Scientific journal
PHYSICAL AND MATHEMATICAL EDUCATION
Has been issued since 2013.
Науковий журнал
ФІЗИКО-МАТЕМАТИЧНА ОСВІТА
Видається з 2013.

p-ISSN 2413-1571
e-ISSN 2413-158X

DOI: 10.31110/2413-1571

https://fmo-journal.org/

DOI **10.31110/fmo2024.v39i2-05**

УДК **378.046.4:004**

ПРОБЛЕМА РОЗВИТКУ ЦИФРОВОЇ КОМПЕТЕНТНОСТІ З КІБЕРБЕЗПЕКИ ВЧИТЕЛІВ ЗАКЛАДІВ ЗАГАЛЬНОЇ СЕРЕДНЬОЇ ОСВІТИ

Валентина КОВАЛЕНКО ✉
Інститут цифровізації освіти НАПН України, Україна
vako88@ukr.net
https://orcid.org/0000-0002-4681-5606

Тетяна ОСИПЧУК
Інститут цифровізації освіти НАПН України, Україна
tanyagv0506@gmail.com
https://orcid.org/0000-0003-3075-1246

АНОТАЦІЯ

У статті досліджено проблему розвитку цифрової компетентності з кібербезпеки вчителів закладів загальної середньої освіти. Проаналізовано наукові публікації щодо розвитку цифрової компетентності вчителів закладів загальної середньої освіти, зокрема, з кібербезпеки. Проаналізовано типи загроз для кібербезпеки які були визначені спеціалістами Microsoft. Сформовано способи захисту які необхідно використовувати для забезпечення кібербезпечного освітнього середовища закладу загальної середньої освіти.

Формулювання проблеми. Для даного дослідження важливим є представлення проблеми розвитку цифрової компетентності з кібербезпеки вчителів закладів загальної середньої освіти та визначення способів забезпечення кібербезпечного освітнього середовища закладу загальної середньої освіти.

Матеріали і методи. Використано комплекс методів: аналіз, систематизація, узагальнення наукових джерел, аналіз наукових публікацій вітчизняних і закордонних вчених, узагальнення власного досвіду та ін.

Результати. У дослідженні представлено проблему розвитку цифрової компетентності з кібербезпеки вчителів закладів загальної середньої освіти та сформовано способи захисту які необхідно використовувати для забезпечення кібербезпечного освітнього середовища закладу загальної середньої освіти: автентифікація та авторизація, шифрування даних, захист мережі та захист від шкідливих програм, свідомість користувачів мережі, забезпечення резервного копіювання даних, моніторинг і виявлення незвичайної активності, регулярне оновлення програмного забезпечення, розробка та виконання політики безпеки.

Висновки. Підвищення рівня своєї цифрової компетентності з кібербезпеки вчителів закладів загальної середньої освіти є необхідним та буде здійснюватися шляхом участі вчителів у лекціях, семінарах, вебінарах, круглих столах та інших заходах, а також через співпрацю з провідними експертами в галузі кібербезпеки. Ці заходи сприятимуть не лише професійному зростанню вчителів, але й нададуть можливість забезпечити учнів, а також їх батьків чи опікунів, необхідними знаннями, уміннями та навичками у сфері принципів кібербезпеки у віртуальному просторі.

КЛЮЧОВІ СЛОВА: *кібербезпека; кібератака; кіберпростір; цифрова компетентність вчителів; професійний розвиток вчителів; самоосвіта вчителів; заклади загальної середньої освіти.*

Для цитування:	Коваленко В., Осипчук Т. Проблема розвитку цифрової компетентності з кібербезпеки вчителів закладів загальної середньої освіти. *Фізико-математична освіта*, 2024. Том 39. № 2. С. 35-41. DOI: 10.31110/fmo2024.v39i2-05
	Коваленко, В. & Осипчук, Т. (2024). Проблема розвитку цифрової компетентності з кібербезпеки вчителів закладів загальної середньої освіти. *Фізико-математична освіта*, *39*(2), 35-41. https://doi.org/10.31110/fmo2024.v39i2-05
For citation:	Kovalenko, V., & Osypchuk, T. (2024). The problem of developing digital competence in cyber security of teachers of general secondary education institutions. *Physical and Mathematical Education*, *39*(2), 35-41. https://doi.org/10.31110/fmo2024.v39i2-05
	Kovalenko, V., & Osypchuk, T. (2024). Problema rozvytku tsyfrovoi kompetentnosti z kiberbezpeky vchyteliv zakladiv zahalnoi serednoi osvity [The problem of developing digital competence in cyber security of teachers of general secondary education institutions]. *Fizyko-matematychna osvita – Physical and Mathematical Education*, *39*(2), 35-41. https://doi.org/10.31110/fmo2024.v39i2-05

✉ Corresponding author

THE PROBLEM OF DEVELOPING DIGITAL COMPETENCE IN CYBER SECURITY OF TEACHERS OF GENERAL SECONDARY EDUCATION INSTITUTIONS

Valentyna KOVALENKO ✉
Institute of digitalization of education of NAES of Ukraine, Ukraine
vako88@ukr.net
https://orcid.org/0000-0002-4681-5606

Tetiana OSYPCHUK
Institute of digitalization of education of NAES of Ukraine, Ukraine
tanyagv0506@gmail.com
https://orcid.org/0000-0003-3075-1246

ABSTRACT

The article examines the problem of developing digital competence in cyber security of teachers of general secondary education institutions. Scientific publications on the digital competence development of teachers of general secondary education institutions, particularly on cyber security, were analyzed. The types of cyber security threats identified by Microsoft specialists were analyzed. Protection methods have been developed that must be used to ensure a cyber-safe educational environment in a general secondary education institution.

Formulation of the problem. This study presents the problem of developing digital competence in cyber security among teachers of general secondary education institutions and determines ways to ensure a cyber-safe educational environment.

Materials and methods. We used a complex of methods, including analysis, systematization, generalization of scientific sources, analysis of scientific publications of domestic and foreign scientists, and generalization of our own experience.

Results. The study presents the problem of developing digital competence in cyber security of teachers of general secondary education institutions and forms protection methods that must be used to ensure a cyber-safe educational environment of a general secondary education institution: authentication and authorization, data encryption, network protection and protection against malicious programs, awareness of network users, provision of data backup, monitoring and detection of unusual activity, regular software updates, development and implementation of security policies.

Conclusions. Increasing the level of cyber security digital competence of teachers of general secondary education institutions is necessary. Teachers are expected to participate in lectures, seminars, webinars, round tables, and other events, as well as through cooperation with leading experts in the field of cyber security. Those activities will contribute not only to the professional growth of teachers but also provide an opportunity to give students, as well as their parents or guardians, the necessary knowledge, skills, and abilities in the field of cyber security principles in the virtual space.

KEYWORDS: *cyber security; cyber attack; cyberspace; digital competence of teachers; professional development of teachers; self-education of teachers; institutions of general secondary education.*

ВСТУП

Постановка проблеми. У Стратегія кібербезпеки України зазначено, що пандемія COVID-19 матиме довготривалий вплив на світовий порядок, посилюючи роль цифрових технологій у повсякденному спілкуванні та роботі, що призводить до збільшення вразливості процесів опрацювання інформації, зокрема особистих даних (Указ Президента України Про рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України», 2021). Вважаємо, що і воєнний стан по всій території України, який ще більше посилив роль цифрових технологій в роботі, навчанні та повсякденному житті кожного громадянина нашої держави.

Необхідність захисту національних інтересів від кіберзагрози змушує Україну впроваджувати додаткові заходи для забезпечення належного рівня захищеності інформаційних ресурсів і систем. Для більш ефективної протидії кіберзагрозам, необхідно швидко виявляти вразливості та кібератаки, реагувати на них та поширювати інформацію для мінімізації можливої шкоди. Однак, у змінюваному цифровому світі, необхідна більш збалансована та ефективна національна система кібербезпеки, яка зможе адаптуватися до змін безпечного кіберсередовища, гарантуючи безпечне функціонування національного сегмента кіберпростору. Це дозволить стимулювати цифрову трансформацію всіх сфер суспільного життя (Указ Президента України Про рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України», 2021).

Кібербезпека є вкрай актуальним та важливим питанням у суспільстві. На тлі стрімкого розвитку цифрових технологій та постійного використання Інтернет мережі, загрози кібератак та кіберзлочинів стають все більш серйозними та різноманітними.

Нині користувачу потрібно розуміти хто є кіберзлочинцями і чому це небезпечно та вживати заходів для захисту своїх особистих даних, відомостей, фінансів, робочих даних тощо. Важливо усвідомити, що доступ до технічних пристроїв та даних – це головна мета кіберзлочинців. Комп'ютер чи смартфон може стати інструментом для вірусів та різних атак. Злочинці можуть навіть використовувати чужі пристрої для майнінгу криптовалют та заражати шкідливим програмним програмне забезпечення пристроїв користувачів мережі. Також на меті у кіберзлочинців може бути доступ до інформації, яка може включати особисті дані і дані організацій, використовуючи їх для шахрайства або корпоративного шпигунства. Банківські дані чи дані карт для виплат, кредитних карток, можуть бути викрадені для незаконного зняття грошей з рахунків.

Важливо розуміти, що незалежно від того, наскільки потужні технічні засоби безпеки встановлені на пристроях чи в мережі, завжди залишається найбільш вразливий – людський фактор. І саме користувач через некомпетентність чи недбалість може вчинити якісь непередбачувані дії чим можуть скористатися кіберзлочинці.

Відсутність правил кібербезпеки у соціальних мережах, також є досить поширеним явищем. У соціальних мережах зловмисники використовують психологічні трюки для отримання конфіденційної інформації про користувача чи його організацію. Найпоширенішими проблемами є недостатнє розуміння користувачами основ кібербезпеки, що може призвести до різних видів кібератак.

Також, не варто недооцінювати і внутрішні загрози в організаціях, оскільки недобросовісні чи незадоволені співробітники можуть спричинити витік важливої інформації, або атакувати мережу вірусами чи іншими шкідливими програмами.

Важливість даного дослідження підсилюється і звітом від Microsoft за 2023 рік (Звіт про цифровий захист Microsoft за 2023 рік, 2023) де зазначено, що приблизно 99 % кібератак відбуваються через недостатнє розуміння користувачами основ кібербезпеки.

Тому, через поширення цифрових технологій проблема кібербезпеки стала однією з найважливіших у сучасному цифровому суспільстві, що призвело до значного збільшення кількості кіберзагроз, таких як віруси, хакерські атаки та ін.

Негативні наслідки цих кіберзагроз можуть бути посяганням на безпеку користувачів в мережі Інтернет, наприклад, втрата користувачами їх конфіденційних відомостей, особистих даних, можливі фінансові втрати та ін., що порушить приватність користувачів та може призвести до серйозних моральних та матеріальних збитків для кібержертв.

Досить велика кількість конфіденційної інформації зберігається в закладах освіти, зокрема, закладах загальної середньої освіти, де пристрої мають доступ до мережі Інтернет та мережі самого закладу загальної середньої освіти (ЗЗСО), що робить їх особливо небезпечними для кібератак.

Аналіз актуальних досліджень. Проаналізуємо деякі наукові публікації, щодо проблеми розвитку цифрової компетентності з кібербезпеки вчителів закладів загальної середньої освіти.

На думку Арсенович Л. А. (2022), наскрізним викликом для України є активний розвитку цифрових технологій та прискорення інновацій та їх використанням. Величезна потреба в висококваліфікованих кадрах виникає з метою трансформації економіки країни в умовах цифрової трансформації та воєнного стану на території України, що спричинило чималий відтік кадрів у різних сферах життєдіяльності країни. Однак основним викликом, продовжує бути, недостатня готовність українського суспільства до "цифрового виклику", яка виявляється у недостатній кількості фахових цифрових компетенцій та компетентностей серед значної частини працездатного населення. Проблема включає в себе вирішення питань, пов'язаних з великою кількістю вакансій для фахівців із цифровими навичками та непрацевлаштованими соціально активними громадянами, у яких відсутні ці необхідні навички для ефективною роботи з новими цифровими технологіями. Перехід до онлайн-формату в економіці, освіті, медичному обслуговуванні, ІТ-сфері, державних і фінансових послуг ставить значні групи населення перед цифровими бар'єрами, які обмежують повноцінне забезпечення їх повсякденного життя.

Кашина Г.С. (2020), вважає, що цифрова трансформація у сфері освіти та системи післядипломної педагогічної освіти, в першу чергу виходить з передового досвіду всіх учасників освітнього процесу, таких як керівники закладів освіти, адміністратори, педагогічні та науково-педагогічні працівники. Основна мета цифрової трансформації - забезпечити ефективність управління змінами і гнучко задовольняти потреби якості освітнього процесу. На думку авторки поняття "особистісно-професійний розвиток педагогів природничо-гуманітарних дисциплін у післядипломній освіті", вона розглядає його як "процес неперервного свідомого особистісно-професійного розвитку педагогів природничо-гуманітарних дисциплін у післядипломній освіті". Цей процес відбувається у визначених організаційно-педагогічних умовах з метою вдосконалення професійних знань, умінь, навичок і особистісних якостей, забезпечення високого рівня професійної компетентності, здійснення науково-дослідної діяльності, генерації наукового знання та подальшої професійної самореалізації.

У дослідженні (Корсіков, 2020), зазначено, що сучасна професійна освіта потребує спеціаліста нового типу, який має високу фахову кваліфікацію та професійну культуру і здатний об’єктивно розуміти закономірності явищ і фактів, критично оцінювати та творчо переосмислювати власну дійсність. Це в першу чергу пов’язано, з проблемами саморозвитку особистості та творчою самореалізацією педагога, новими концептуальними підходами до реформування післядипломної педагогічної освіти. Суспільство продовжує висувати високі вимоги до педагогічних працівників, оскільки покращення якості навчання та виховання безпосередньо залежить від рівня підготовки педагогічних працівників. Вчитель має бути добре освіченим в різних галузях науки та сферах суспільного життя. Важливим також є постійна самоосвіта та оволодіння новими знаннями, уміннями і навичками з предмету, який викладає вчитель, ознайомлення з сучасними цифровими технологіями в освіті та наукових дослідженнях, постійному підвищенні рівня своєї педагогічної майстерності.

У публікації (Коваленко та ін., 2021) були сформовані напрями самоосвіти вчителя в умовах цифровізації суспільства, що відображені на рис. 1.

У Законі України «Про основні засади забезпечення кібербезпеки України» зазначено, що: «… *кібербезпека* – це захист життєво важливих інтересів людей, громадян, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі» (Закон України «Про основні засади забезпечення кібербезпеки України», 2022).

Ю. П. Лісовська (2019) вбачає в кібербезпеці також стан захищеності життєво важливих інтересів кожної людини, суспільства і держави в цілому, за якого запобігається нанесення шкоди через:

– неповноту, невчасність та невірогідність інформації, що використовується;

– негативний інформаційний вплив;

– негативні наслідки застосування інформаційних технологій;

– несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Рис. 1. Напрями самоосвіти вчителя в умовах цифровізації суспільства

Джерело: за дослідженням (Коваленко та ін., 2021).

Кіберзлочинці постійно вдосконалюють свої методи кібератак, шукаючи нові вразливі місця в системі та підбирають психологічні методи впливу на користувача, що спричиняє загрози для кібербезпеки.

Спеціалісти Microsoft (Що таке кібербезпека? Microsoft, 2024) розуміють загрозу для кібербезпеки як умисну спроба отримати доступ до системи окремого користувача або цілої організації та визначають такі ***типи загроз для кібербезпеки:***

1. *Шкідливе програмне забезпечення* представляє собою загальний термін для програм, що створені зловмисниками, такими як хробаки, шкідливі програми з вимогою викупу, шпигунське програмне забезпечення та віруси. Це вражає комп'ютери і мережі, змінюючи або видаляючи файли, витягуючи конфіденційні дані, такі як паролі та банківські реквізити, а також поширюючи зловмисні електронні листи чи трафік. Зловмисники, які мають доступ до мережі, можуть встановлювати шкідливе програмне забезпечення, але частіше це відбувається тоді, коли окремі користувачі випадково викликають його, переходячи за ненадійним посиланням або завантажуючи заражене вкладення.

2. *Зловмисна програма з вимогою викупу* – це форма шахрайства, при якій кіберзлочинці шифрують файли за допомогою шкідливого програмного забезпечення та обмежують доступ користувачів до них. Під час таких атак зловмисники часто викрадають дані і вимагають викуп, шантажують користувача, загрожуючи їх публікацією у випадку відмови від оплати. Для отримання ключа розшифрування кібержертвам потрібно здійснити оплату, зазвичай це відбувається у криптовалюті, щоб важко було відсткжити зловмисника. Однак оплата не завжди гарантує відновлення файлів, оскільки не всі ключі розшифрування будуть ефективними.

3. *Соціотехніки*. Зловмисники, використовуючи соціотехніку, стараються втертись в довіру користувачів та шахрайськими методами змушувати їх надавати інформацію про обліковий запис або завантажувати шкідливе програмне забезпечення. Під час таких кібератак зловмисники представляються представниками відомого бренду, колегами або друзями потенційної жертви та використовують психологічні методи, такі як виклик відчуття терміновості, з метою маніпулювання користувачем.

4. *Фішинг* – це метод соціотехніки, при якому кіберзлочинці відправляють електронні листи, а також текстові або голосові повідомлення від імені довіреного джерела з метою переконати користувачів викласти їм доступ до конфіденційної інформації або перейти за невідомим покликанням. Зловмисники проводять фішингові кампанії, спрямовані на широку аудиторію, сподіваючись, що хтось відкриє їх. Інші кампанії, відомі як "цільовий фішинг", мають спрямований характер і націлюються на конкретних користувачів. Наприклад, зловмисник може видати себе за особу, що шукає роботу, і шахрайським чином змусити роботодавця до завантаження ураженого резюме тощо.

5. *Внутрішні загрози* полягають в тому, що користувачі, які вже мають доступ до систем, такі як працівники, підрядники або клієнти, можуть спричиняти порушення вимог кібербезпеки і призводять до фінансових втрат. Іноді це може відбуватися ненавмисно, наприклад, коли працівник випадково розголошує конфіденційну інформацію у своєму особистому обліковому записі. Проте є випадки, коли користувачі роблять це навмисно.

6. *Постійна серйозна загроза*. Принцип дії цієї постійної серйозної загрози полягає в тому, що зловмисники отримують доступ до систем і залишаються непоміченими на протязі значного часового інтервалу. Вони досліджують системи цільової компанії та викрадають дані, уникаючи виявлення своїх дій захисними програмами (Що таке кібербезпека? Microsoft, 2024).

В. Ю. Биков, О. Ю. Буров та Н. П. Дементієвська стверджують, що для створення ефективної стратегії кібербезпеки, придатної для прийняття рішень, необхідно сформулювати просту концепцію, яку користувачі зможуть легко запам'ятати. Один з ефективних методів досягнення цієї мети – це представлення стратегії за допомогою одного слайда у програмі PowerPoint, який може бути представлений протягом 2-5 хвилин. Важливо відзначити, що всі заклади освіти повинні впроваджувати інтегрований підхід до кібербезпеки, спрямований на вирішення проблем, пов'язаних з їх місією. Цей підхід повинен охоплювати технічні та нетехнічні аспекти, залучаючи кваліфікованих та досвідчених фахівців. З метою відповіді на виклики кібербезпеки у наступному десятилітті важливо, щоб заклади освіти забезпечували компетентність викладачів для підготовки майбутніх фахівців до конкурентоспроможності в сучасному освітньому

середовищі. Заклади освіти стикаються з різноманітністю технологічних загроз і новим поколінням молоді, яке активно використовує нові технології, ігноруючи можливі наслідки, що можуть призвести до фізичного, емоційного, психологічного, духовного та економічного виснаження (Биков та ін., 2019).

Погоджуємося з думкою висловленою у публікації (Арсенович, 2022), що важливим елементом професійної компетентності фахівців у сфері кібербезпеки є їх цифрова компетентність. Цифрова компетентність передбачає вміння логічно та системно використовувати інформаційні технології, надає можливість успішно функціонувати в сучасному інформаційному просторі, ефективно керувати інформацією, оперативно приймати рішення та розвивати ключові життєві навички. Фахівець з кібербезпеки має володіти сучасними технологіями та вміло їх використовувати у своїй професійній діяльності, забезпечуючи таким чином важливі інтереси людини, громадянина, суспільства та держави в контексті використання кіберпростору. Це важливо для забезпечення сталого розвитку інформаційного суспільства та цифрового комунікативного середовища, а також для своєчасного виявлення, запобігання і нейтралізації реальних і потенційних загроз національній безпеці України у кіберпросторі.

Проте, проблема розвитку цифрової компетентності з кібербезпеки вчителів закладів загальної середньої освіти не достатньо розкрита і потребує подальшого дослідження.

Мета дослідження: представити проблему розвитку цифрової компетентності з кібербезпеки вчителів закладів загальної середньої освіти та визначити способи забезпечення кібербезпечного освітнього середовища закладу загальної середньої освіти.

МЕТОДИ ДОСЛІДЖЕННЯ

Для досягнення мети дослідження було використано комплекс методів, а саме: аналіз, систематизація, узагальнення наукових джерел, аналіз наукових публікацій вітчизняних і закордонних вчених, узагальнення власного досвіду та ін. На основі прогностичного підходу було визначено шляхи подальших наукових досліджень щодо розвитку цифрової компетентності з кібербезпеки вчителів закладів загальної середньої освіти.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Розвиток цифрової компетентності вчителів у сфері кібербезпеки є важливим складником сучасної освітньої системи загальної середньої освіти. Опанування вчителями необхідними навичками та знаннями з кібербезпеки сприятиме створенню кібербезпечного освітнього середовища ЗЗСО. Освоєння правил кібербезпеки дозволить вчителю зрозуміти основні принципи кібербезпеки, зокрема, захист від кібербулінгу, захист паролів, виявлення онлайн-загроз та шахрайських дій по відношенню до учасників освітнього процесу та від учасників освітнього процесу.

Вчителям ЗЗСО постійно потрібно підвищувати рівень своєї цифрової компетентності, зокрема, з кібербезпеки через участь у лекціях, семінарах, вебінарах, круглих столах та інших заходах, і через співпрацю з провідними експертами у галузі кібербезпеки для отримання консультацій та проведення освітніх заходів. Такі заходи сприятимуть не тільки професійному розвитку вчителів а і можливістю забезпечити учнів та їх батьків/опікунів необхідними знаннями, уміннями та навичками щодо принципів кібербезпеки у цифровому просторі.

Відтак, планування безпечного освітнього середовища для ЗЗСО передбачає комплексний підхід до захисту даних та користувачів, що дозволить створити безпечне та захищене освітнє середовище для всіх його учасників.

Ми вважаємо, що для забезпечення кібербезпечного освітнього середовища закладу загальної середньої освіти необхідно використовувати різні способи захисту, які ми сформували на підставі проведеного дослідження та ґрунтуючись на науковій публікації даного дослідження (Коваленко & Осипчук, 2023) та схематично зобразили їх на рис. 2, а саме:

– *автентифікація та авторизація* (важливо мати механізми перевірки ідентифікації користувачів та контролю доступу до систем, використовувати надійні паролі, багатофакторної автентифікації та обмежувати права доступу, щоб уникнути несанкціонованого доступу до даних та відомостей);

– *шифрування даних* (використання шифрування даних допоможе захистити передачу та збереження цих даних, це забезпечить конфіденційність інформації та обмежить несанкціонований доступ);

– *захист мережі та захист від шкідливих програм* (потрібно мати надійні механізми захисту мережі, наприклад брандмауери та інтерфейси безпеки, для запобігання несанкціонованому доступу до мережі та бази даних; встановлення ефективних антивірусних та антишпигунських програм допоможуть виявляти та видаляти шкідливі програми, які можуть пошкодити систему або отримати доступ до конфіденційної інформації);

– *свідомість користувачів мережі* (користувачів слід навчати основним принципам кібербезпеки, що охоплюють розуміння кіберзагроз, таких як фішинг, шкідливі посилання та вірусні додатки в електронних листах, також важливо зміцнювати захист за допомогою надійних паролів, регулярного оновлення програмного забезпечення та використання безпечних мереж);

– *забезпечення резервного копіювання даних* (важливо мати наявну систему регулярного резервного копіювання, можна створювати резервні копії важливої інформації, що є важливим у випадку втрати або пошкодження даних.);

– *моніторинг і виявлення незвичайної активності* (системи моніторингу та виявлення допомагають своєчасно визначати незвичайну активність або кібератаки. Такий моніторинг допоможе виявляти потенційні загрози та оперативно реагувати на них);

– *регулярне оновлення програмного забезпечення* (потрібно регулярно оновлювати програмне забезпечення, операційні системи та інші компоненти, які використовуються. Виробники постійно випускають оновлення для усунення виявлених вразливостей, і їх своєчасне встановлення є важливим для забезпечення безпеки мережі);

– *розробка та виконання політики безпеки* (розробка та впровадження політики безпеки є ключовою складовою кібербезпеки. Це включає визначення правил, процедур та стандартів, які регулюють доступ до мережі, обмін даними та їх захист).

Рис. 2. Забезпечення кібербезпечного освітнього середовища закладу загальної середньої освіти
Джерело: авторське формулювання грунтуючись на основі дослідження (Коваленко & Осипчук, 2023).

ЗЗСО також мають враховувати ризики, пов'язані з використанням цифрових технологій, які можуть допомогти і полегшити організацію і проведення освітнього процесу та сприяти більш ефективнішому спілкуванню та співпраці учасників освітнього процесу, але в той же час вони можуть стати джерелом загроз для кібербезпеки.

Кібербезпека є невід'ємною складовою успішної діяльності ЗЗСО. Важливо вживати всі можливі заходи для захисту від кіберзагроз, в тому числі розробляти та виконувати плани навчання з кібербезпеки, використовувати спеціалізовані програмні засоби для моніторингу та аналізу кіберзагроз, а також прогнозувати імовірність кібернападу. ЗЗСО повинні бути готові до можливих кіберінцидентів та мати можливість швидко реагувати на них, щоб забезпечити безпеку даних та ефективну роботу закладу.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШОГО ДОСЛІДЖЕННЯ

За результатами проведеного дослідження дійшли певних висновків. Отже, проблема розвитку цифрової компетентності з кібербезпеки вчителів закладів загальної середньої освіти є важливою та актуальною з огляду на швидкоплинний розвиток цифрового суспільства.

Розвиток цифрової компетентності вчителів ЗЗСО з питань кібербезпеки є важливий компонент освітньої парадигми загальної середньої освіти. Впровадження принципів кібербезпеки та оволодіння вчителями ЗЗСО необхідними навичками та знаннями у сфері кібербезпеки сприятиме можливості створенню безпечного цифрового освітнього середовища в закладах загальної середньої освіти.

Підвищення рівня цифрової компетентності вчителів ЗЗСО є необхідною, зокрема, з кібербезпеки і відбуватиметься шляхом участі вчителів у лекціях, семінарах, вебінарах, круглих столах та інших заходах, а також через співпрацю з провідними експертами в галузі кібербезпеки. Ці заходи сприятимуть не лише професійному зростанню вчителів, але й нададуть можливість забезпечити учнів, а також їх батьків чи опікунів, необхідними знаннями, уміннями та навичками у сфері принципів кібербезпеки у віртуальному просторі.

Подальші дослідження варто спрямувати на детальний розгляд різних сервісів для розвитку цифрової компетентності з кібербезпеки вчителів закладів загальної середньої освіти.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про основні засади забезпечення кібербезпеки України» № 2470-IX (2022). *Відомості Верховної Ради* (ВВР). URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.
2. *Звіт про цифровий захист Microsoft за 2023 рік*. (2023). URL: https://www.microsoft.com/uk-ua/security/securityinsider/microsoft-digital-defense-report-2023.
3. Кашина, Г.С. (2020). *Теоретико-методичні засади інформаційно-технологічного забезпечення природничо-гуманітарної підготовки педагогів у системі післядипломної освіти*. Автореф. дис. д-ра пед. наук, Національний педагогічний університет імені М. П. Драгоманова. URL: https://enpuir.npu.edu.ua/bitstream/handle/123456789/35491/100431283.pdf.
4. Коваленко, В.В., Мар'єнко, М.В., & Сухіх, А.С. (2021). Самоосвіта та саморозвиток педагогічних працівників із застосуванням інструментів відкритої науки. *Освітній дискурс: збірник наукових праць,* 37(10), 28-38. https://doi.org/10.33930/ed.2019.5007.37(10)-3.
5. Коваленко, В.В., & Осипчук, Т.О. (2023). Проєктування кібербезпечного освітньо-наукового середовища закладу вищої освіти у площині відкритої науки і освіти. М. П. Шишкіна & О. П. Пінчук (Ред.), *Відкрита наука в умовах інтеграції освіти України до Європейського дослідницького простору : збірник матеріалів І Науково-практичної конференції з міжнародною участю*, (с. 34-36). ІЦО НАПН України. https://lib.iitta.gov.ua/735288.

6. Кормич, Б.А. (2003) *Організаційно-правові засади політики кібербезпеки України*. Юридична література.
7. Корсікова, К.Г. (2020). Самоосвіта сучасного вчителя як безперервний процес удосконалення педагогічної майстерності. *Технології, інструменти та стратегії реалізації наукових досліджень*, 97-99.
8. Лісовська, Ю.П. (2019). *Кібербезпека: ризики та заходи: навч. посібник.* Видавничий дім «Кондор».
9. Порядок взаємодії суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти/кібератаки одноголосно затверджено на засіданні НКЦК (2022). https://www.rnbo.gov.ua/files/2022/NKCK/Порядок_взаємодії.pdf.
10. Указ Президента України Про рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України» (2021). URL: https://zakon.rada.gov.ua/laws/show/447/2021#n12.
11. Що таке кібербезпека? Microsoft. (б. д.). Взято 15 січня 2024 з https://www.microsoft.com/uk-ua/security/business/security-101/what-is-cybersecurity.
12. Kovach, V., Deinega, I., Iatsyshyn, A., Iatsyshyn, A., Kovalenko, V., & Buriachok, V. (2020). Electronic Social Networks as Supporting *Means of Educational Process in Higher Education Institutions. CEUR Workshop Proceedings*, 2588, 418–433. http://ceur-ws.org/Vol-2588/paper35.pdf.
13. Kovalenko, V. V., Marienko, M. V., & Sukhikh, A. S. (2021). Use of Augmented and Virtual Reality Tools in a General Secondary Education Institution in The Context of Blended Learning. *Information Technologies and Learning Tools*, 86(6), 70–86. https://doi.org/10.33407/itlt.v86i6.4664.
14. Marienko, M. V., Nosenko, Yu. H., & Shyshkina, M. P. (2022). Smart systems of open science in teachers' education. *Journal of Physics : Conference Series*, 2288, 012035. https://iopscience.iop.org/article/10.1088/1742-6596/2288/1/012035/pdf.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Zakon Ukrainy «Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy» [The Law of Ukraine "On the Basic Principles of Ensuring Cyber Security of Ukraine"] № 2470-IX. (2022). *Vidomosti Verkhovnoyi Rady – Verkhovna Rada information*. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (in Ukrainian).
2. Zvit pro tsyfrovyi zakhyst Microsoft za 2023 rik. [Microsoft Digital Security Report 2023] (2023). URL: https://www.microsoft.com/uk-ua/security/security insider/microsoft-digital-defense-report-2023 (in Ukrainian).
3. Kashina, G.S. (2020). *Teoretyko-metodychni zasady informatsiino-tekhnolohichnoho zabezpechennia pryrodnycho-humanitarnoi pidhotovky pedahohiv u systemi pisliadyplomnoi osvity*. *[Theoretical and methodological principles of information and technological support of natural and humanitarian training of teachers in the system of postgraduate education]*. Avtoref. dys. d-ra ped. nauk, Natsionalnyi pedahohichnyi universytet imeni M. P. Drahomanova. https://enpuir.npu.edu.ua/bitstream/handle/123456789/35491/100431283.pdf. (in Ukrainian).
4. Kovalenko, V.V., Marienko, M.V., & Sukhikh, A.S. (2021). Samoosvita ta samorozvytok pedahohichnykh pratsivnykiv iz Zastosuvanniam instrumentiv vidkrytoi nauky [Self-education and self-development of pedagogical workers with application tools of open science]. *Osvitnii dyskurs: zbirnyk naukovykh prats – Educational discourse: a collection of scientific papers*, 37(10), 28-38. https://doi.org/10.33930/ed.2019.5007.37(10)-3 (in Ukrainian).
5. Kovalenko, V.V., & Osypchuk, T.O. (2023). Proiektuvannia kiberbezpechnoho osvitno-naukovoho seredovyshcha zakladu vyshchoi osvity u ploshchyni vidkrytoi nauky i osvity [Designing a cyber-safe educational and scientific environment of a higher education Institution education in the field of open science and education]. M. P. Shyshkina & O. P. Pinchuk (Red.), *Vidkryta nauka v umovakh intehratsii osvity Ukrainy do Yevropeiskoho doslidnytskoho prostoru – Open science in the context of the integration of Ukrainian education into the European research space*, 34-36. ITSO NAPN Ukrainy. https://lib.iitta.gov.ua/735288 (in Ukrainian).
6. Kormych, B.A. (2003). *Orhanizatsiino-pravovi zasady polityky kiberbezpeky Ukrainy. [Organizational and legal foundations of cyber security policy of Ukraine].* Yurydychna literatura (in Ukrainian).
7. Korsikova, K.G. (2020). Samoosvita suchasnoho vchytelia yak bezperervnyi protses udoskonalennia pedahohichnoi maisternosti. [Self-education of modern teachers as a continuous process of improving pedagogical skills]. *Tekhnolohii, instrumenty ta stratehii realizatsii naukovykh doslidzhen – Technologies, tools and strategies for the implementation of scientific research*, 97-99. (in Ukrainian).
8. Lisovska, Yu.P. (2019). *Kiberbezpeka: ryzyky ta zakhody: navch. posibnyk. [Cyber security: risks and measures: education. manual].* Vydavnychyi dim «Kondor» (in Ukrainian).
9. Poriadok vzaiemodii subiektiv zabezpechennia kiberbezpeky pid chas reahuvannia na kiberintsydenty/kiberataky odnoholosno zatverdzheno na zasidanni NKTSK [The procedure for the interaction of cyber security entities during the response to cyber incidents/cyber attacks unanimously approved at the meeting of the NCCC] (2022). https://www.rnbo.gov.ua/files/2022/NKCK/Порядок_взаємодії.pdf. (in Ukrainian).
10. Ukaz Prezydenta Ukrainy Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy «Pro Stratehiiu kiberbezpeky Ukrainy» [Decree of the President of Ukraine On the decision of the National Security and Defense Council of Ukraine "On Cyber Security Strategy of Ukraine"] (2021). https://zakon.rada.gov.ua/laws/show/447/2021#n12 (in Ukrainian).
11. Shcho take kiberbezpeka? Microsoft. [What is cyber security? Microsoft] (b. d.). Vziato 15 sichnia 2024 z https://www.microsoft.com/uk-ua/security/business/security-101/what-is-cybersecurity (in Ukrainian).
12. Kovach, V., Deinega, I., Iatsyshyn, A., Iatsyshyn, A., Kovalenko, V., & Buriachok, V. (2020). Electronic Social Networks as Supporting *Means of Educational Process in Higher Education Institutions. CEUR Workshop Proceedings*, 2588, 418–433. http://ceur-ws.org/Vol-2588/paper35.pdf.
13. Kovalenko, V. V., Marienko, M. V., & Sukhikh, A. S. (2021). Use of Augmented and Virtual Reality Tools in a General Secondary Education Institution in The Context of Blended Learning. *Information Technologies and Learning Tools*, 86(6), 70–86. https://doi.org/10.33407/itlt.v86i6.4664.
14. Marienko, M. V., Nosenko, Yu. H., & Shyshkina, M. P. (2022). Smart systems of open science in teachers' education. *Journal of Physics : Conference Series*, 2288, 012035. https://iopscience.iop.org/article/10.1088/1742-6596/2288/1/012035/pdf.

Матеріал надійшов до редакції 22.01.2024р.