УДК 378.14:004
DOI:

Владислав Кива, *доктор філософії, старший науковий співробітник наукового відділу загального та ресурсного планування штабу Національного університету оборони України імені Івана Черняховського*

КІБЕРГІГІЄНА ВИКЛАДАЧІВ СИСТЕМИ ВІЙСЬКОВОЇ ОСВІТИ

У статті проаналізовано важливість забезпечення кібербезпеки України в умовах війни з боку Російської Федерації. Зосереджено увагу на визнанні на державному рівні необхідності формування та розвитку знань громадян України з кіберзахисту в умовах їх повсякденної цифрової діяльності. Визначено ключову причину низького рівня знань громадян України з кіберзахисту, зокрема викладачів системи військової освіти. Надано авторське трактування поняття "кібергігієна". Обґрунтовано необхідність формування у викладачів системи військової освіти компетентності з кіберзахисту, зокрема кібергігієни. На основі аналізу предметної області щодо формування кібергігієни викладачів системи військової освіти визначено об'єктивно наявні суперечності у педагогічній теорії та практиці, а також з консолідації наявних суперечностей сформульовані нерозв'язані наукові завдання для їх вирішення в майбутніх дослідженнях.

Ключові слова: *цифрові технології; цифровізація; кібергігієна; викладачі; система військової освіти.*
Літ. 16.

Vladyslav Kyva, *Ph.D.(Pedagogy), Senior Research Fellow of Research Branch of General and Resource Planning Staff The National Defense University of Ukraine named after Ivan Cherniakhovskiy*

CYBER HYGIENE OF TEACHERS IN THE MILITARY EDUCATION SYSTEM

Today, the digital transformation of the military education system has a huge impact on the behavior and interconnection between the subjects (teachers and students) of digital educational and research activities of higher military educational institutions. Thus, increasingly more teachers of the military education system cannot imagine their educational and research activities and everyday life without modern digital technology tools (smartphones, computers, etc.). Accordingly, these tools have become an integral part of their lives as "everyday friends". However, despite all the revolutionary changes and benefits associated with the digital transformation, the problematic issue arose regarding safe use of the relevant digital technology by teachers in the military education system in their daily educational and research activities, namely adherence to best practices in cyber security including cyber hygiene. Moreover, the constant cyber-attacks against the subjects of educational and research activities of higher military educational institutions during the COVID-19 pandemic and distance learning have confirmed the importance and necessity of personal cyber hygiene. As an example, disinfection of hands with an alcohol solution is a precaution against infection with the dangerous COVID-19 virus. Similarly, the observance of cyber hygiene by teachers in the military education system is a precautionary measure against possible cyber incidents. In this regard, the article analyzes the importance of ensuring the cyber security of Ukraine during the war by the Russian Federation. Attention is focused on the recognition at the state level of the need to form and develop the knowledge of Ukrainian citizens on cyber security in the context of their daily digital activities. The key reason is identified for the low level of knowledge of Ukrainian citizens regarding cyber defense, in particular of teachers in the military education system. The author's interpretation of the concept of cyber hygiene is given. The necessity is substantiated of forming cyber defense competences, in particular cyber hygiene, in teachers of the military education system. Also, based on the analysis of the subject area on cyber hygiene of teachers in the military education system, the objectively existing contradictions in pedagogical theory and practice are identified, and unresolved scientific problems are formulated to be resolved in future research.

Keywords: *digital technology; digitalization; cyber hygiene; teacher; military education system.*

Постановка проблеми. Сьогодні, як ніколи, є актуальним питання щодо забезпечення кібербезпеки України в умовах війни з боку Російської Федерації з початку 2014 р. і до сьогодні. До того ж, це питання є актуальним і для інших країн, що є членами ЄС і НАТО, або тих що обрали курс на набуття членства в цих організаціях. Варто зазначити, що Росія постійно намагається використовувати Україну як полігон для випробування не тільки нових зразків озброєння та військової техніки, а й для нових засобів і методів ведення кібервійни.

Так, на протидію російській агресії щодо кібернетичного впливу на інформаційні системи України (вірус Petya/NotPetya та інші) Верховна Рада України у жовтні 2017 р. ухвалила важливий закон "Про основні засади забезпечення

© В. Кива, 2022

кібербезпеки України" [10], яким враховує європейський досвід та принципи щодо взаємодії державних інституцій з приватним сектором і громадянським суспільством у сфері кібербезпеки. При цьому у, статті 10, на наш погляд, один з найголовніших аспектів, а саме "підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, комплексних знань, навичок і вмінь, необхідних для підтримки цілей кібербезпеки, реалізації державних і громадських проектів з підвищення рівня" [10], який з, одного боку, засвідчує на державному рівні визнання необхідності формування та розвитку знань громадян України щодо кіберзахисту їх повсякденної цифрової діяльності, а з іншого – підтверджує низький рівень їх знань. Варто наголосити, що зумовлено це неефективним функціонуванням кіберосвіти в Україні, а саме відсутністю комплексних освітніх програм підготовки, перепідготовки та підвищення кваліфікації громадян, які б функціонували на державному рівні.

До того ж, аналогічна ситуація склалася і в системі військової освіти (СВО), де навіть у викладачів вищих військових навчальних закладів (ВВНЗ) спостерігається часткова або повна відсутність необхідного рівня знань та нерозуміння важливості кіберзахисту під час застосування цифрових технологій (засобів) в освітньо-науковій діяльності. Тому особливо важливим в цьому аспекті вбачається необхідність формування у викладачів СВО компетентності з кіберзахисту, зокрема кібергігієни.

При цьому формування їх кібергігієни має бути динамічним та неперервним, що зумовлено геометричним розвитком методів та засобів здійснення різного типу кібератак на інформаційний простір ВВНЗ, де ключовими об'єктами кібервпливу є викладачі, які у своїй освітньо-науковій діяльності постійно працюють з різними цифровими засобами, на яких, зі свого боку може зберігатися військова інформація (дані) з різним грифом секретності. Відповідно, розповсюдження якої може дестабілізувати функціонування Сектора безпеки та оборони України. У зв'язку з цим виникає гостра необхідність в усвідомленості викладачами СВО важливості кібергігієни під час застосування цифрових технологій (засобів) у їх освітньо-науковій діяльності.

Аналіз останніх досліджень і публікацій. Аналізу проблемних питань щодо стану сформованості й усвідомлення важливості кібергігієни та кібербезпеки присвячені роботи таких дослідників, як: A. Cain, M. Edwards та J. Still; J. Esparza, N. Caporusso та A. Walters; F. Eboibi; K. Maennel, S. Mдses та O. Maennel; Ken Modeste; J. Nicholson та J. McGlasson; J. Oravec; S. Panda, E. Panaousis, G. Loukas та C. Laoudias; P. Pusey та W. Sadera; J. Such, P. Ciholas, A. Rashid, J. Vidler та T. Seabrook; В. Биков, О. Буров та Н. Дементієвська; О. Буров, О. Бутнік-Сіверський, О. Орлюк та К. Горська; В. Бурячок, В. Богуш, Ю. Борсуковський, П. Складанний та В. Борсуковська; В. Олексюк та О. Олексюк та інші.

Так, дослідники A. Cain, M. Edwards та J. Still [3] з'ясувала вплив віку, статі, досвіду та рівня їх навченості щодо кібергігієни. Вони зазначають, що кібергігієна користувачів є ключовим елементом, що відіграє ключову роль у протидії кіберзагрозам. Крім того, стверджують, що є необхідність в постійному оновленні знань, умінь та навичок щодо використання різного програмного забезпечення, з метою підвищення рівня кібербезпеки у їх повсякденній діяльності. Відповідно, ті користувачі, що дотримуються заходів кібергігієни, мають менші кіберризики.

Дослідники J. Esparza, N. Caporusso та A. Walters [4] звертають увагу, що кіберзагрози стають все більш складними та різноманітними, а отже, є потреба в оновленні заходів щодо протидії різним типам кібератак.

S. Panda, E. Panaousis, G. Loukas та C. Laoudias [12] стверджують, що заходи кібергігієни необхідні для зміцнення рівня кібербезпеки організації, особливо для захисту від кібератак соціальної інженерії, які спрямовані на людський фактор. Крім того, вони зазначають, що відповідні заходи (рекомендації), як правило, поверхові та не враховують усіх нюансів застосування й функціонування різного за призначенням програмного забезпечення.

У P. Pusey та W. Sadera [13] досліджено рівень підготовки вчителів, зокрема їх здатність щодо інтеграції різних інформаційних технологій у процес навчання та питання кібербезпеки під час їх впровадження. Відповідно, дослідники провели оцінювання 318 вчителів, результати якого засвідчили, що вони не були готові до впровадження та використання інформаційних технологій.

Цікавим є дослідження V. Buriachok, V. Bohush, Yu. Borsukovskyi, P. Skladannyi та V. Borsukovska [1], які проаналізували найбільш критичні загрози глобальної безпеки в інформаційній сфері, у результаті чого зробили висновок про наростання інформаційного протистояння та проникнення напруженості у відносинах різних країн. Крім того, вони наголошують на необхідності вироблення якісної моделі підготовки фахівців з кіберзахисту.

Зі свого боку науковці H. Xiao та B. Zhao [14]

у дослідженні діляться важливими знаннями щодо кіберзахисту Adobe Reader від кібератак, зокрема в їх праці детально проаналізовано функціональні можливості, різні технічні засоби та обмеження пісочниці Adobe Reader.

R. Mahajan, M. Singh та S. Miglani [11] демонструють як хакер може використати вразливість файлової системи NTFS, щоб приховати шкідливі коди на машині жертви, з метою реалізації кібератаки.

Також дуже цікавим є дослідження Y. Khera, D. Kumar та N. Garg [5], які наголошують, що збільшення кількості різноманітних інформаційних технологій підвищило ефективність різноманітного програмного забезпечення, зокрема мобільних та Windows додатків. Але при цьому це призвело до ускладнення використання цих систем та наявності у них потенційних кібервразливостей, які можуть бути використані зловмисниками (хакерами) для реалізації різного типу кібератак та експлуатації систем зламаних користувачів. Крім того, дослідники наголошують, що за останні 10 років хакерська діяльність дуже розширилася. Відповідно будь-яка організація, зокрема і користувач, опиняються у складній кіберневизначеності щодо кіберзахисту своїх систем та конфіденційних даних від зростаючої кількості кібератак. Тому, вчені наголошують, що краще було б виявити та ідентифікувати ці вразливості заздалегідь, перш ніж хакер міг би їх використати в своїх цілях. А отже, автори акцентують увагу на аналізі життєвого циклу тестування на проникнення в інформаційну систему з метою оцінювання ступеня її кіберзахисту та удосконалення в подальшому.

Достатньо цікавим для науковців є дослідження Yu. Bykov, O. Burov та N. Dementiievska [2], які проаналізували проблему кібербезпеки учасників освітнього процесу та акцентували увага на тому, що вона не зводиться лише до технічних аспектів захисту інформаційних ресурсів, а має охоплювати такі види захисту, як правові, технічні, інформаційні, організаційні та психологічні. Крім того, дослідники наголошують, що найбільш розповсюдженою кібератакою на учасників освітнього процесу, зокрема і користувачів, є метод соціальної інженерії. При цьому, автори також підкреслюють постійну необхідність у формуванні та розвитку кібергігієни в умовах цифрового буття.

Проте незважаючи на вагомі результати дослідження щодо кібергігієни різних фахівців, треба наголосити, що проблемні питання її формування та розвитку ще не достатньо досліджено й не приведено у відповідність до єдиного освітнього стандарту, а представлення науковців про кібергігієну фахівців суттєво різняться, а інколи і суперечать одне одному.

Метою статті є обґрунтування актуальності формування кібергігієни викладачів системи військової освіти.

Результати дослідження. Завдяки розвитку цифрових технологій СВО перебуває у неперервному процесі цифрової трансформації, її результати свідчать, що вона забезпечує підвищення ефективності функціонування освітньо-наукової діяльності ВВНЗ [8].

Так, у ВВНЗ впроваджуються технології дистанційного навчання та цифровізується вся можлива операційна діяльність закладу вищої освіти. Водночас, цифрова трансформація СВО, з одного боку, відкриває нові технологічні можливості для неї, а з іншого – створює проблеми забезпечення її кібербезпеки. Зі свого боку, питання забезпечення кібербезпеки ВВНЗ в кращому варіанті лягає на плечі фахівців з цієї предметної області, а в гіршому – на викладачів.

Окрім того, перед викладачами постає довічна дилема щодо правильності застосування цифрових технологій у ВВНЗ з врахуванням сучасних підходів до кіберзахисту, а також усвідомленості дій (необережності та неуважності) під час освітньо-наукової діяльності, які прямо або опосередковано впливають на їх кібербезпеку, що є однією з головних причин зниження її рівня.

При цьому аналіз неусвідомлених дій викладачами СВО по відношенню до кіберзахисту свідчить, що передумовою їх прояву були такі причини [7]:

- відсутність цінностей та мотивації щодо дотримання правил кіберзахисту (відсутність з боку керівництва дій щодо формування у викладачів ВВНЗ цінностей та мотивації до виконання правил кіберзахисту при застосуванні інформаційно-комунікаційних технологій (ІКТ) у науково-педагогічній діяльності, а також відсутність розуміння важливості діагностування їх рівня сформованості [9], [6], [15]);

- низький рівень освітнього, наукового та методичного забезпечення кібербезпеки освітньо-наукової діяльності (фрагментований підхід до формування у викладачів ВВНЗ компетентності з кіберзахисту або його відсутність взагалі; відсутність досліджень щодо проблемних питань пов'язаних із забезпеченням кібербезпеки викладачів в їх освітньо-науковій діяльності; відсутність методичної літератури з практичними прикладами щодо кіберзахисту).

Причому, розглянувши причини неусвідомлених

дій викладачів СВО стосовно кіберзахисту, необхідно зазначити, що без забезпечення їх ціннісно-мотиваційної підготовки досягнути кіберзахищеності не вдасться. Крім того, питання підготовки з кіберзахисту є системоутворювальним елементом забезпечення кібербезпеки викладачів СВО, зокрема, це пов'язано з тим, що від рівня підготовленості (компетентності) викладачів СВО залежить їх кібербезпека, це зумовлено усвідомленням або неусвідомленням дій щодо застосування ІКТ в освітньо-науковій діяльності, що може призвести до кіберзагроз. Звідси можна зробити висновок, що проблема підготовки (навченості) викладачів СВО у сфері кіберзахисту актуальна, як ніколи, і цьому питанню необхідно приділяти першочергову увагу [7].

До того ж, кібербезпека будь-яких суб'єктів (викладачів) чи об'єктів (цифрових пристроїв) інформаційного простору все більше залежить від розв'язання проблем, пов'язаних з різними поглядами її забезпечення, зокрема, способами мислення та наявними знаннями тих хто приймає відповідні рішення щодо обраного механізму кіберзахисту, в нашому випадку – викладачі СВО. Тому саме від якості знань викладачів СВО щодо кіберзахисту, залежить їх рівень кібербезпеки в умовах повсякденної цифрової діяльності у ВВНЗ.

Відповідно, кібербезпека, як ВВНЗ, так і викладачів СВО є важливим аспектом сьогодення. Зокрема, це обумовлюється тим, що:

- по-перше, ВВНЗ виконує стратегічне завдання щодо підготовки висококваліфікованих фахівців для Сектора безпеки та оборони України, а отже кібервплив на цифрові освітні системи може зупинити освітньо-науковий процес закладу вищої освіти;

- по-друге, викладачі СВО опрацьовують і зберігають величезні обсяги конфіденційної інформації (даних) на цифрових пристроях у ВВНЗ під час їх освітньо-наукової діяльності, а отже несанкціонований доступ кіберзлочинців до цих даних або їх розкриття / витік може мати негативний вплив, як на ВВНЗ, так і на Сектор безпеки та оборони України загалом;

- по-третє, аналіз різних джерел свідчить, що з 2020 р. посилилися кіберінциденти на заклади освіти і ВВНЗ не є винятком, зокрема, спостерігається посилення кібератак на дистанційне (електронне) навчання, крадіжка конференційної інформації (даних) та розповсюдження програм вимагачів для вимагання грошей.

Водночас, найпоширенішими кібератаками на ВВНЗ є:

1. Фішинг

Фішинг – це шахрайський електронний лист або веб-сайт, метою якого є збір конфіденційної інформації, такої як паролі, номери кредитних карток та інша особиста інформація, від користувачів, за умови використання їх. Фішингові листи часто використовуються як офіційні сповіщення від відомої компанії з проханням оновити свої особисті чи банківські реквізити, натиснувши посилання або завантаживши документ чи вкладений файл, вони заражають систему шкідливим програмним забезпеченням.

Інший спосіб, яким фішинг може спробувати отримати доступ до вашої системи, це встановити на ваш комп'ютер шкідливе програмне забезпечення,тобто – це програма або файл, який заражає систему і може викрасти конфіденційну інформацію.

2. Програми вимагачі

Програми вимагачі – це різновид зловмисного програмного забезпечення, яке шифрує файли комп'ютера користувача та вимагає викуп в обмін на ключ дешифрування, щоб розблокувати ваші файли. Атаки програм вимагачів поширюються через фішингові електронні листи та заражені веб-сайти. Як тільки вона заражає вашу систему, всі файли шифруються та блокується доступ до системи, що вимагатиме від вас заплатити певну суму грошей, щоб розблокувати та отримати доступ до файлів (даних).

3. Спам

Спам – це ще один спосіб, яким кіберзлочинці можуть отримати доступ до вашої системи, розсилаючи спамповідомлення зі шкідливими посиланнями або вкладенням. Спамові листи часто виглядають як офіційне сповіщення від закладу освіти чи компанії з проханням оновити особисту інформацію, натискаючи посилання або завантажуючи вкладення, ваша система заражається шкідливим програмним забезпеченням (вірусами).

4. Шкідливе програмне забезпечення

Шкідливе програмне забезпечення – спеціалізований софт, який залежно від функціоналу може отримати повний доступ до операційної системи, зокрема: контролювання дій об'єкта впливу та натискання клавіш; відправка, знищення або модифікація конфіденційної інформації і т.д.

5. SQL Injection

SQL Injection – застосування мови структурованих запитів для впливу на базу даних сайту (сервера) об'єкта впливу, що дозволяє виконувати шкідливий код.

6. XSS

XSS – міжсайтовий скриптинг, що дозволяє

використовувати вразливий сайт (сервер) для кібератаки на об'єкт впливу, зокрема шкідливий код інтегрується у сайт, який буде відвідувати об'єкт впливу, що надалі тому, хто атакує, отримати авторизаційні куки.

7. DoS

DoS – відмова в обслуговуванні, яка полягає в неможливості отримати доступ до інформаційного ресурсу (об'єкта атаки) у зв'язку з одночасним підключенням до нього мережі ботів, що призводить до повної витрати пам'яті та процесорного ресурсу сервера.

8. Атака нульового дня

Атака нульового дня – використання вразливості апаратно-програмного забезпечення, яка невідома його користувачам чи розробникам, що дає змогу атакуючому використати її у своїх намірах, з метою порушення конфіденційності, цілісності та доступності інформаційного ресурсу.

Водночас, кібератаки постійно вдосконалюються, а їх масштабність стає критичною. З цієї причини викладачі ВВНЗ мають чітко усвідомлювати ефект впливу кібератак на функціонування їх інформаційного простору [7].

У зв'язку з цим для забезпечення кібербезпеки як ВВНЗ, так і викладачів СВО, необхідно обрати сучасну стратегію кібергігієни. У нашому дослідженні під кібергігієною будемо розуміти – системне планування, реалізацію та підтримку запобіжних заходів щодо протидії кібернетичним загрозам в інформаційному просторі. При цьому під кібергігієною викладачів СВО будемо розуміти – динамічну здатність викладачів системи військової освіти системно планувати, реалізовувати та підтримувати запобіжні заходи щодо протидії кібернетичним загрозам в інформаційному просторі.

До того ж, кібергігієну необхідно розглядати як відносно нову парадигму, засновану на ідеї формування компетентності з планування, реалізації та підтримування запобіжних заходів надійного кіберзахисту. Проте перешкодами розвитку цієї парадигми є наявність об'єктивно наявних суперечностей у педагогічній теорії та практиці між:

- постійною увагою науковців до проблеми кібергігієни суб'єктів інформаційного суспільства та відсутністю наукових досліджень щодо її формування у викладачів СВО;

- підвищеною увагою військо-політичного керівництва України до проблеми кібергігієни суб'єктів інформаційного суспільства та відсутністю досліджень, в яких розкрито концепцію та методологічні підходи, які б цьому сприяли;

- необхідністю цілеспрямованого формування кібергігієни у викладачів СВО та відсутністю методичної системи, яка б забезпечувала цей процес у закладах військової освіти;

- системним розвитком масштабів застосування ІКТ викладачами СВО у повсякденній (науково-педагогічній) діяльності та відсутністю сформованості в них кібергігієни для забезпечення цієї діяльності.

А отже, з консолідації наявних суперечностей у педагогічній теорії та практиці постає нерозв'язане наукове завдання (проблема), а саме відсутність методичної системи формування кібергігієни викладачів СВО, для вирішення якого необхідно розв'язати такі взаємопов'язані із суперечностями дослідницькі завдання, а саме:

1. Здійснити аналіз стану дослідженості наукової проблеми формування кібергігієни викладачів СВО у педагогічній теорії і практиці та уточнити понятійний апарат дослідження.

2. Визначити поняття, виокремити структуру та зміст кібергігієни викладачів СВО.

3. Теоретично обґрунтувати та розробити авторську концепцію формування кібергігієни викладачів СВО.

4. Визначити та обґрунтувати методологічні підходи до формування кібергігієни викладачів СВО.

5. Розробити та обґрунтувати методичну систему формування кібергігієни викладачів СВО.

6. Розробити й впровадити у закладах військової освіти навчально-методичний комплекс "Кібергігієна викладачів системи військової освіти".

7. Розробити та впровадити у закладах військової освіти методичні рекомендації щодо формування кібергігієни викладачів СВО.

8. Експериментально перевірити результативність методичної системи формування кібергігієни викладачів СВО.

Висновки та перспективи подальших досліджень. Отже, проведений аналіз свідчить, що дослідженням формування кібергігієни викладачів СВО в України ще ніхто не займався, що, зі свого боку породжує актуальність і необхідність проведення відповідного дослідження щодо її формування згідно з вимогами та принципами сучасних методологічних підходів – компетентнісного, суб'єктно-діяльнісного, інформаційного, контекстного тощо.

У зв'язку з цим вважаємо, що подальша робота може бути спрямована на теоретико-методичне обґрунтування і розроблення методичної системи формування кібергігієни викладачів СВО.

ЛІТЕРАТУРА

1. Buriachok, V. L., Bogush, V. M., Borsukovskii, Yu. V., Skladannyi, P. M. & Borsukovska, V. Yu. (2018). Training model for professionals in the field of information and cyber security in the higher educational institutions of Ukraine. *Information Technologies and Learning Tools*. Vol. 67(5), pp. 277–291. [in Ukrainian].

2. Bykov, V. Yu., Burov, O. Yu. & Dementievska, N. P. (2019). Cyber security in a digital learning environment. *Information Technologies and Learning Tools*. Vol. 70(2), pp. 313–331. [in Ukrainia].

3. Cain, A. A., Edwards, M. E. & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of information security and applications*. Vol. 42, pp. 36–45. [in English].

4. Esparza, J., Caporusso, N. & Walters, A. (2020). Addressing Human Factors in the Design of Cyber Hygiene Self-assessment Tools. *International Conference on Applied Human Factors and Ergonomics*, Springer, Cham. pp. 88–94. [in English].

5. Khera, Y., Kumar, D. & Garg, N. (2019). Analysis and Impact of Vulnerability Assessment and Penetration Testing. *In 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)*. pp. 525–530. [in English].

6. Kyva, V. Y. (2018). The development of information and communication competence of teachers of the military education system as methodological problem. *Adaptive Management: Theory and Practice. Pedagogics*. No. 5(9), pp. 1–20. [in Ukrainian].

7. Kyva, V. Yu. (2022). Analysis of factors affecting cyber security of a higher military educational institution. *Cybersecurity: Education, Science, Technique*. Vol. 3(15), pp. 53–70. [in Ukrainian].

8. Kyva, V. Yu. (2020). Development of the information and communication competence of teachers in the system of military education in the process of remote learning. *Candidate's thesis.* Kyiv, 318 p. [in Ukrainian].

9. Kyva, V. Yu. (2019). Information and communication competence of teachers in the system of military education: concept, content and structure. *Cherkasy University Bulletin: Pedagogical Sciences*. 2019. No. 1, pp. 287–293. [in Ukrainian].

10. Law of Ukraine "On Basic Principles of Cyber Security of Ukraine". Available: https://zakon.rada.gov.ua/laws/show/2163-19#Text. (Accessed 24 Dec. 2021). [in Ukrainian].

11. Mahajan, R., Singh, M. & Miglani, S. (2014). ADS: Protecting NTFS from hacking. *In International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014)*. pp. 1–4. [in English].

12. Panda, S., Panaousis, E., Loukas, G. & Laoudias, C. (2020). Optimizing investments in cyber hygiene for protecting healthcare users. *In From Lambda Calculus to Cybersecurity Through Program Analysis*, Springer, Cham. pp. 268–291. [in English].

13. Pusey, P. & Sadera, W. A. (2011). Cyberethics, cybersafety, and cybersecurity: Preservice teacher knowledge, preparedness, and the need for teacher education to make a difference. *Journal of Digital Learning in Teacher Education*. Vol. 28(2), pp. 82–85. [in English].

14. Xiao, H. Y. & Zhao, B. B. (2013). Analysis on sandbox technology of adobe reader X. *In 2013 International Conference on Computational and Information Sciences*. pp. 137–140. [in English].

15. Yahupov, V. V. & Kyva, V. Y. (2019). Criteria and indicators of information and communication competence diagnostics development of teachers in the system of military education. *Information Technologies and Learning Tools*. No. 71(3), pp. 248–266.

Стаття надійшла до редакції 18.04.2022

"Найважливіше завдання цивілізації – навчити людину мислити".

Томас Едісон
всесвітньо відомий американський винахідник

"Досвід – це велика річ, він дозволяє вам визнавати помилку кожний раз, коли ви її здійснюєте".

невідомий автор