УДК 37.018.43

П. Грабовський,
кандидат педагогічних наук,
старший викладач кафедри педагогіки й андрагогіки,
комунальний заклад «Житомирський обласний
інститут післядипломної педагогічної освіти»
Житомирської обласної ради
https://orcid.org/0000-0002-2555-3678
grabovskyp@gmail.com

Протидія кіберзагрозам під час використання цифрових засобів освітньої взаємодії

Анотація. У статті розглядається актуальна проблема, що стосується організації та реалізації дистанційної форми навчання у закладах загальної середньої освіти, зокрема протидія явищам і чинникам, що загрожують педагогічному працівникові у кіберпросторі під час використання відповідних цифрових засобів. На основі аналізу нормативних документів, науково-методичної літератури уточнено сутність основних понять, здійснено класифікацію кіберзагроз та сформульовано рекомендації для протидії їм. Запропоновані матеріали сприятимуть розвитку інформаційно-цифрової компоненти професійних компетентностей учителя.

Ключові слова: кіберзагроза, цифрові інструменти освітньої взаємодії, дистанційна форма навчання.

P. Hrabovskyi,
Candidate of Pedagogical Sciences,
Municipal Institution «Zhytomyr Regional In-Service
Teacher Training Institute» of Zhytomyr Regional Council
https://orcid.org/0000-0002-2555-3678
grabovskyp@gmail.com

Combating cyber threats when using digital means of educational interaction

Abstract. The article considers a topical issue related to the organization and implementation of distance learning in general secondary education. In particular, counteracting the phenomena and factors that threaten the teacher in cyberspace in the process of using appropriate digital tools. On the basis of the analysis of regulations, scientific and methodical literature the essence of the basic concepts is specified, classification of cyberthreats is carried out and recommendations for counteraction to them are formulated. The proposed materials will contribute to the development of information and digital components of teachers' professional competencies.

Keywords: cyber threat, digital tools of educational interaction, distance learning.

Постановка проблеми та актуальність. Наявні умови життєдіяльності (військовий стан, пандемія COVID-19) суттєво впливають на організацію існування українського суспільства. Зокрема, у сфері освіти відбувся перехід до здійснення навчального процесу за дистанційною формою у синхронному та асинхронному режимах [1]. Тому педагогічні працівники закладів різних видів (вищої освіти – ЗВО, загальної середньої – ЗЗСО та ін.) мають організовувати свою професійну діяльність виключно на основі відповідних цифрових засобів освітньої взаємодії: системи управління навчальною діяльністю (*Learning Management System – LMS*); програм та хмарних сервісів для відеоконференцзв'язку, комп'ютерного тестування; використовувати хмарні сховища даних і т. д. Разом з тим це сприяє збільшенню ризиків реалізації відповідних кіберзагроз, що існують у цифровому інформаційному просторі, а отже, вимагає забезпечення належного рівня захищеності та змушує користувачів впроваджувати додаткові механізми і заходи щодо належного функціонування і захисту всіх необхідних інформаційних ресурсів і систем. Особливо це актуально для педагогів ЗЗСО, оскільки у таких закладах зазвичай відсутні працівники за штатом, які мають забезпечувати відповідну протидію можливим кіберзагрозам. Проте, згідно з діючим професійним стандартом для вчителя ЗЗСО, педагогічний працівник має дотримуватися правил безпеки в цифровому середовищі, зокрема уникати небезпек в інформаційному просторі; забезпечувати захист і збереження персональних даних (власних, а також інших осіб, якщо вони використовуються вчителем у професійній діяльності) [2].

Аналіз останніх досліджень і публікацій. Теоретичні та практичні аспекти реалізації дистанційної форми навчання за допомогою відповідних цифрових засобів у закладах освіти представлені у наукових дослідженнях численної когорти українських та іноземних вчених: Т. Андерсона, В. Бикова, Д. Гарісона, В. Кухаренка, Н. Морзе, В. Олійника та інших. Проблематика інформаційної безпеки, протидії кіберзагрозам, що можуть бути реалізовані у цифровому освітньому середовищі, розвитку цифрової компетентності фахівців із кібербезпеки в освітньому процесі представлена у роботах Л. Арсеновича [3], В. Бикова, О. Бурова [4], М. Шабатури [5] та інших.

У відповідних нормативних документах (Закон України «Про основні засади забезпечення кібербезпеки України», «Стратегія кібербезпеки України») визначаються основні поняття:

– «кіберзагроза» – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів»;

– «кібербезпека» – захищеність життєво важливих інтересів людини і громадянина, 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»;

– останній розуміється як «середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі «Інтернет» та/або інших глобальних мереж передачі даних»;

– «кіберзлочин» – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України;

– а також «кібершпигунство», «кіберрозвідка», «кібертероризм» та інші [6; 7].

Крім того, програмними документами ООН [8] визначається, що доцільно формувати та розвивати глобальну культуру кібербезпеки, зокрема і у пересічних користувачів цифрових засобів, на основі таких взаємодоповнюючих елементів: 1) поінформованість; 2) відповідальність; 3) реагування; 4) етика; 5) демократія; 6) оцінка ризику; 7) проєктування і впровадження засобів забезпечення безпеки тощо.

Водночас широкомасштабна реалізація дистанційної форми навчання у ЗЗСО (як найбільш безпечної у наявних умовах) із застосуванням необхідних цифрових засобів обумовлює додаткові виклики у діяльності вчителя та вимагає розвитку відповідних компонентів його професійної компетентності.

Мета даної статті – систематизація та узагальнення рекомендацій для педагогічних працівників щодо протидії кіберзагрозам у процесі реалізації дистанційної форми навчання у ЗЗСО за допомогою відповідних цифрових засобів освітньої взаємодії.

Виклад основного матеріалу. Для досягнення зазначеної мети передусім уточнимо тлумачення поняття «кіберзагроза» у науково-методичній літературі. Оскільки пропоноване визначення цього поняття у Законі України «Про основні засади забезпечення кібербезпеки України» [6] (наведене вище) акцентує увагу на небезпеці життєво важливих національних інтересів держави у кіберпросторі, а це створює враження, що такі негативні дії до процесу освітньої взаємодії між учителями, учнями та їхніми батьками не стосуються. Проте у відповідних літературних джерелах загальноприйнятого визначення цього поняття немає. У межах цієї статті під терміном «кіберзагроза» розумітимемо протиправні, карані дії суб'єктів інформаційних правовідносин, які створюють небезпеку життєво важливим інтересам людини, суспільства та держави загалом, реалізація яких залежить від належного функціонування інформаційних систем, а також відносинам щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації [9]. Наведене визначення, на думку автора статті, краще розкриває сутність поняття та акцентує увагу на протиправності та можливості таких негативних дій щодо пересічного

громадянина, який бере участь у різних сферах життєдіяльності суспільства, зокрема і освітній.

Крім того, важливо здійснити класифікацію наявних кіберзагроз. Для цього розглянемо їх у хронологічній послідовності появи та технологічному аспекті реалізації.

В історичному ракурсі можемо виокремити такі кіберзагрози: програмно-технічні (ціль – ураження програмно-апаратного забезпечення інформаційно-комунікаційних систем та мереж); економічні (зловмисне використання систем інтернет-платежів, інтернет-банкінгу тощо); контентні (викрадення та зловмисне використання даних із соціальних мереж, хмарних сховищ, розповсюдження реклами, пропаганда наркотиків, насильства, злочинів та відео щодо їх скоєння тощо).

Зазначені протиправні дії здійснюються із застосуванням відповідного шкідливого програмного забезпечення, що здатне до самопоширення у інформаційно-комунікаційних системах (різноманітні комп'ютерні віруси: вимагачі, знищувачі, кейлогери, майнери та інші). До того ж, зловмисники поєднують застосування цифрових засобів, зокрема і телекомунікаційних, із технологіями соціальної інженерії для спонукання людини або групи людей, які є «потенційними жертвами», до «потрібних» для правопорушників дій. Зокрема, у такий спосіб здійснюються такі види кіберзагроз, як смішинг (застосування повідомлень через sms у злочинних цілях), вішинг (використання телефонних дзвінків зловмисниками), фішинг (створення копій офіційних вебресурсів), бейтінг (розповсюдження зловмисником зовнішніх носіїв даних, зокрема usb-флеш накопичувачів із шкідливим програмним забезпеченням).

Загалом кіберзагрозам притаманні такі ознаки та властивості:

– реалізуються у модульваному за допомогою цифрових засобів інформаційному просторі;

– масштаб загроз інформаційному простору не обмежується кордонами однієї держави;

– цифрові пристрої та відповідне програмне забезпечення може бути як засобом вчинення, так і предметом злочину;

– швидкозмінні та високотехнологічні;

– реалізація кіберзагроз передбачає відповідну «компетентність» злочинця;

– високий рівень латентності.

Враховуючи зазначене, для здійснення ефективної протидії кіберзагрозам, що можуть виникнути у процесі реалізації дистанційної форми навчання педагогічним працівником ЗЗСО за допомогою цифрових інструментів, він має бути поінформованим про ці загрози, здатним оцінювати потенційні ризики своєї діяльності у кіберпросторі, дотримуватись етики поведінки, належним чином реагувати та відповідально користуватися такими засобами.

Зокрема, для поінформованості потрібно систематично ознайомлюватися з відповідними офіційними інформаційними ресурсами. Наприклад, з нормативними документами [6; 7], рекомендаціями на вебсайті кіберполіції

України та у періодичних виданнях [10], з матеріалами освітніх платформ [11] тощо.

Також педагогічному працівнику ЗЗСО доцільно дотримуватися таких рекомендацій:

– використовувати ліцензійне програмне забезпечення, зокрема операційну систему, пакет офісних додатків (текстовий редактор, табличний процесор та інші);

– мінімізувати використання безкоштовного програмного забезпечення та уникати використання «взламаного» програмного забезпечення, надавати перевагу відповідним хмарним сервісам із аналогічним функціоналом;

– обов'язково використовувати брадмауер та антивірус, зокрема версії, доступні на безоплатній основі (Avast Free Antivirus, Kaspersky Security Cloud Free, Avira Free Antivirus та інші), що передбачають можливість оновлення власних баз із офіційних ресурсів;

– систематично оновлювати все програмне забезпечення, якщо є можливість, зокрема операційну систему, браузер, офісні застосунки тощо;

– надавати перевагу 64-розрядним версіям програмного забезпечення (зокрема і операційним системам), що є більш продуктивними за свої 32-розрядні аналоги та вважаються краще захищеними від можливого ураження комп'ютерними вірусами;

– уникати або мінімізувати використання «не своїх» зовнішніх носіїв даних, особливо флеш-накопичувачів, які були знайдені у громадських місцях;

– здійснювати резервне копіювання даних (бекап) за правилом – не менше трьох копій із застосуванням двох видів сховищ (наприклад, локальне на цифровому пристрої та хмарне) і одна із копій фізично зберігається окремо від інших;

– завжди блокувати цифровий пристрій (персональний комп'ютер, ноутбук, смартфон, планшет тощо), якщо він не використовується та перебуває у громадському місці;

– застосовувати, наскільки можливо, біометричне розблокування цифрового пристрою або складні паролі: не менше 8 символів, включно із цифрами, літерами верхнього та нижнього регістрів, спеціальних символів (розділові знаки, математичні тощо);

– не використовувати як пароль ім'я, прізвище, номер телефону, дату народження, фразу зі щоденного вжитку, назв книг, відомих цитат, текстів пісень тощо;

– користуватися сервісами генерації паролів, зокрема ресурсом кіберполіції України (URL: https://www.cyberpolice.gov.ua/generate-password/);

– систематично змінювати паролі до важливих ресурсів щомісяця, у інших випадках – щоквартально;

– відповідально зберігати паролі, не пересилати їх за допомогою месенджерів;

– уникати або мінімізувати підключення та використання безкоштовних мереж Wi-Fi, у яких зловмисники можуть викрасти особисті дані;

– у операційній системі Windows працювати в мережі «Інтернет» з облікового запису «Гість»;

– уникати використання для доступу до потрібних хмарних сервісів чужих пристроїв або використовувати для цього у браузері режим «Гість» чи анонімного перегляду;

– застосовувати, наскільки можливо, двофакторну аутентифікацію (підтвердження того, що користувач є саме тим, за кого себе видає, двома різними способами, наприклад, за допомогою введення постійного пароля та тимчасового, що був надісланий на зазначений номер мобільного телефону, який належить особі і контролюється нею) у процесі авторизації у потрібному хмарному сервісі;

– надавати перевагу вебресурсам, що функціонують на основі протоколу HTTPS (англ. *HyperText Transfer Protocol Secure*, дослівний переклад – захищений протокол передачі гіпертексту), що передбачає шифрування даних, які надсилаються браузером/браузерові користувача до/від сервера, що обслуговує вебресурс (відповідне попередження про підтримку HTTPS чи HTTP ресурсом сучасні браузери демонструють у адресній стрічці);

– сформувати звичку аналізувати отримані повідомлення, телефонні дзвінки, які спонукають до негайних дій або надають можливість отримання певних винагород чи бонусів на приналежність до технологій соціальної інженерії;

– уникати розміщення в мережі приватної інформації фото, відеоматеріалів, аудіозаписів, фотодокументів, номерів телефону, зокрема фінансового, за допомогою якого реалізується інтернет-банкінг;

– слід пам’ятати, що інформацію, яка потрапила в інтернет, дуже складно, а часом і взагалі неможливо видалити, тому перед її завантаженням потрібно оцінити можливі ризики через це.

Зазначимо, що значна кількість педагогічних працівників ЗЗСО у процесі організації та здійснення дистанційного навчання застосовують хмарні сервіси Google особистого облікового запису користувача (для таких записів електронна адреса користувача відповідає шаблону exampleyourtext@gmail.com). Для таких осіб для протидії кіберзагрозам можливе застосування функціоналу хмарного сервісу «Обліковий запис», що наявний у переліку доступних додатків Google на безоплатній основі. Зокрема, за допомогою цього цифрового інструменту можливе налаштування конфіденційності: які дані із особистих, що були внесені при реєстрації облікового запису, будуть бачити інші користувачі; чи має фіксуватися геолокація, відслідковуватися вподобання та інтереси для особистого добору реклами і результатів пошуку; які дії застосувати до всіх даних у хмарному сховищі у випадку, якщо користувач не авторизовувався вказаний ним період часу (можливе знищення або надсилання логіну та пароля користувача вказаній ним особі). Крім того, наявний функціонал дозволить оцінити надійність паролів до різних хмарних додатків (якщо користувач авторизований та працює у браузері Google Chrome, то паролі до вебресурсів, що були збережені і доступні для автозаповнення, передаються у так званий

менеджер паролів облікового запису, що забезпечує можливість їх аналізу, відновлення тощо); здійснити дистанційний вихід із свого облікового запису, якщо залишилось активне підключення на не вашому пристрої але було здійснене вами; активувати двофакторну авторизацію тощо.

Висновки. Зазначені вище рекомендації дозволять педагогічному працівникові закладу загальної середньої освіти ефективно протидіяти можливим кіберзагрозам, що виникатимуть у процесі здійснення ним дистанційної форми навчання за допомогою відповідних цифрових засобів освітньої взаємодії. Запропоновані матеріали доцільно використати як зміст навчання у закладах післядипломної педагогічної освіти в організації процесу підвищення кваліфікації вчителів для забезпечення розвитку інформаційно-цифрової компоненти їхніх професійних компетентностей.

Список використаних джерел та літератури

1. Про затвердження методичних рекомендацій щодо окремих питань завершення 2021/2022 навчального року : наказ Міністерства освіти і науки від 01.04.2022 р. № 290. URL: https://mon.gov.ua/storage/app/uploads/public/624/7f7/087/6247f7087d9f763589810 8.pdf (дата звернення: 16.05.2022).

2. Про затвердження професійного стандарту за професіями «Вчитель початкових класів закладу загальної середньої освіти», «Вчитель закладу загальної середньої освіти», «Вчитель з початкової освіти (з дипломом молодшого спеціаліста)» : наказ Міністерства розвитку економіки, торгівлі та сільського господарства України від 23.12.2020 р. № 2736-20. URL: https://zakon.rada.gov.ua/rada/show/v2736915-20#Text (дата звернення: 16.05.2022).

3. Арсенович Л. А. Інструментарій підвищення рівня цифрової компетентності фахівців із кібербезпеки в освітньому процесі. *Кібербезпека: освіта, наука і техніка.* 2022. Т. 3 (15). С. 93–109. DOI10.28925/2663-4023.2022.15.93109 (дата звернення: 16.05.2022).

4. Биков В. Ю., Буров О. Ю., Дементієвська Н. П. Кібербезпека в цифровому навчальному середовищі. *Інформаційні технології і засоби навчання.* 2019. Т. 70 (2). С. 313–331. DOI:10.33407/itlt.v70i2.2876 (дата звернення: 16.05.2022).

5. Шабатура М. М., Тихолаз Д. О., Бумба І. Ю. Дослідження стану кібербезпеки сервісів відеозв'язку. *Кібербезпека: освіта, наука і техніка.* 2021. Т. 1 (13). С. 113–122. DOI 10.28925/2663-4023.2021.13.113122 (дата звернення: 16.05.2022).

6. Про основні засади забезпечення кібербезпеки України : закон України від 05.10.2017 р. № 2136-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 17.05.2022).

7. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : указ Президента України.

URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 17.05.202).

8. Элементы для создания глобальной культуры кибербезопасности : документи ООН. URL: http://www.un.org/ru/documents/decl_conv/conventions/elements.shtml. (дата звернення: 17.05.2022).

9. Діордіца І. Поняття і зміст кіберзагроз на сучасному етапі. *Підприємництво, господарство і право.* 2017. Т. 4. С. 99–107. URL: http://pgp-journal.kiev.ua/archive/2017/4/22.pdf (дата звернення: 17.05.2022).

10. Кібербезка: освіта, наука, техніка : електронне фахове наук. вид. URL: https://csecurity.kubg.edu.ua/ (дата звернення: 17.05.2022).

11. Дія. Цифрова освіта : національна онлайн-платформа з цифрової грамотності. URL: https://osvita.diia.gov.ua (дата звернення: 17.05.2022).