони України.

Продовжуючи дослідження, слід розглянути групу освітніх інструментів сфери захисту критичної інфраструктури, які формують цифрові компетентності фахівців зазначеної сфери, сприяють ефективності освітнього процесу на всіх його рівнях, а також забезпечують розвиток інноваційних засобів навчання.

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

Освітньо-практичні інструменти призначені для творчої самореалізації, урізноманітнення навчального процесу та вмотивування слухачів. Так, Educreations – онлайн-інструмент для iPad, який створює навчальне відео, а StudySync – це освітня платформа з інструментарієм для навчання та викладання, включаючи онлайн твори і експертні оцінки, цифрову бібліотеку, а також щотижневі публікації практичного призначення.

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

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

Сьогодні в умовах швидких цифрових трансформацій впровадження освітніх інструментів сфери захисту критичної інфраструктури у систему підготовки кадрів є одним із пріоритетних напрямів державно-приватного партнерства у зазначеній сфері. Безумовно, зростають вимоги і до особистості сучасного викладача, який, крім вільного володіння сучасними цифровими технологіями, повинен також вільно використовувати їх у своїй професійній та службовій діяльності і тим самим забезпечувати ефективність всього навчального процесу.

Четвертою групою цифрових інструментів, які можуть застосовувати фахівці суб'єктів національної системи захисту критичної інфраструктури, є група обміну інформацією та взаємодії суб'єктів національної системи захисту критичної інфраструктури. Метою впровадження цифрових інструментів даної групи є автоматизація всіх процесів та доступність інформації. Такі інструменти,

крім підвищення рівня цифрової компетентності фахівців національної системи захисту критичної інфраструктури, вже зараз закладають зміни до цифрових компетентностей при наймі персоналу, основи до оновлення системи підготовки та підвищення кваліфікації різних категорій працівників із цифрової грамотності, зміни до чинних професійних стандартів та до посадових обов'язків тощо.

Мета підгрупи інструментів комунікації – об'єднати розмови і потрібних людей, робочі елементи і інструменти в одному місці, вирішити службові проблеми, розставити пріоритети в роботі, а також поєднати інформацію та інструменти для виконання певної роботи. Так, такий універсальний магазин цифрових інструментів як Webex допомагає спілкуватися, зустрічатися і співпрацювати з віддалених місць. Своєю чергою цифрові продукти компанії LogMeIn розкривають потенціал сучасної робочої сили, дозволяючи фахівцям по всьому світу безпечно виконувати роботу якнайкраще. А компанія Appear займається розробкою і виробництвом цифрових рішень шляхом створення унікальних цифрових продуктів, що відкривають нові можливості для візуальної комунікації по всьому світу.

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

Серед інструментів сумісної схематизації необхідно виділити Piktochart – ефективний інструмент для створення інфографіки, який можна використовувати у освітніх проєктах сфери захисту критичної інфраструктури, Visme – платформу для створення банерів, звітів, інфографіки, презентацій, анімацій та іншого візуального контенту, а також Easel. ly – цифровий інструмент, який використовує інтерфейс перетягування, що максимально спрощує його використання і робить процес створення інфографіки зрозумілим і зручним.

Діалогові інструменти – це онлайн сервіси, які створюють та зберігають медійні дидактичні вправи. Це: LearningApps.org – цифровий інструмент, створений для навчання і викладання за допомогою загальнодоступних модулів. Дані вправи можливо створити онлайн і використовувати в освітньому процесі.

Висновки. На сьогодні, в умовах ринкової економіки, значну роль у цьому відіграють ІТ-інструменти, які все більше застосовують в управлінні будь-яким підприємством, у тому числі серед суб'єктів національної системи захисту критичної інфраструктури. Володіння цифровими інструментами, призначеними для розбудови сфери захисту критичної інфраструктури – одна з ключових компетенцій Уряду, Адміністрації Держспецзв'язку та керівників усіх рівнів національної системи захисту критичної інфраструктури.

На теперішній час модернізація системи освіти у сфері захисту критичної інфраструктури перебуває на шляху до позитивних змін, спрямовуючи освітній процес у зазначеній сфері на забезпечення інтеграції міжнародних освітніх цифрових стандартів в українську освіту, а також на реалізацію інноваційних підходів на основі державно-приватного партнерства. І такі інновації у сфері захисту критичної інфраструктури відображаються у покроковому впровадженні цифрових інструментів у публічному управлінні та більш широкому розповсюдженні такого поняття як «цифрові інструменти сфери захисту критичної інфраструктури».

Використання розглянутого у дослідженні інструментарію підвищення рівня цифрової компетентності фахівців національної системи захисту критичної інфраструктури у публічному управлінні, безсумнівно, у подальшому буде спрямовуватися на швидкий розвиток цифровізації суспільства, у тому числі в освітньому напрямку. Фахівці національної системи захисту критичної інфраструктури, які ведуть освітню діяльність, повинні підвищувати якість навчального процесу, готувати молодь до успішного життя, а також бути готовими до реалізації нових ідей, використовуючи можливості інформаційних технологій. Цифрова компетентність фахівців національної системи захисту критичної інфраструктури є ключовою у процесі професійного розвитку, яка проявляється при вирішенні різних завдань із залученням засобів інформаційних технологій.

Цифровий інструментарій фахівців національної системи захисту критичної інфраструктури, крім підвищення рівня цифрової компетентності, забезпечує реалізацію інтерактивного підходу освітнього процесу та особистісно-орієнтований підхід у сфері захисту критичної інфраструктури, а також підвищує пізнавальну активність за рахунок різноманіт-

ної відео- та аудіоінформації. Серед недоліків впровадження цифрового інструментарію необхідно виділити необхідність постійного Інтернет доступу, зручність інтерфейсу (все нове нам здається незрозумілим та складним), та скорочення штату працівників муніципалітетів, що вказує на певну недосконаліть процесу цифровізації та штовхає на подальший розвиток та розбудову сфери захисту критичної інфраструктури і публічного управління в цілому.

Слід визнати, що потроху суб'єкти національної системи захисту критичної інфраструктури все більше долучаються до участі у розробленні та впровадженні відповідного інструментарію у сфері захисту критичної інфраструктури. Так, 13 червня 2024 року Національним координаційним центром кібербезпеки при РНБО України спільно з Мінцифри та Держспецзв'язку презентовано новий інструмент CyberTracker, що дозволяє автоматизувати моніторинг виконання Стратегії кібербезпеки України. Використання CyberTracker дозволить:

– аналізувати вплив слабких та сильних сторін активностей Стратегії для прийняття відповідних рішень, у тому числі щодо набуття здатності швидко адаптуватися до внутрішніх і зовнішніх загроз у кіберпросторі, підтримувати та відновлювати стале функціонування національної інформаційної інфраструктури, насамперед об'єктів критичної інформаційної інфраструктури;

– ефективно інформувати громадськість та міжнародних партнерів щодо забезпечення оцінки спроможностей суб'єктів сектору безпеки і оборони в частині спільного виконання завдань кібероборони, зокрема під час проведення оборонних оглядів, оглядів національної системи кібербезпеки, оглядів стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури;

– спростити процедуру звітування щодо виконання Стратегії для відповідних державних органів та суб'єктів кібербезпеки, у тому числі з питань кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури.

«Виконання Стратегії кібербезпеки України є надзвичайно важливим для забезпечення національної безпеки. Портал CyberTracker стане незамінним інструментом у керуванні процесами щодо забезпечення стійкості національної системи кібербезпеки, надаючи можливість більш ефективного систематичного моніторингу та аналізу даних. Використання інструменту сприятиме підвищенню ефективності відстеження прогресу виконання завдань та реалізації цілей Стратегії, а також підвищенню позиції України в міжнародних рейтингах кібербезпеки», – зазначив керівник управління забезпечення діяльності НКЦК профільної служби Апарату РНБО України Сергій Прокопенко [6].

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 [1, с. 106].

Література:

1. Арсенович Л. А. Інструментарій підвищення рівня цифрової компетентності фахівців із кібербезпеки в освітньому процесі. *Кібербезпека: освіта, наука, техніка.* 2022. Вип. 3 (15). С. 93–109.

2. Боско Н. Формування цифрової компетентності здобувачів закладів фахової передвищої освіти. *Фізико-математична освіта.* 2024. Вип. 2. Т. 39. С. 7–13.

3. Бубній С. М. Цифрова компетентність як критичний аспект сучасної професійної освіти. *Академічні візії.* 2024. Вип. 30/2024. С. 1–7.

4. Бурячок В. Л. Модель підготовки фахівців у сфері інформаційної та кібернетичної безпеки в закладах вищої освіти України. *Інформаційні технології і засоби навчання.* 2018. Вип. 5. Т. 67. С. 277–291.

5. Гриценчук О. О. Цифрові інструменти для створення та підтримки середовища освіти для демократичного громадянства у європейських країнах. *Комп'ютер у школі та сім'ї.* 2020. Вип. 2/2020. С. 52–56.

6. Держспецзв'язку та НКЦК презентували CyberTracker – інструмент для автоматичного моніторингу виконання Стратегії кібербезпеки України. URL: https://cip.gov.ua/ua/news/derzhspeczv-yazkuta-nkck-prezentuvali-cybertracker-instrument-dlya-avtomatichnogo-monitoringu-vikonannya-strategiyi-kiberbezpeki-ukrayini. (дата звернення: 21.06.2024).

7. Дорогий Я. Ю. Життєвий цикл критичної ІТ-інфраструктури. *Electronics and communications.* 2015. Вип. 4. Т. 20. С. 100–105.

8. Красильников С. Р. Особливості розвитку цифрової компетентності у бакалаврів професійної освіти в ЗВО. *Академічні візії.* 2024. Вип. 32/2024. С. 1–10.

9. Кух А. М. Цифрова компетентність: на шляху до метакомпетентності. *Збірник наукових праць Кам'янець-Подільського національного університету імені Івана Огієнка. Серія : Педагогічна.* 2019. Вип. 25. С. 30–33.

10. Морзе Н. В. 3D картування цифрової компетентності в системі освіти України. *Інформаційні технології і засоби навчання.* 2019. Вип. 2. Т. 70. С. 28–42.

11. Про критичну інфраструктуру: Закон України від 16 листопада 2021 року № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text. (дата звернення: 21.06.2024).

12. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації: розпорядження Кабінету Міністрів України від 17 січня 2018 року № 67-р. URL: https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text. (дата звернення: 21.06.2024).

13. Про схвалення Концепції створення державної системи захисту критичної інфраструктури: розпорядження Кабінету Міністрів України від 6 грудня 2017 року № 1009-р. URL: https://zakon.rada.gov.ua/laws/show/1009-2017-%D1%80#Text. (дата звернення: 21.06.2024).

14. Теленик С.С. Напрями підготовки та підвищення кваліфікації фахівців із захисту критичної інфраструктури. *Правові новели.* 2020. Вип. 10/2020. Т. 2. С. 91–99.

15. Шатілова О. В. Цифрові інструменти інноваційного розвитку бізнес-організації. *Проблеми економіки.* 2020. Вип. 4. С. 249–255.