БІБЛІОТЕКОЗНАВСТВО. БІБІЛОГРАФОЗНАВСТВО

УДК 021
DOI 10.32461/2409-9805.3.2023.290974

Цитування:
Ржеуський А. В., Кунанець Н. Е. Роль бібліотеки як соціального інституту в розвитку інформаційної безпеки. *Бібліотекознавство. Документознавство. Інформологія.* 2023. № 3. С. 5–12.

Rzheuskyi A., Kunanets N. (2023). The Role of Library as a Social Institution in the Development of Information Security. Library Science. Record Studies. Informology, 3, 5–12 [in Ukrainian].

Ржеуський Антоній Валентинович,
кандидат наук із соціальних комунікацій,
докторант Національної академії
керівних кадрів культури і мистецтв
https://orcid.org/0000-0001-8711-4163,
antonii.v.rzheuskyi@lpnu.ua

Кунанець Наталія Едуардівна,
доктор наук із соціальних комунікацій,
професор кафедри інформаційних систем та мереж
Національного університету
«Львівська політехніка»,
https://orcid.org/0000-0003-3007-2462,
nek.lviv@gmail.com

РОЛЬ БІБЛІОТЕКИ ЯК СОЦІАЛЬНОГО ІНСТИТУТУ В РОЗВИТКУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Мета *статті полягає у визначенні функцій бібліотек України в напрямі формування інформаційної безпеки держави.* ***Методологія дослідження*** *полягає в застосуванні загальнонаукових та спеціальних методів дослідження: аналізу, синтезу, узагальнення, систематизації матеріалів, індукції та дедукції.* ***Наукова новизна****. Проаналізовано погляди на зміст поняття «інформаційна безпека» закордонних та вітчизняних фахівців. Визначено, що фейки є лише одним із різновидів інформаційних загроз. Встановлено види інформаційних загроз та визначено роль і функції бібліотечних фахівців відповідно до кожного з них щодо запобігання спричинення, а також поширення недостовірної інформації. Розглянуто основні аспекти формування бібліотеками закладів вищої освіти України стратегії інформаційної безпеки.* ***Висновки.*** *Інформаційна безпека є необхідною складовою діяльності бібліотек. Увесь комплекс заходів є важливим для гарантування безпеки інформації в бібліотеці та підвищення довіри користувачів до бібліотеки як до надійного джерела інформації. Для цього слід використовувати такі практики: захист мережі та баз даних бібліотеки (що містять не тільки метадані, а й повнотекстові документи) від несанкціонованого доступу: встановлення брандмауерів, антивірусного програмного забезпечення, регулярне оновлення програмного забезпечення та операційних систем; захист конфіденційної інформації: шифрування даних, контроль доступу до інформації, регулярне оновлення паролів та перевірка безпеки сторонніх сервісів; резервне копіювання даних: забезпечення регулярного резервного копіювання даних для відновлення інформації в разі втрати або пошкодження даних; підготовку співробітників: навчання співробітників правилам інформаційної безпеки, викладення політики безпеки, організація тренінгів та семінарів.*

Ключові слова: *бібліотека, інформаційна безпека, інформаційні загрози, фейки, недостовірна інформація, захист інформації, соціальні мережі, месенджери, інформаційний воротар, блокчейн, сентиментальний аналіз.*

Rzheuskyi Antonii,
Candidate of Sciences in Social Communications (PhD),
Doctoral Student, National Academy of Culture and Arts Management

Kunanets Natalia,
Doctor of Sciences in Social Communications,
Professor, Department of Information Systems and Networks,
Lviv Polytechnic National University

THE ROLE OF LIBRARY AS A SOCIAL INSTITUTION IN THE DEVELOPMENT OF INFORMATION SECURITY

The purpose of the article *is to determine the functions of the libraries of Ukraine in the direction of the formation of information security of the state.* ***The research methodology*** *consists in the application of general scientific and special research methods: analysis, synthesis, generalisation, systematisation of materials, induction, and deduction.* ***Scientific novelty.*** *The views on the content of the concept of "information security" of foreign and domestic specialists were analysed. It was determined that "fakes" are only one of the types of information threats. The types of information threats have been established and the role and functions of library specialists have been determined in accordance with each of them in terms of preventing the occurrence and spread of inaccurate information. The main aspects regarding the formation of information security strategies by libraries of higher education institutions of Ukraine are considered.* ***Conclusions.*** *Information security is an important component of library activity. The entire set of measures is important for ensuring the security of information in the library and increasing users' trust in the library as a reliable source of information. To do this, the following practices should be used: protection of the network and library databases (containing not only metadata, but also full-text documents) from unauthorised access: installation of firewalls, anti-virus software, regular software and operating system updates; protection of confidential information: encryption of data, control of access to information, regular updating of passwords and verification of the security of third-party services; data backup: providing regular data backup to restore information in case of data loss or damage; employee training: training employees in the rules of information security, setting out the security policy, organising trainings and seminars.*

Keywords: *library, information security, information threats, "fakes", unreliable information, information protection, social networks, messengers, information gatekeeper, blockchain, sentimental analysis.*

Актуальність теми дослідження. У минулому інформацію ретельно контролювали представники різних служб, до засобів масової інформації надходила лише перевірена щодо політичної лояльності інформація. Аналогічна ситуація була й у бібліотеках. Законодавство про свободу слова, з одного боку, дозволило журналістам і бібліотекарям вільно висловлювати свої думки, з іншого – відкритий характер цифрового світу ускладнив контроль і перевірку достовірності інформації. Однак поширення дезінформації має потенційно катастрофічні та небезпечні наслідки для політичної та суспільної сфери. У часи, коли люди не знають, яким джерелам довіряти, роль бібліотекарів, які надають достовірну інформацію, є надзвичайно важливою.

Аналіз досліджень і публікацій. У Законі України «Про основи національної безпеки України» до загроз в інформаційній сфері відносять «поширення засобами масової інформації культу насильства, жорстокості; комп'ютерну злочинність та комп'ютерний тероризм, розголошення інформації, яка становить державну та іншу передбачену законом таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави; намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації» [1].

У Законі України «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» інформаційна безпека трактують як «стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому 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» [2].

Згідно з визначенням Національного інституту стандартів та технологій (National Institute of Standards and Technology), інформаційна безпека означає захист інформації та інформаційних систем від несанкціонованого доступу, використання, розголошення, порушення, модифікації або

знищення з метою забезпечення цілісності, конфіденційності та доступності [3].

Метою статті є визначити функції бібліотек України в напрямі формування інформаційної безпеки держави.

Виклад основного матеріалу. Із повномасштабним вторгненням 2022 року інформаційна безпека стала невід'ємною компонентою збереження та розвитку інформаційного суспільства й національної безпеки інформаційного простору України. Соціальні інститути, а саме: архіви, музеї та бібліотеки, у фондах яких зберігаються документальні та електронні інформаційні ресурси, формують історичну пам'ять та національний інтелектуальний капітал держави. Університетські бібліотеки відіграють важливу роль в інформаційному ланцюжку, який становить низку інформаційних процесів, зокрема: отримання, створення, упорядкування, зберігання, індексування та поширення інформації.

Аріф Хан (Arif Khan), Мухаммад Ібрагім (Muhammad Ibrahim), Абід Хусейн (Abid Hussain) вважають, що безпека даних та інформації є однією із головних проблем для бібліотек, особливо в країнах, де розвиток інформаційних і комунікаційних технологій є відносно низьким. Щодо безпеки даних та інформації в університетських бібліотеках Пакистану дослідники зазначають, що ситуація складається не найкращим чином й існують певні недоопрацювання з убезпечення інтелектуальних надбань бібліотек. А саме: відсутність оновленого антивірусного програмного забезпечення та програмного забезпечення для управління бібліотечними процесами, брандмауерів, механізмів тестування та налагодження, оновлених патчів безпеки для операційних систем, дозвіл обмеженого доступу користувачів до баз даних, механізм обміну файлами та ведення журналу доступу. Підключення бездротових пристроїв є одними з критичних питань, які мають розглянути фахівці університетських бібліотек Пакистану. Окрім того, дослідники стурбовані масовим оцифруванням інтелектуальної власності, як-от: дослідницьких проєктів, звітів, тез, дисертацій, що вимагає особливої обережності й уваги через відсутність високотехнологічних засобів збереження та опрацювання даних, з одного боку, та стрімкий розвиток мережевих засобів – з іншого [4].

Одрі Андей (Audrey Anday), Енріко Франчезе (Enrico Francese), Уго С. Хурдеман (Hugo C. Huurdeman), Мухаррем Їлмаз (Muharrem Yilmaz), Дідімус Зенгенене (Dydimus Zengenene) виокремили основні категорії, які стосуються інформаційної безпеки в цифровому середовищі:

Інфраструктура. Зосереджено увагу на важливості інформаційної безпеки, що застосовують у будь-якій системній інфраструктурі, яка охоплює захист апаратного та програмного забезпечення, гарантування інформаційної безпеки мережі та вивчення вразливостей у мережі, які можуть перешкоджати передачі інформації в дротовому чи бездротовому середовищі.

Цифровий контент. Гарантування інформаційної безпеки цифрового вмісту в електронному середовищі, відновлення даних та створення резервних копій є найпоширенішим способом запобігання втраті даних.

Безпека інформації користувача. Розширення використання комп'ютерних технологій призвело до збільшення збору персональних даних, що може призвести до потенційних проблем з конфіденційною інформацією. Пріоритетом є підтримка конфіденційності користувачів у середовищі електронної бібліотеки, тобто особиста інформація користувачів зберігається надійно та не використовується без їх відома [5].

Цайхонг Гао (Caihong Gao) розглядає різноманітні фактори, а саме: хакерські атаки та віруси, неадекватне внутрішнє управління провайдерами хмарних послуг, національні чи регіональні законодавчі конфлікти, які можуть становити загрозу для особистої інформаційної безпеки користувачів бібліотеки, і наголошує, що бібліотечні фахівці повинні вдосконалити політику та правила захисту особистої інформації, прийняти гнучкі стратегії застосування технології конфіденційності [6].

Майкл Мет [7] і Лі Занг [8] розглядають перешкоди та проблеми впровадження технології блокчейн у бібліотеках. Зокрема, Майкл Мет вважає блокчейн перспективною технологією, що здатна змінити спосіб надання бібліотечних послуг, опрацювання та збереження інформації. На нашу думку, технологію блокчейн [9; 10] слід застосовувати для збереження персональних даних користувачів.

Вікас Сінгх (Vikas Singh) і Мадхусудхан Маргам (Madhusudhan Margam) розглядають фізичні, організаційні та технологічні заходи інформаційної безпеки в Університеті Джавахара Лал Неру (Jawahar Lal Nehru University), Університеті Делі (University of Delhi) та Джамія Мілліа Ісламія (Jamia Millia Islamia). Зокрема, технологічна безпека стосується безпеки бібліотечного програмного забезпечення, апаратного забезпечення, мережі, сервера, даних, робочих станцій. Особливу увагу приділено електронним системам безпеки, таким як: RFID, пожежна сигналізація, камери відеоспостереження, детектори руху, смарткарти, біометрична система для відвідування персоналу, технологія захист від злому та штрих-коди [11].

Ннатубемуго Нгвум (Nnatubemugo Ngwum), Сагар Райна (Sagar Raina), Сабіна Агуон (Sabina Aguon), Блер Тейлор (Blair Taylor), Сіддхарт Каза (Siddharth Kaza) визначили п'ять ключових критеріїв для оцінки безпеки електронної бібліотеки, зокрема: шифрування, автентифікація та авторизація, слабкість і вразливість платформи, аудит-системи безпеки, зручність використання та людський фактор [12].

Женбіао Хан (Zhengbiao Han), Швейкінг Хвен (Shuiqing Huang), Хуан Лі (Huan Li), Ні Рен (Ni Ren) встановили, що ризики для електронної бібліотеки проявляються переважно в таких аспектах: стратегія доступу до інформаційних систем, програмного забезпечення, мережі, баз даних мають недоліки або в деяких випадках застосовуються лише частково. Усе це може спричинити загрози (безпека мережі, неправильна робота та несанкціонований доступ) програмному забезпеченню, електронним ресурсам, файлам даних. Механізм резервного копіювання має недоліки. Усі системи та дані створюються локально та зберігаються в одній комп'ютерній кімнаті на одному сервері чи сховищі даних. Виникають такі ризики, як пожежа, збій зв'язку чи інші загрози; тому всі об'єкти, особливо електронні ресурси та масиви електронних документів, піддаються серйозному ризику. І сервери, і персональні комп'ютери вразливі через оновлення системи. Крім того, не встановлено суворої політики контролю доступу, коли систему не вдається оновити вчасно з певних причин. Тому дії хакерів спричиняють такі загрози, як зловмисне проникнення, втручання, деструктивні атаки та виявлення вразливості електронних ресурсів, файлів даних, програмного чи апаратного забезпечення.

Що стосується серверів і парку комп'ютерів бібліотеки, то існують загрози, спричинені низьким рівнем керування паролями, низьким рівнем або навіть відсутню автентифікації особи, незмінними паролями та спільними обліковими записами й паролями [13].

На наш погляд, поняття інформаційної безпеки не може бути обмежене безпекою технічних засобів, інформаційних систем чи безпекою інформації в електронному вигляді. Розглянуті вище дослідження стосуються кібербезпеки автоматизованих бібліотечних систем та електронних інформаційних ресурсів. Спільним у проаналізованих публікаціях є те, що автори розглядають діяльність бібліотек у доковідний період, а також закордонні бібліотеки не перебували у стані війни та не зазнавали подібних інформаційних загроз, на відміну від українських бібліотек (зокрема встановлення паролів до мережі WiFi чи на локальних комп'ютерах у бібліотеці для українських книгозбірень вже не актуально, оскільки бібліотечно-інформаційне обслуговування спрямоване передусім на віддаленого користувача). Ще однією ознакою є те, що в жодній публікації не розглянуто інформаційні загрози, які поширюються через соціальні мережі, що транслюють великий потік інформації, зокрема й дезінформації, фейків, що робить користувачів соціальних мереж вразливими до ненадійних джерел, які можуть спричинити руйнування інформаційного суверенітету [14] нашої держави.

Хорхе Ревес (Jorge Revez), Луїс Корухо, (Luís Corujo) [15], М. Коннор Салліван (M. Connor Sullivan) розглядають роль бібліотечних працівників у боротьбі з поширенням фейкових новин [16].

Бібліотекарів завжди вважали інформаційними воротарями й тими, хто перевіряє факти (fact-checkers), які надають громадськості надійну, неупереджену та перевірену інформацію. Вони традиційно цінують рівний доступ до інформації та визнають важливість здатності людей мислити незалежно й критично для створення ефективного демократичного суспільства. Однак у зв'язку зі збільшенням швидкості та кількості інформації, що поширюється в інтернеті, їхня роль зміщується від інформаційних воротарів до просвітництва [17]. Інформаційна грамотність постає як один із можливих та ефективних методів боротьби з фейковими новинами [18]. Ніколь Єва (Nicole Eva) та Ерін Ши (Erin Shea) наголошують на потенціалі й важливості навичок критичного мислення у війні із фейковими новинами та визнає бібліотекаря експертом і фахівцем, що набув ці навички [19]. Визначення «фейкові новини» в останні роки мало пряму політичну приналежність. Інші дослідники визначили це як новинні статті, які є навмисно згенерованими, підтверджено неправдивими та намагаються ввести читача в оману [20].

Стівен Вейд і Джулі Хорнік з бібліотеки Роекс Південного коледжу Флориди в Лейкленді (Roux Library at Florida Southern College in Lakeland) зазначають, що бібліотекарі навчають користувачів, як перевіряти авторитетність і достовірність джерел, формують навички в користувачів, необхідні для критичного аналізу достовірності постів у соціальних мережах.

Бібліотечні фахівці закликають користувачів ретельно вивчати докази та джерела, використані в пості, і розробили низку питань, за якими можна проаналізувати допис у соціальній мережі: Які докази використано для підтвердження положень у статті? Як використано ці докази? За якими критеріями ми можемо оцінити джерело інформації? Коли анонімні джерела прийнятні? Чи може читач визначити автора? Якщо так, то хто ця особа та яка в неї освіта? Чи можна їх вважати авторитетом? Чому так або ні? Чи є організація, яка відповідає за вміст або фінансування сайту? Чи може спонсор заохочувати автора (авторів) подавати неправдиву інформацію? Якщо так, то як це зменшує або збільшує імовірність упередженості статті? [21].

У публікаціях закордонних колег порушено питання поширення та протидії фейковим новинам у політичній сфері, щодо появи та поширення Covid-19.

На нашу думку, інформаційну грамотність потрібно розвивати, однак ми не погоджуємось із тим, щоб бібліотекарі делегували свою роль користувачам, адже прерогативою бібліотечних працівників як фахівців, що працюють з інформацією, є фільтрація, опрацювання та надання релевантної інформації користувачам, які очікують на неї. Для працівників бібліотек слід проводити семінари, робочі

зустрічі з підвищення інформаційної грамотності.

Серед вітчизняних дослідників питання поширення недостовірної інформації порушували: І. Вільчинська [22], М. Кіца [23], І. Мудра [24], Л. Доскіч та ін. Зокрема, Л. Доскіч охарактеризувала особливості фейкових новин та слушно зауважила, що маніпулюванням шкідливою інформацією реалізують завдання терору та залякування населення [25].

М. Сахарова, Я. Хіміч на прикладі обласних універсальних наукових бібліотек порушили проблему невчасної та недостатньої комунікації, відсутності актуальної інформації на вебсайтах та в соцмережах в акаунтах бібліотек з моменту вторгнення російських військ на територію України [26].

Однак проблематика, яка б стосувалась фейкових новин під час повномасштабної війни Україні, у публікаціях не була висвітлена.

Р. Гула, І. Передерій та В. Сажко висунули думку про те, що головним завданням війни в мережі «стане перенесення центру протиборства з матеріально-військової сфери на інформаційно-духовну» [27].

В. Горовий зазначив, що «соціальні мережі можуть створювати певні небезпеки національному інформаційному простору України через недостатній розвиток технологій нейтралізації негативних, в умовах інформаційної війни, і відкрито ворожих впливів на процеси інформаційних обмінів у суспільстві». Дослідник продовжує думку, що важливою умовою в боротьбі з дезінформацією є обов'язкова присутність інформаційно-аналітичних структур, зокрема й бібліотечних [14].

З огляду на проаналізовані дослідження, ми сформулювали основні аспекти щодо формування бібліотеками закладів вищої освіти України стратегії інформаційної безпеки.

1. Безпечне онлайн-обслуговування. Передусім бібліотеки мають здійснювати онлайн-запис користувачів, запровадити систему віртуальних кабінетів користувачів, де б містилася персональна інформація про користувача, історія його відвідувань, електронних замовлень, термін дії електронного читацького квитка, час перебування в онлайн-режимі. Надати вже зареєстрованому користувачеві доступ до баз даних бібліотеки виключно за індивідуальним паролем, прив'язаним до його електронного читацького квитка.

Бібліотеки відіграють важливу роль у гарантуванні інформаційної безпеки, оскільки можуть зберігати, накопичувати та опрацьовувати значну кількість конфіденційної інформації про своїх користувачів, таку, наприклад, як персональні дані. Тому інформаційна безпека в бібліотеках має бути одним із пріоритетних завдань. Для цього можуть бути використані такі практики:

• Захист мережі та баз даних бібліотеки (що містять не тільки метадані, а й повнотекстові документи) від несанкціонованого доступу: встановлення брандмауерів, антивірусного програмного забезпечення, регулярне оновлення програмного забезпечення та операційних систем.

• Захист конфіденційної інформації: шифрування даних, контроль доступу до інформації, регулярне оновлення паролів та перевірка безпеки сторонніх сервісів.

• Підготовка співробітників: навчання співробітників правилам інформаційної безпеки, викладення політики безпеки, організація тренінгів та семінарів.

• Резервне копіювання даних: забезпечення регулярного резервного копіювання даних для відновлення інформації в разі втрати або пошкодження даних.

2. Достовірність інформації. Оскільки бібліотечно-інформаційне обслуговування відбувається в онлайн-форматі засобами поштової скриньки, онлайн-чату, віртуальної довідкової служби, дистанційного сервісу «пошук літератури за темою дослідження» (за основу цієї послуги взято вибіркове поширення інформації), бібліотечні фахівці набувають функцій інформаційних брокерів. У своїй роботі вони зіштовхуються з великим потоком інформації з різних джерел, кількість яких з кожним днем тільки зростає. А на вимогу користувача необхідно надати інформацію оперативно, у зручному для сприйняття форматі, а головне – перевірену та релевантну. Тому інформаційні працівники, перш ніж надіслати інформацію (а йдеться про забезпечення інформаційних потреб науковців та співробітників закладів вищої освіти), мають детально її вивчити.

Ми запропонували такі рекомендації для визначення достовірності інформації. Бібліотечні працівники мають володіти та розвивати критичний підхід й аналітичне мислення. Працюючи із науковими публікаціями, бібліотечний фахівець повинен звернути увагу на автора, його афіляцію, країну і так не допустити поширення ворожого контенту в науковому інформаційному просторі. Якщо ж це блог з наукової тематики, бібліотечний фахівець повинен звернути увагу на його доменну адресу. Так можна визначити, до якої країни належить інформаційний ресурс. Також слід звертати увагу на списки використаних джерел у науковій статті: там можуть закрастися посилання на інформаційні ресурси, що корелюють з інформаційним простором країни-агресора. Виявивши підозрілі елементи чи сумнів з приводу наукової статті, бібліотечний фахівець має право не допустити поширення такої статті, аби користувач відчував впевненість щодо наданої інформації.

3. Соціальні мережі. Бібліотеки створюють офіційні акаунти в соціальних мережах. Як правило, вони є відкритими для перегляду та коментування користувачами. У площині соціальних мереж бібліотечний фахівець виконує роль інформаційного воротаря: а) вирішує, які новини

транслювати через соціальну сторінку бібліотеки; б) слідкує за розміщенням дописів від користувачів бібліотеки або сторонніх осіб, які зайшли на сторінку бібліотеки в соцмережі.

У першому випадку, коли бібліотечний фахівець збирається розмістити пост або ретранслювати новину, він насамперед має провести детальний аналіз інформації, перевірити факти, джерело новини.

У другому випадку, коли стороння особа вже розмістила інформацію, бібліотечний фахівець має діяти так:

• Визначити актуальність розміщеного матеріалу, коли інформація була опублікована.

• З'ясувати, хто написав / створив / опублікував пост; встановити першоджерело інформації. Джерело опубліковано науковим видавництвом чи авторитетною організацією?

• Встановити особу автора. Які повноваження або організаційна приналежність автора? Чи має автор право писати на певну тему? Бібліотечний фахівець має вивчити інформацію про автора, який розмістив пост, перейшовши у його профіль і переконавшись у професійній компетентності дописувача. Якщо інформація недостатньо вичерпна або профіль закритий, у бібліотечного фахівця вже можуть з'явитися сумніви в достовірності інформації. На нашу думку, користувачі соцмереж, які беруть на себе функцію створення та поширення інформації, повинні мати верифікований профіль.

• Чи використовує автор докази? Чи підтверджують їх інші експерти? Чи враховано різні погляди? Бібліотекар має перевірити факти, на яких ґрунтується пост.

• Визначити тон повідомлення. Чи наявні упередження: політичні, ідеологічні, культурні, релігійні? У цьому питанні бібліотечним фахівцям допоможе метод сентиментального аналізу тексту за допомогою програмних засобів [28; 29].

Лише після опублікування посту в соціальних мережах бібліотечний фахівець може приступити до оцінки інформації. Функції соціальних мереж у разі визнання посту таким, що містить шкідливу та недостовірну інформацію, передбачають такі дії: «видалення коментаря», «поскаржитись на повідомлення», «видалити користувача».

4. Месенджери. Бібліотечні фахівці виступають адміністраторами при створенні спільнот у месенджерах. Для того щоб вступити до спільноти, адміністратор повинен схвалити заявку від користувача. Щоб повідомлення користувача було розміщене в спільноті, його також має схвалити адміністратор після того, як матеріал пройде належну перевірку на предмет правдивості, адже повідомлення в месенджерах також несуть дезінформацію, агресію, розпалювання ворожнечі. Бібліотечний працівник відповідальний за перевірку та розміщення повідомлення користувачів, адже в разі пропуску повідомлення сумнівного характеру, яке виявиться фейком, воно миттєво поширюється в мережі з багатотисячною аудиторією та здійснить свій негативний інформаційний вплив. Тобто й у цьому випадку бібліотечні фахівці виконують роль інформаційних воротарів, але на випередження, оскільки опрацьовують інформацію завчасно – до моменту опублікування та поширення, на відміну від соціальних мереж.

5. Віртуальні екскурсії та тури. У воєнний час доцільно прибрати віртуальні екскурсії та тури з вебсайтів бібліотек, на яких представлено будівлі бібліотек, натомість краще зосередитись на віртуальному представлені фонду книгозбірень.

Наукова новизна. Фейки, неправдива інформація, дезінформація, інформаційні вкиди є лише одним із різновидів інформаційних загроз. Встановлено види інформаційних загроз та визначено роль і функції бібліотечних фахівців з їх запобігання. Розглянуто основні аспекти формування бібліотеками закладів вищої освіти України стратегії інформаційної безпеки.

Висновки. Інформаційна безпека є важливою складовою діяльності бібліотек. Увесь вказаний вище комплекс заходів є важливим для гарантування безпеки інформації в бібліотеці та підвищення довіри користувачів до бібліотеки як до надійного джерела інформації.

Список використаних джерел

1. Про основи національної безпеки України : Закон України від 19.06.2003 № 964-IV. *Відомості Верховної Ради України*. 2003. № 39.

2. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України від 09.01.2007 № 537-V. *Відомості Верховної Ради України*. 2007. № 12. Ст. 102.

3. Information security. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-59.pdf (дата звернення: 28.04.2023).

4. Arif Khan, Muhammad Ibrahim, Abid Hussain. An exploratory prioritization of factors affecting current state of information security in Pakistani university libraries. *International Journal of Information Management Data Insights*. 2021. 1(2). DOI: doi.org/10.1016/j.jjimei.2021.100015.

5. Anday Francese, Huurdeman Yilmaz, Zengenene. Information security issues in a digital library environment: A literature review. *Information World/Bilgi Dunyasi*. 2012. № 13(1). P. 117–137.

6. Gao C. A study on strategies to improve the protection of personal information for university libraries users. *International Conference on Applied System Innovation (ICASI)*. Okinawa, Japan, 2016. P. 1–3.

7. Michael Meth. Blockchain in Libraries. *Library Technology Reports*. 2019. № 8. DOI: https://doi.org/10.5860/ltr.55n8.

8. Zhang L. Blockchain: The new technology and its applications for libraries. *Journal of Electronic Resources Librarianship*. 2019. № 31 (4). P. 278–280.

9. Kunanets N., Lenko V., Pasichnyk V., Shcherbyna Yu. Decentralized Blockchain-based platform for collaboration in virtual scientific communities. *Econtechmod*. 2019. № 8 (1). P. 21–26.

10. Кунанець Н., Ленько В., Пасічник В., Щербина Ю. Персональні бази даних та знань віртуальних дослідницьких спільнот. *Науковий вісник НЛТУ України*. 2017. № 27(6). P. 185–191.

11. Singh V., Margam M. Information security measures of libraries of central universities of Delhi: A study. *DESIDOC Journal of Library & Information Technology*. 2018. № 38 (2). P. 102–109.

12. Ngwum N., Raina S., Aguon S., Taylor B., Kaza S. A model for security evaluation of digital libraries: A case study on a cybersecurity curriculum library. *Journal of The Colloquium for Information Systems Security Education*. 2020. № 7 (1). P. 12.

13. Han Z., Huang S., Li H., Ren N. Risk assessment of digital library information security: a case study. *The Electronic Library*. 2016. № 34(3). P. 471–487.

14. Горовий В. Особливості використання електронних ресурсів національних бібліотек в умовах воєнного протистояння. *Наукові праці Національної бібліотеки України імені В. І. Вернадського*. 2022. Вип. 64. С. 11–27.

15. Jorge Revez, Luís Corujo, Librarians against fake news: A systematic literature review of library practices. *The Journal of Academic Librarianship*. 2021. № 47(2). DOI: https://doi.org/10.1016/ j.acalib.2020.102304.

16. Connor Sullivan M. Leveraging library trust to combat misinformation on social media. *Library & Information Science Research*. 2019. № 41 (1). P. 2–10.

17. Saoirse De Paor, Bahareh Heravi. Information literacy and fake news: How the field of librarianship can help combat the epidemic of fake news. *The Journal of Academic Librarianship*. 2020. № 46(5). DOI: https://doi.org/10.1016/j.acalib.2020.102218.

18. Batchelor O. Getting out the truth: The role of libraries in the fight against fake news. *Reference Services Review*. 2017. № 45(2). P. 143–148.

19. Eva N., Shea E. Marketing libraries in an era of "fake news". *Reference & User Services Quarterly*. 2018. № 57 (3). P. 168–171.

20. Allcott H., Gentzkow M. Social media and fake news in the 2016 election. *Journal of Economic Perspectives*. 2017. № 31 (2). P. 211–236.

21. Steven Wade, Julie Hornick. Stop! Don't Share That Story!: Designing a Pop-Up Undergraduate Workshop on Fake News. *The Reference Librarian*. 2018. № 59(4). P. 188–194.

22. Вільчинська І. Ю. Неправдива інформація як засіб маніпулятивної взаємодії. *Інформаційна освіта та професійно-комунікативні технології XXI століття* : матер. XII Міжнар. наук.-практ. конф. Одеса, 2021. С. 105–108.

23. Кіца М. О. Фейкова інформація в українських соціальних медіа: поняття, види, вплив на аудиторію. *Наукові записки [Української академії друкарства]*. 2016. № 1. С. 281–287.

24. Мудра І. Поняття "фейк" та його види у ЗМІ. *Теле- та радіожурналістика*. 2016. Вип. 15. С. 184–188.

25. Доскіч Л. Фейкові новини як новітній засіб маніпуляції та дезінформації. *Бібліотекознавство. Документознавство. Інформологія*. 2022. № 4. С. 72–77.

26. Сахарова М., Хіміч Я. Розробка та актуалізація комунікаційної політики бібліотеки в умовах воєнного стану: кризові комунікації. *Бібліотекознавство. Документознавство. Інформологія*. 2022. № 2. С. 65–74.

27. Гула Р. В., Передерій І. Г., Сажко В. В. Соціокультурний вимір інформаційних війн XXI століття з погляду місця й ролі в них бібліотек. *Вісник Харківської державної академії культури*. 2021. Вип. 60. С.7–23.

28. Kunanets Nataliia, Rzheuskyi Antonii, Oliinyk Yurii, Kobylynskyi Dmytro, Shunevich Khristina, Tomashevskyi Valentyn. The Model "Information Gatekeepers" for Sentiment Analysis of Text Data. *CEUR Workshop Proceedings*. 2019. 2387. P. 164–177.

29. Kunanets N., Rzheuskyi A., Oliinyk Y., Artemenko O. Sentiment analysis of user responses of tourist services Infocommunications. *Science and Technology PIC S&T`2019*. October 8–11, 2019. Kyiv. P. 502–506.

References

1. Verkhovna Rada of Ukraine. (06.19.2003). On the basics of national security of Ukraine: Law of Ukraine №. 964-IV, 39 [in Ukrainian].

2. Verkhovna Rada of Ukraine (09.01.2007). On the Basic principles of the development of the information society in Ukraine for 2007–2015: Law of Ukraine № 537-V, 12, (102) [in Ukrainian].

3. Information security. Retrieved from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecial publication800-59.pdf [in English].

4. Arif, Khan, Muhammad, Ibrahim, Abid, Hussain. (2021). An exploratory prioritization of factors affecting the current state of information security in Pakistani university libraries. International Journal of Information Management Data Insights, 1(2). DOI: doi.org/10.1016/j.jjimei.2021.100015 [in English].

5. Anday, Francese, Huurdeman, Yilmaz, Zengenene. (2012). Information security issues in a digital library environment: A literature review. Information World/Bilgi Dunyasi, 13(1), 117–137 [in English].

6. Gao, C. (2016). A study on strategies to improve the protection of personal information for university library users. International Conference on Applied System Innovation (ICASI), Okinawa, Japan, 1–3 [in English].

7. Michael, Meth. (2019). Blockchain in Libraries. Library Technology Reports, (8). DOI: https://doi.org/ 10.5860/ltr.55n8.

8. Zhang, L. (2019). Blockchain: The new technology and its applications for libraries. Journal of Electronic Resources Librarianship, 31 (4), 278–280 [in English].

9. Kunanets, N., Lenko, V., Pasichnyk, V., Shcherbyna, Yu. (2019). Decentralized Blockchain-based platform for collaboration in virtual scientific communities. Econtechmod, 8 (1), 21–26 [in English].

10. Kunanets, N., Lenko, V., Pasichnyk, V., Shcherbina, Yu. (2017). Personal databases and knowledge of virtual research communities. Scientific Bulletin of the National Forestry University of Ukraine, 27(6), 185–191.

11. Singh, V., Margam, M. (2018). Information security measures of libraries of central universities of Delhi: A study. DESIDOC Journal of Library & Information Technology, 38 (2), 102–109 [in English].

12. Ngwum, N., Raina, S., Aguon, S., Taylor, B., Kaza, S. (2020). A model for security evaluation of digital libraries: A case study on a cybersecurity curriculum library Journal of The Colloquium for Information Systems Security Education, 7 (1), 12 [in English].

13. Han, Z., Huang, S., Li, H., Ren, N. (2016). Risk assessment of digital library information security: a case study. The Electronic Library, 34(3), 471–487 [in English].

14. Horovyi, V. (2022). Peculiarities of the use of electronic resources of national libraries in the conditions of military confrontation. Scientific works of the National Library of Ukraine named after V. I. Vernadskyi, 64, 11–27 [in Ukrainian].

15. Jorge, Revez, Luís, Corujo. (2021). Librarians against fake news: A systematic literature review of library practices. The Journal of Academic Librarianship, 47(2). DOI: https://doi.org/10.1016/j.acalib. 2020.102304 [in English].

16. Connor Sullivan, M. (2019). Leveraging library trust to combat misinformation on social media, Library & Information Science Research, 41 (1), 2–10 [in English].

17. Saoirse, De Paor, Bahareh, Heravi. (2020). Information literacy and fake news: How the field of librarianship can help combat the epidemic of fake news. The Journal of Academic Librarianship, 46(5). DOI: https://doi.org/10.1016/j.acalib.2020.102218 [in English].

18. Batchelor, O. (2017). Getting out the truth: The role of libraries in the fight against fake news. Reference Services Review, 45(2), 143–148 [in English].

19. Eva, N., Shea, E. (2018). Marketing libraries in an era of "fake news". Reference & User Services Quarterly, 57 (3), 168–171 [in English].

20. Allcott, H., Gentzkow, M. (2017). Social media and fake news in the 2016 election. Journal of Economic Perspectives, 31 (2), 211–236 [in English].

21. Steven, Wade, Julie, Hornick. (2018). Stop! Don't Share That Story!: Designing a Pop-Up Undergraduate Workshop on Fake News. The Reference Librarian, 59(4), 188–194 [in English].

22. Vilchynska, I. Yu. (2021). False information as a means of manipulative interaction. Information education and professional communication technologies of the 21st century: Proceedings of the 12th International Scientific and Practical Conference. Odesa, 105–108 [in Ukrainian].

23. Kitsa, M. O. (2016). Fake information in Ukrainian social media: concepts, types, influence on the audience. Scientific notes [of the Ukrainian Academy of Printing], 1, 281–287 [in English].

24. Mudra, I. (2016). The concept of "fake" and its types in mass media. Television and radio journalism, 15, 184–188 [in Ukrainian].

25. Doskich, L. (2022). Fake news as the latest means of manipulation and disinformation. Library science. Documentary science. Informatology, 4, 72–77 [in Ukrainian].

26. Sakharova, M., Khimich, Ya. (2022). Development and actualization of the library's communication policy in the conditions of martial law: crisis communications. Library science. Documentary science. Informatology, 2, 65–74 [in Ukrainian].

27. Gula, R. V., Perederii, I. G., Sazhko, V. V. (2021). Socio-cultural dimension of information wars of the 21st century from the point of view of the place and role of libraries in them. Bulletin of the Kharkiv State Academy of Culture, 60, 7–23 [in Ukrainian].

28. Kunanets, N., Rzheuskyi, A., Oliinyk, Yu., Kobylynskyi, D., Shunevich, Kh., Tomashevskyi, V. (2019). The Model "Information Gatekeepers" for Sentiment Analysis of Text Data. CEUR Workshop Proceedings, 2387, 164–177 [in English].

29. Kunanets, N., Rzheuskyi, A., Oliinyk, Y., Artemenko, O. (8–11.10.2019). Sentiment analysis of user responses of tourist services Infocommunications. Science and Technology PIC S&T`2019. Kyiv. Ukraine. 502–506 [in English].

Стаття надійшла до редакції 12.07.2023
Отримано після доопрацювання 16.08.2023
Прийнято до друку 25.08.2023