РОЗДІЛ 6. ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ

ТЕОРЕТИЧНІ ПІДХОДИ ЩОДО ВИЗНАЧЕННЯ ПРОБЛЕМИ РОЗВИТКУ ЦИФРОВОЇ КОМПЕТЕНТНОСТІ З КІБЕРБЕЗПЕКИ ВЧИТЕЛІВ ЗАКЛАДІВ ЗАГАЛЬНОЇ СЕРЕДНЬОЇ ОСВІТИ

THEORETICAL APPROACHES TO DETERMINING THE PROBLEM OF DEVELOPING DIGITAL COMPETENCE IN CYBER SECURITY OF TEACHERS OF GENERAL SECONDARY EDUCATION INSTITUTIONS

УДК 378:004.5
DOI https://doi.org/10.32782/2663-6085/2023/67.2.53

Коваленко В.В.,
канд. пед. наук, ст. дослідник,
ст. науковий співробітник відділу хмаро орієнтованих систем інформатизації освіти
Інституту цифровізації освіти
Національної академії педагогічних наук України

Осипчук Т.О.,
аспірантка
Інституту цифровізації освіти
Національної академії педагогічних наук України

Стаття присвячена аналізу теоретичних підходів щодо визначення проблеми розвитку цифрової компетентності з кібербезпеки вчителів закладів загальної середньої освіти. У статті було обґрунтовано актуальність проблеми розвитку цифрової компетентності з кібербезпеки вчителів закладів загальної середньої. Зокрема, проаналізовано звіт від Microsoft 2023 рік де підкреслено, що приблизно 99% кібератак відбуваються через недостатнє розуміння користувачами основ кібергігієни. Досліджено другий додатковий протокол до Конвенції про кіберзлочинність (Будапештська конвенція), що спрямований на посилення співпраці та розкриття електронних доказів і був підписаний державами-членами Ради Європи, у якому зазначено про посилену співпрацю та розкриття електронних доказів. Розглянуто підходи до визначення понять: «кібербезпека», «кібергігієна», «кібератака», «кіберзагроза», «кібертероризм», «кіберзахист», «кіберзлочин», «кіберзлочинність», «кіберпростір», «цифрова компетентність вчителів», «заклади загальної середньої освіти», «безпечне освітнє середовище» та ін. Визначено 5 основ кібергігієни, які були сформовані спеціалістами Microsoft і подані у звіті про цифровий захист Microsoft 2023 р. (застосування багатофакторної автентифікації, дотримання принципів моделі «нульової довіри», використання засобів розширеного виявлення й реагування, а також захисту від шкідливих програм, своєчасне оновлення засобів і програм, захист даних). Описано безпечне освітнє середовище закладу загальної середньої освіти, яке включає в себе кібербезпечне освітнє середовище закладу загальної середньої освіти, і зумовлює підвищення кваліфікації педагогічних працівників шляхом проведення різних заходів щодо забезпечення кібербезпеки у закладі загальної середньої освіти. Визначено політику кібербезпечного освітнього середовища закладу загальної середньої освіти яку можна впроваджувати шляхом рекомендацій щодо встановлення складних паролів та їх періодичній зміні, оновлення програмного забезпечення та операційної системи пристроїв, щоб запобігти кібератакам тощо.

Ключові слова: *кібербезпека, кібергігієна, кібератака, кіберзагроза, кібертероризм, кіберзахист, кіберзлочин, кіберзлочинність, кіберпростір, цифрова компетентність вчителів, заклади загальної середньої освіти, безпечне освітнє середовище.*

The article is devoted to the analysis of theoretical approaches to determining the problem of developing digital competence in cyber security of teachers of general secondary education institutions. The article substantiated the relevance of the problem of developing digital competence in cyber security of teachers of general secondary schools. In particular, the report Microsoft 2023 was analyzed, where it was emphasized that approximately 99% of cyberattacks occur due to insufficient understanding by users of the basics of cyber hygiene. Researched the second additional protocol to the Convention on Cybercrime (Budapest Convention), aimed at strengthening cooperation and disclosure of electronic evidence, was signed by the member states of the Council of Europe, which specifies enhanced cooperation and disclosure of electronic evidence. Approaches to the definition of concepts were considered: «cyber security», «cyber hygiene», «cyberattack», «cyber threat», «cyber terrorism», «cyber defense», «cybercrime», «cybercrime», «cyberspace», «digital competence of teachers», «institutions general secondary education», «safe educational environment» and others. 5 fundamentals of cyber hygiene were identified, which were formed by Microsoft specialists and presented in the report Microsoft 2023 (application of multi-factor authentication, compliance with the principles of the «zero trust» model, use of advanced detection and response tools, as well as protection against malicious programs, timely updating means and programs, data protection). The safe educational environment of the institution of general secondary education is described, which includes the cyber-safe educational environment of the institution of general secondary education, and leads to the improvement of the qualifications of pedagogical workers by conducting various measures to ensure cyber security in the institution of general secondary education. The policy of the cyber-safe educational environment of the general secondary education institution has been defined, which can be implemented through recommendations on setting complex passwords and changing them periodically, updating the software and operating system of devices to prevent cyberattacks etc.

Key words: *cyber security, cyber hygiene, cyberattack, cyber threat, cyber terrorism, cyber defense, cybercrime, cybercrime, cyber space, digital competence of teachers, institutions of general secondary education, safe educational environment.*

Постановка проблеми у загальному вигляді. У звіті від Microsoft 2023 рік [3] підкреслено, що приблизно 99% кібератак відбуваються через недостатнє розуміння користувачами основ кібергігієни.

На офіційному сайті Офісу Ради Європи в Україні, у розділі новини та заходи від 12 травня 2022 року [9], зазначено про посилену співпрацю та розкриття електронних доказів: 22 країни підписали новий Протокол до Конвенції про кіберзлочинність.

Другий додатковий протокол до Конвенції про кіберзлочинність (Будапештська конвенція) [9], спрямований на посилення співпраці та розкриття електронних доказів, який був підписаний державами-членами Ради Європи: Австрія, Бельгія, Болгарія, Естонія, Фінляндія, Ісландія, Італія, Литва, Люксембург, Чорногорія, Нідерланди, Північна Македонія, Португалія, Румунія, Сербія, Іспанія та Швеція, а також країнами які не є державами-членами Ради Європи: Чилі, Колумбія, Японія, Марокко та США.

За словами Генеральної секретарки Ради Європи Марія Пейчинович-Бурич: «…Кіберзлочинність активно зростає та еволюціонує з великою швидкістю. Це викликає серйозні проблеми у різних сферах, від бізнесу до медичних установ і критичної інфраструктури, яка становить основу для нашого повсякденного життя. На сьогоднішній день ми активно вносимо свій вклад у загальні зусилля світового співтовариства у боротьбі із кіберзлочинністю. Другий протокол призначений для адаптації Будапештської конвенції до сучасних технологічних викликів, забезпечуючи її актуальність та ефективність як міжнародної основи для протидії кіберзлочинності в наступних роках. Це відкриває двері до безпечнішого майбутнього» [9].

Міністр юстиції Італії Марта Картабія заявила – «…Кіберзлочинці використовують інформаційно-комунікаційні технології у різних «секторах», таких як сексуальна експлуатація, торгівля наркотиками, контрабанда та тероризм, що створює додатковий виклик для судових органів і установ. Наші уряди повинні адекватно та ефективно реагувати на всі ці злочини відповідно до технологічного прогресу. Тож, Другий додатковий протокол покликаний на потребу більш широкого та ефективного співробітництва між країнами та між країнами і приватним сектором, конкретизуючи ситуації, коли «постачальники послуг» можуть передавати дані, якими вони володіють, безпосередньо компетентним органам інших країн. Актуальність цього Протоколу є великою надією для жертв кіберзлочинів» [9].

Другий протокол надає засоби для посилення співпраці та розкриття цифрових доказів, такі як: прямий контакт з «постачальниками послуг» і реєстраторами, ефективні методи отримання інформації щодо абонентів і трафіку, оперативну взаємодію у надзвичайних ситуаціях або спільні розслідування, які входять у сферу захисту прав людини та принципів верховенства права, і включають гарантії щодо конфіденційності особистих даних [9].

У галузі кібербезпеки та захисту особистих даних, встановлюють права та обов'язки державних органів та організацій України такі нормативно-правові документи як: Закон України «Про основні засади забезпечення кібербезпеки України», Порядок взаємодії суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти/кібератаки одноголосно затверджено на засіданні НКЦК, Постанова Кабінету Міністрів України «Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі», Указ Президента України Про рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України» та ін.

На загальнодержавному рівні питання формування цифрової компетентності педагогів визначається у: Національній доктрині розвитку освіти України, Законах України «Про освіту», «Про вищу освіту», Рамці цифрової компетентності педагогічного й науково-педагогічного працівника та інших нормативних документах.

Аналіз останніх досліджень і публікацій. Проблеми забезпечення кібербезпеки у нормативно-правовому полі України розглядали: В. І. Андрєєв, І. Ф. Бінько, І. Ю. Бумба, С. О. Гнатюк, С. Ф. Гончар, І. Г. Грабар, Р. В. Грищук, Г. О. Дзяна, Н. Р. Дзяний, Д. В. Дубов, Я. А. Жаліло, З. Б. Живко, Б. А. Кормич, Є. В. Котух, В. А. Ліпкан, Ю. П. Лісовська, В. Г. Маргасова, К. В. Молодецька, М. А. Ожеван, О. В. Скорук, Т. О. Сліпченко, О. А. Ткаченко, Д. О. Тихолаз, М. І. Цюцюра, М. О. Цензура, В. С. Чередниченко, М. М. Шабатура, М. Є. Шелест, Я. І. Шестак, С. М. Шкарлет, В. Т. Шлемко та ін.

Технічні аспекти забезпечення кібербезпеки представлені у публікаціях: В. Л. Бурячка, О. В. Криворучко, Т. В. Савченко, М. В. Сашньової, К. В. Степашкіної, В. І. Чубаєвського, Ю. Г. Даника, П. П. Воробієнка, В. М. Чернеги, В. Б. Толубко, С. В. Толюпи, В. О. Хорошка та ін.

Кібербезпека у освітньому процесі розглянута у публікаціях: Л. А. Арсеновича, В. Ю. Бикова, О. Ю. Бурова, І. П. Гончарової, Н. П. Дементієвської, О. Б. Жильцової, Н. В. Коршун, А. Ю. Нашинець-Наумової, П. М. Складанного та ін.

Дослідження пов'язані з підвищенням рівня цифрової компетентності вчителів закладів загальної середньої освіти проводили: В. М. Андрієвська, В. Ю. Биков, В. О. Гальпєріна, Н. П. Дементієвська, Ю. О. Жук, І. В. Іванюк, В. В. Коваленко, В. В. Лапінський, М. П. Лещенко, О. О. Литвиненко, С. Г. Литвинова, М. В. Мар'єнко, Ю. Г. Носенко, О. В. Овчарук, Н. В. Олефіренко, О. П. Пінчук,

О. М. Соколюк, Н. В. Сороко, О. В. Співаковський, А. С. Сухіх, О.І. Шиман, М. П. Шишкіна та ін.

Проте, вивчення джерел показує, що теоретичні підходи щодо визначення проблеми розвитку цифрової компетентності з кібербезпеки вчителів закладів загальної середньої освіти, не достатньо представлені і потребують ґрунтовного вивчення.

Виділення невирішених раніше частин загальної проблеми. Вивчення нами джерел показує, що теоретичні підходи щодо визначення проблеми розвитку цифрової компетентності з кібербезпеки вчителів закладів загальної середньої освіти не достатньо розкриті і потребують подальшого дослідження.

Мета статті. Здійснити аналіз теоретичних підходів щодо визначення проблеми розвитку цифрової компетентності з кібербезпеки вчителів закладів загальної середньої освіти.

Виклад основного матеріалу. Останнім часом кібербезпека стала предметом багатьох робіт дослідників, але проблема розуміння цього явища залишається невирішеною, зважаючи на швидкий розвиток цифровізації суспільства та збільшення можливостей впливу на суспільні відносини. Це призводить до виникнення нових загроз для громадської безпеки в цілому і вимагає оновлення та вдосконалення системи її забезпечення. Також потрібне ґрунтовне переосмислення поняття «кібербезпеки», оскільки феномен інформації швидко змінюється, а світове співтовариство стає все більше залежним від цифрових технологій. Ці перетворення інформаційної сфери викликають ряд теоретичних і практичних проблем, які потребують уточнення поняття «кібербезпеки» та більш системного підходу до її забезпечення.

В рамках нашого дослідження є потреба розглянути підходи до визначення «кібербезпека», «кібергігієна», «кібератака», «кіберзагроза», «кібертероризм», «кіберзахист», «кіберзлочин», «кіберзлочинність», «кіберпростір», «цифрова компетентність вчителів», «заклади загальної середньої освіти», «безпечне освітнє середовище» та ін.

Нормативно-правові документи України, зокрема у сфері кібербезпеки та захисту особистих даних, регулюють права та обов'язки державних органів та організацій. Ці правила впливають на особистий рівень кібергігієни кожного громадянина, визначаючи умови збереження та використання особистих даних користувачів. Існує потенційна загроза з боку хакерів та кіберзлочинців, які можуть порушувати закони та використовувати конфіденційну інформацію для шахрайства. У разі кіберзлочинних дій по відношенню до користувачів чи організацій, зокрема, шахрайства чи незаконного доступу, надзвичайно важливо звертатися до кіберполіції чи служби безпеки України.

У статті 1 Закону України «Про основні засади забезпечення кібербезпеки України» [14] наведені терміни в рамках нашого дослідження такі як: *«кібератака»* – визначається як цілеспрямовані (навмисні) дії в кіберпросторі, які виконуються за допомогою електронних засобів комунікації, таких як програмне і програмно-апаратне забезпечення, інші технічні засоби та обладнання. Основною метою таких дій є порушення конфіденційності, цілісності та доступності електронних інформаційних ресурсів, які опрацьовуються, передаються або зберігаються в комунікаційних та/або технологічних системах. Ці дії можуть призвести до негативних наслідків, таких як несанкціонований доступ до таких ресурсів, порушення безпеки та стійкості нормального режиму функціонування комунікаційних та/або технологічних систем. Крім того, ці дії можуть використовуватися для проведення кібератак на інші об'єкти кіберзахисту; *«кібербезпека»* – це забезпечення захисту життєво важливих інтересів осіб, громадян, суспільства та держави під час використання кіберпростору. Це передбачає забезпечення стійкого розвитку інформаційного суспільства та цифрового комунікативного середовища, а також вчасне виявлення, запобігання та нейтралізація конкретних і потенційних загроз національній безпеці України в кіберпросторі; *«кіберзагроза»* – це існуючі та потенційно можливі явища і чинники, які створюють у кіберпросторі загрозу життєво важливим національним інтересам України. Вони викликають негативний вплив на стан кібербезпеки країни, її кібербезпеку та кіберзахист об'єктів; *«кіберзахист»* – сукупність організаційних, правових, інженерно-технічних заходів, криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення функціонування комунікаційних, технологічних систем; *«кіберзлочин»* – суспільно небезпечні дії у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України; *«кіберзлочинність»* – сукупність кіберзлочинів; «*кіберпростір»* – це віртуальне середовище, яке виникає внаслідок роботи взаємопов'язаних комунікаційних систем і забезпечує можливості для взаємодії та спілкування в суспільстві. Воно формується завдяки функціонуванню з'єднаних комунікаційних систем і надає можливості для електронних комунікацій за допомогою мережі Інтернет або інших глобальних мереж передачі даних; *«система активної протидії агресії у кіберпросторі»* – сукупність організаційних, правових, наукових та технічних заходів, спрямованих на підвищення рівня кіберзахисту держави шляхом здійснення впливу на

інформаційні (автоматизовані), електронно-комунікаційні, інформаційно-комунікаційні системи держави-агресора, джерела походження кіберзагроз та кібератак; *«активна протидія агресії у кіберпросторі»* – це комплекс організаційних, правових, наукових та технічних заходів, спрямованих на підвищення рівня кіберзахисту держави. Це досягається шляхом впливу на інформаційні (автоматизовані), електронно-комунікаційні, інформаційно-комунікаційні системи агресором, а також джерелами походження кіберзагроз та кібератак [14].

У Порядку взаємодії суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти/кібератаки одноголосно затверджено на засіданні НКЦК від 22.09.2022 [11] використовуються такі терміни як: *«подія кібербезпеки»* – це визначена ситуація на об'єкті кіберзахисту, яка сигналізує про можливе порушення політики безпеки або невдалу роботу засобів захисту, також може вказувати на раніше невідому ситуацію, що може стосуватися безпеки; *«рівень критичності кіберінциденту/кібератаки»* – рівень негативних наслідків для інформаційної інфраструктури країни, які можуть виникнути внаслідок кіберінциденту або кібератаки [11].

Кібертероризм – це суспільно небезпечна діяльність, яка усвідомлено здійснюється у кіберпросторі або за допомогою його технічних можливостей, окремими особами або організованими злочинними групами з терористичною метою і реалізується через заздалегідь сплановані кібератаки на інформаційно-телекомунікаційну систему з використанням високих технологій [4, с. 57].

Кібергігієна представляє собою комплекс процедур, спрямованих на зменшення ризику кібератак. За допомогою принципів кібергігієни, таких як обмеження доступу та багатофакторна автентифікація, несанкціонованим особам стає важче отримати доступ до даних та відомостей. Також цей підхід включає стандартні рекомендації, такі як регулярне оновлення програмного забезпечення та резервне копіювання даних, що допомагає зменшити кількість системних кібератак [17].

У звіті про цифровий захист Microsoft 2023 р. [3] зазначено, що в контексті особистої кібергігієни розвідка хакерів часто базується на зборі даних і відомостей про конкретних осіб через соціальні мережі або робочі електронні пошти. Забезпечення безпеки передбачає усвідомлення як соціальних, так і технічних аспектів, таких як використання надійних паролів та уважність до фішингових атак.

Також у цьому звіті [3] визначено п'ять основ кібергігієни, які подані на рис. 1 і описані нижче.

Основи кібергігієни, які визначені у [3]:

1) *застосування багатофакторної автентифікації* (може захистити користувачів від уражених

Рис. 1. Основи кібергігієни [3]

паролів і забезпечує більш високий рівень стійкості ідентифікації);

2) *дотримання принципів моделі «нульової довіри»* (обмеження впливу атаки на організацію: активна перевірка, використання доступу з мінімальними правами та постійне усвідомлення можливості порушення);

3) *використання засобів розширеного виявлення й реагування, а також захисту від шкідливих програм* (використання програмного забезпечення, яке виявляє та автоматично блокує кібератаки, а також забезпечує аналітику для захисного програмного забезпечення. Моніторинг аналітики, що надходить з систем виявлення загроз, має велике значення для оперативного усунення потенційних проблем);

4) *своєчасне оновлення засобів і програм* (внаслідок використання вразливих та застарілих систем, організації можуть потрапити під кібератаку. Потрібно постійно перевіряти стан системи, включаючи мікропрограми, операційні системи тощо);

5) *захист даних* (для належного захисту, потрібно знати, які дані важливі, де вони розташовані і чи вживаються належні заходи для їхнього захисту).

На думку Б. А. Кормич, *кібербезпека* – це забезпечення захищеності визначених законом правил і норм, які регулюють інформаційні процеси в державі, що має на меті створення гарантованих умов, які передбачені Конституцією, для існування та розвитку людини в сучасному інформаційному просторі всього суспільства та держави [6, с. 142].

Д. В. Дубов і Ожеван М. А. визначають *кібербезпеку* як спрямовані дії, які відбуваються в кіберпросторі або використовують його технічні

можливості і можуть призвести до досягнення незаконних цілей, таких як порушення конфіденційності, цілісності, автентичності та доступності інформації, а також до застосування деструктивних інформаційно-психологічних впливів на свідомість та психічний стан громадян [2].

У публікації [8, с. 55] *кібербезпека* подана, як захист інформації та відповідної інфраструктури від непередбачених чи навмисних впливів, які можуть призвести до неприйнятної шкоди для учасників інформаційних взаємодій, включаючи власників та користувачів даних, а також технічну підтримку інфраструктури.

Погоджуємось з думкою, Р. М. Пріми, О. В. Гончарука, Д. А. Пріми [12, с. 399], що активне використання цифрових технологій в освіті сприяє покращенню освітнього процесу на всіх рівнях і сприяє формуванню професійної майстерності майбутніх педагогів, що передбачає перегляд підходів до їх освіти.

Сучасні реалії ставлять перед системою освіти завдання забезпечити майбутнім педагогам не лише фахові знання, а й акцентують увагу на розвитку їх цифрової компетентності. Це стає ключовим чинником для отримання їх якісної освіти, оскільки цифрова компетентність дозволяє майбутнім педагогам бути конкурентоспроможними на ринку праці і успішно адаптуватися до сучасного інформаційно-технологічного середовища, вирішуючи існуючі цифрові виклики між ними та їх майбутніми учнями [12, с. 400].

У рамці цифрової компетентності педагогічного й науково-педагогічного працівника, *цифрова компетентність* – це динамічне поєднання знань, умінь, навичок, способів мислення, поглядів, цінностей та інших особистих якостей в галузі цифрових технологій. Вона визначає здатність особи успішно інтегруватись у суспільство, здійснювати професійну та/або навчальну діяльність з використанням цифрових технологій [16].

Цифрова компетентність вчителя визначається його здатністю ефективно використовувати цифрові технології в освітньому процесі. Це охоплює знання та навички в таких областях, як створення цифрового контенту, використання онлайн платформ, комунікація та співпраця, цифрова безпека та етичне використання технологій. Цифрово-компетентний вчитель також має вміти інтегрувати цифрові технології у свою навчальну програму та оцінювати їх ефективність в освітньому процесі [5].

У статті 8 пункті 1 Закону України «Про освіту» [13] «*заклад загальної середньої освіти*» (ЗЗСО) визначено, як заклад освіти, основним видом діяльності якого є освітня діяльність у сфері загальної середньої освіти. Також у статті 1 пункті 1 цього Закону *«безпечне освітнє середовище»* визначається як комплекс умов у закладі освіти, які запобігають заподіянню учасникам освітнього процесу фізичної, майнової та/або моральної шкоди. Це включає в себе також дотримання санітарних, протипожежних та/або будівельних норм і правил, відповідність законодавству щодо кібербезпеки та захисту особистих даних, забезпечення безпеки та якості харчових продуктів, уникнення надання неякісних харчових послуг, запобігання фізичному та/або психологічному насильству, експлуатації, дискримінації за будь-якою ознакою, порушенню честі, гідності та ділової репутації, також включає в себе боротьбу з булінгом, поширенням неправдивих відомостей, пропагандою та/або агітацією, включаючи використання кіберпростору. Крім того, забороняється вживання алкогольних напоїв, тютюнових виробів, наркотичних засобів, психотропних речовин та інших психоактивних речовин на території та в приміщеннях закладу освіти [13].

Безпечне освітнє середовище ЗЗСО, що включає в себе кібербезпечне освітнє середовище ЗЗСО, зумовлює підвищення кваліфікації педагогічних працівників шляхом проведення різних заходів щодо забезпечення кібербезпеки у ЗЗСО. Також необхідно впроваджувати ефективні заходи забезпечення безпеки мережі та пристроїв, таких як встановлення антивірусного програмного забезпечення та брандмауерів. Крім того, необхідно встановлювати чіткі правила доступу до конфіденційних даних і відомостей та забезпечувати їх безпечне зберігання в ЗЗСО.

Політику кібербезпечного освітнього середовища ЗЗСО можна впроваджувати шляхом рекомендацій щодо встановлення складних паролів та їх періодичній зміні, оновлення програмного забезпечення та операційної системи пристроїв, щоб запобігти кібератакам тощо.

Висновки та перспективи подальших досліджень. Здійснивши аналіз теоретичних підходів щодо визначення проблеми розвитку цифрової компетентності з кібербезпеки вчителів закладів загальної середньої освіти нами було:

Обґрунтовано актуальність проблеми розвитку цифрової компетентності з кібербезпеки вчителів закладів загальної середньої. Зокрема, проаналізовано звіт від Microsoft 2023 рік де підкреслено, що приблизно 99% кібератак відбуваються через недостатнє розуміння користувачами основ кібергігієни. Досліджено другий додатковий протокол до Конвенції про кіберзлочинність (Будапештська конвенція), що спрямований на посилення співпраці та розкриття електронних доказів був підписаний державами-членами Ради Європи, у якому зазначено про посилену співпрацю та розкриття електронних доказів.

Розглянуто підходи до визначення понять: «кібербезпека», «кібергігієна», «кібератака», «кіберзагроза», «кібертероризм», «кіберзахист», «кіберзлочин», «кіберзлочинність»,

«кіберпростір», «цифрова компетентність вчителів», «заклади загальної середньої освіти», «безпечне освітнє середовище» та ін.

Визначено 5 основ кібергігієни, які були сформовані спеціалістами Microsoft і подані у звіті про цифровий захист Microsoft 2023 р.: застосування багатофакторної автентифікації; дотримання принципів моделі «нульової довіри»; використання засобів розширеного виявлення й реагування, захист від шкідливих програм; своєчасне оновлення засобів і програм; захист даних.

Описано безпечне освітнє середовище ЗЗСО, яке включає в себе кібербезпечне освітнє середовище ЗЗСО, і зумовлює підвищення кваліфікації педагогічних працівників шляхом проведення різних заходів щодо забезпечення кібербезпеки у ЗЗСО.

Отже, забезпечення кібербезпеки повинно стати одним з важливих завдань для ЗЗСО у цифровому світі. Необхідно приділяти належну увагу заходам з кібербезпеки, організовувати регулярне навчання для педагогічних працівників, учнів та їх батьків чи опікунів, і постійно вдосконалювати свої системи та програмне забезпечення. Тільки таким чином ЗЗСО зможуть ефективно захищати свої системи та дані від потенційних кіберзлочинців.

Подальші розвідки плануємо спрямувати на більш глибше дослідження щодо заходів кібербезпеки у ЗЗСО.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі : Постанова Кабінету Міністрів України від 04.04.2023 № 299. URL: https://zakon.rada.gov.ua/laws/show/299-2023-%D0%BF#Text (дата звернення: 10.12.2023).

2. Дубов Д. В., Ожеван М. А. Майбутнє кіберпростору та національні інтереси України : нові міжнародні ініціативи провідних геополітичних гравців : аналіт. доп. Київ : НІСД, 2012. 32 с.

3. Звіт про цифровий захист Microsoft за 2023 рік. URL: https://www.microsoft.com/uk-ua/security/security-insider/microsoft-digital-defense-report-2023 (дата звернення: 03.01.2024).

4. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. ; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. Київ : ДУТ, 2015. 288 с.

5. Інформаційно-цифрова компетентність сучасного педагога. AR Book – платформа для вчителів та шкіл. URL: https://arbook.info/informaczijno-czyfrova-kompetentnist-suchasnogo-pedagoga (дата звернення: 16.01.2024).

6. Кормич Б. А. Організаційно-правові засади політики кібербезпеки України : монографія. Одеса : Юридична література, 2003. 472 с.

7. Лісовська Ю. П. Кібербезпека : ризики та заходи : навч. посібник. Київ : Видавничий дім «Кондор», 2019. 272 с.

8. Основи інформаційної безпеки / Андреєв В. І., Хорошко В. О., Чередниченко В. С. , Шелест М. Є. 2-е вид., доп. і перероб. Київ : ДУІКТ, 2009. 292 с.

9. Офіс Ради Європи в Україні. Новини та Заходи. URL: https://www.coe.int/uk/web/kyiv/-/enhanced-co-operation-and-disclosure-of-electronic-evidence-22-countries-sign-new-protocol-to-cybercrime-convention (дата звернення: 12.01.2024).

10. Павленко В. В., Петровська О. Ю. Цифрова компетентність майбутнього учителя як чинник забезпечення якості педагогічної діяльності. *Актуальні проблеми в системі освіти: загальноосвітній заклад середньої освіти – доуніверситетська підготовка – заклад вищої освіти*, 1(2), 633–640. URL : https://doi.org/10.18372/2786-5487.1.16649.

11. Порядок взаємодії суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти/кібератаки одноголосно затверджено на засіданні НКЦК від 22.09.2022. URL: http://surl.li/eybfv (дата звернення: 05.12.2023).

12. Пріма Р.М., Гончарук О.В, Пріма Д.А. Цифрова компетентність майбутнього педагога як необхідна складова забезпечення якості професійної майстерності. *Педагогічні науки: теорія, історія, інноваційні технології*, 2023, № 2 (126) С. 398–409. DOI: 10.24139/2312-5993/2023.02/398-409.

13. Про освіту : Закон України від 05.09.2017 № 2145-VIII. Дата оновлення : 08.12.2023. URL: https://zakon.rada.gov.ua/laws/show/2145-19#Text (дата звернення: 09.01.2024).

14. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. Дата оновлення : 28.07.2022. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 20.12.2023).

15. Про рішення Ради національної безпеки і оборони України від 14.05.2021 «Про Стратегію кібербезпеки України» : Указ Президента України. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n12 (дата звернення: 22.12.2023).

16. Рамка цифрової компетентності педагогічного й науково-педагогічного працівника. URL: https://osvita.diia.gov.ua/uploads/0/2900-2629_frame_pedagogical.pdf (дата звернення: 18.01.2024).

17. Що таке кібербезпека? Microsoft. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-cybersecurity (дата звернення: 10.01.2024).