Ігор М. Лях[1], Михайло М. Кляп[2], Петро А. Овчар[3], Володимир Ю. Орел[4], Віктор В. Махонько[5]

АНАЛІЗ ЗАХИСТУ ІНФОРМАЦІЇ У ВОЛОНТЕРСЬКИХ СИСТЕМАХ

У статті розглянуто сучасні виклики та проблеми захисту інформації у волонтерських базах даних неурядових громадських організацій (НУО) України, що виникли внаслідок змін у напрямках їх діяльності з початку 2010-х років, особливо після початку війни у 2014 році та повномасштабного вторгнення у 2022 році. До подій Революції Гідності інформаційна безпека не була пріоритетом для більшості НУО, адже їх діяльність здебільшого не потребувала зберігання великої кількості важливих даних. Однак із розширенням функцій громадських та благодійних організацій – зокрема збору гуманітарної допомоги, логістичної підтримки, обліку донорських внесків, закупівель військового обладнання тощо – зросла не лише кількість оброблюваної інформації, але й загрози з боку ворожих державних структур, хакерських угруповань та інших зловмисників.

Проаналізовано потенційні загрози та запропоновано низку технічних заходів щодо мінімізації ризиків. Зокрема, рекомендується впровадження шифрування даних як під час передачі, так і під час зберігання інформації, двофакторна аутентифікація, менеджери паролів, сегментування прав доступу, використання брандмауерів, моніторинг активності в режимі реального часу, а також обмеження доступу до систем через whitelist-списки IP- або MAC-адрес.

У статті підкреслюється, що через обмежені фінансові та кадрові ресурси, характерні для волонтерських НУО, не всі рішення корпоративного рівня можуть бути їм доступні. Тому доцільно орієнтуватися на спеціалізовані продукти, розроблені для потреб неприбуткових організацій або доступні для них за пільговими умовами, було досліджено програмне забезпечення від компанії «Bitdefender SRL», яке може забезпечити необхідний рівень кіберзахисту.

Таким чином обґрунтовується необхідність адаптації систем захисту інформації до умов та можливостей волонтерських організацій, з урахуванням специфіки їх діяльності під час воєнного стану, значущості оброблюваної інформації та високого ризику її компрометації. Дослідження мають практичне значення для організацій, що працюють у сфері волонтерства, гуманітарної допомоги, громадського активізму та потребують ефективного впровадження інформаційної безпеки на всіх рівнях.

Ключові слова: захист інформації, сховища даних, безпека даних, інформаційні загрози, несанкціонований доступ, волонтерські організації.

Табл. 1. Літ. 24.

DOI: 10.32752/1993-6788-2025-1-287-192-198

Ihor Liakh, Mykhailo Kliap, Petro Ovchar, Volodymyr Orel, Viktor Mahonko

ANALYSIS OF INFORMATION SECURITY IN VOLUNTEER SYSTEMS

The article examines the current challenges and problems of information protection in volunteer databases of non-governmental public organizations (NGOs) of Ukraine, which arose as a result of changes in the areas of their activities since the beginning of the 2010s, especially after the

[1] National Academy of Management, Uzhhorod National University. Ukraine.
[2] National Academy of Management, Uzhhorod National University. Ukraine.
[3] National Academy of Management. Ukraine.
[4] Uzhhorod National University. Ukraine.
[5] National Academy of Management. Ukraine.

outbreak of the war in 2014 and the full-scale invasion in 2022. Before the events of the Revolution of Dignity, information security was not a priority for most NGOs, since their activities mostly did not require the storage of a large amount of important data. However, with the expansion of the functions of public and charitable organizations - in particular, the collection of humanitarian aid, logistical support, accounting of donor contributions, purchases of military equipment, etc. - not only the amount of information processed has increased, but also the threats from hostile state structures, hacker groups and other attackers. Potential threats are analyzed and a number of technical measures are proposed to minimize risks. In particular, it is recommended to implement data encryption both during transmission and during information storage, two-factor authentication, password managers, segmentation of access rights, use of firewalls, real-time activity monitoring, as well as restricting access to systems through IP or MAC address whitelists.

The article emphasizes that due to limited financial and human resources typical of volunteer NGOs, not all corporate-level solutions may be available to them. Therefore, it is advisable to focus on specialized products developed for the needs of non-profit organizations or available to them on preferential terms; software from the company Bitdefender SRL was studied, which can provide the necessary level of cyber protection.

Thus, the need to adapt information protection systems to the conditions and capabilities of volunteer organizations is justified, taking into account the specifics of their activities during martial law, the significance of the information processed and the high risk of its compromise. The research has practical significance for organizations working in the field of volunteering, humanitarian aid, and civic activism and requiring effective implementation of information security at all levels.

Keywords: *information protection, data storages, data security, information threats, unauthorized access, volunteer organizations.*

Peer-reviewed, approved and placed: *05.05.2025.*

Постановка проблеми. З початку 2010-х років неурядові громадські організації (НУО) в Україні відіграють рушійну роль в різних за характером суспільних, політичних та економічних процесах. До подій Революції Гідності питання захисту інформації, пов'язаної з діяльністю НУО, підіймалось дуже рідко, оскільки напрямки діяльності таких організацій не передбачали потреби в розвинутих системах захисту інформації. Найпоширенішими напрямками діяльності були збір коштів для покриття витрат на медичні потреби важко хворим особам, особливо дітям, та соціально-політичний активізм з метою підтримки поширення демократичних цінностей та розвитку інституцій [1]. Для останніх в умовах політичної боротьби та тиску з боку державних структур, до захисту конфіденційної інформації ставились вищі вимоги, проте відносно малий об'єм даних, якими оперували такі організації, не створював необхідності використання спеціалізованих інформаційних систем для їх аналізу.

У 2014 році почали з'являтись нові напрямки діяльності громадських об'єднань, таких як: збір гуманітарної допомоги постраждалим унаслідок бойових дій в Південно-Східних регіонах України, збір коштів на потреби Сил оборони України тощо. Організації, що працюють в цих напрямках, оперують наступними даними: розміри внесків; донори; закупівлі матеріального забезпечення; передачі майна іншим неприбутковим організаціям, фізичним особам або військовим частинам; персональні дані отримувачів допомоги; логістичні маршрути доставки вантажів тощо. Разом із цим розширилось коло

потенційних порушників інформаційної безпеки: інформаційні системи різних волонтерських організацій стали ціллю для атак зі сторони державних служб та структур Російської Федерації або пов'язаних з ними утворень.

Від 24 лютого 2022 року благодійні та громадські організації стали важливою силою в підтримці обороноздатності країни, організації волонтерського руху, спротиві окупації. Надходження коштів на рахунки НУО збільшились в рази: за період від 2015 до початку 2022 року міжнародний благодійний фонд «Повернись живим» є одним з найбільших в Україні, зібрав 170,8 млн грн пожертв, а за період 2022-2024 роки було акумульовано більше 14,67 млрд грн від донорів зі всього світу [2]. Загальна сума витрат Фонду на закупівлі майна для потреб військових перевищує 15,5 млрд грн та включає в себе витрати, які виключно пов'язані на військові напрямки, такі як: зброя та військова техніка, аеророзвідка, протиповітряна оборона, FPV та бомбардувальники тощо [3].

Об'єми конфіденційних відомостей у цієї та інших організацій, спрямованих на підтримку військових та цивільних потреб, значно збільшились, а самі дані представляють стратегічну і тактичну цінність для держави. У зв'язку з таким ускладненням діяльності, все більше волонтерських організацій впроваджують у себе інформаційні системи для своїх потреб: CRM-системи, системи захисту інформації, захищені хмарні та фізичні сховища даних, суворі правила обмеження доступу до конфіденційної інформації.

Питання організації систем захисту інформації для інформаційних систем волонтерських організацій потребує більшого дослідження в період, коли ризик несанкціонованого доступу до відомостей, що зберігаються в їх базах даних, є як ніколи високим.

Аналіз останніх публікацій по проблемі. Дослідженню питань захисту інформації банків, неприбуткових громадських організацій, у сфері національної безпеки, аналізу розробки інформаційних систем для волонтерських організацій, проблеми кібератак проти України присвячено численні роботи вітчизняних та зарубіжних дослідників: Н. Ситник, І. Половчак, Є. Логачова, М. Єсіна, В. Бобух, В. Ліпінський, О. Шпак, М. Юришинець, О. Парфило, Lee E. Rice, Syed (Shawon) M. Rahman, Stan Mierzwa, James Scott, Thomas R. Imboden, Jeremy N. Phillips, J. Drew Seib, Susan R. Fiorentino та інші [4-11].

Через довготривалі військові дії на території України, вітчизняні волонтерські організації у питанні роботи, пріоритетних напрямків та загроз їх діяльності сильно відрізняються від представників інститутів громадянського суспільства інших країн Західної Європи та Північної Америки. Недостатньо уваги приділяється питанню захисту інформаційних систем НУО від кібератак зі сторони урядових установ інших країн та афілійованих з ними злочинних організацій.

Рішення, розроблені в результаті аналізу досвіду великих компаній, рідко підходять для волонтерських організацій з порівняно малими фінансовими та людськими ресурсами, що зумовлено їх неприбутковістю. Тематика захисту інформації у волонтерських організаціях потребує більшого дослідження з

урахуванням специфіки їх діяльності, можливостей та роботи в умовах воєнного стану.

Мета дослідження. Основною метою цього дослідження є визначити технічні вимоги до систем захисту інформації для організацій, що працюють по волонтерському напрямку, та проаналізувавши існуючі програмні рішення у сфері захисту інформації, які орієнтовані на неурядові громадські організації або можуть бути впроваджені, визначити найефективніші серед них.

Основні результати дослідження. Найбільш чутливими до несанкціонованого розголошення є наступні дані:

- дані волонтерів, отримувачів допомоги;
- найменування матеріального забезпечення;
- дані про розташування складів, отримувачів;
- інформація про донорів, транзакції;
- дані аутентифікації користувачів у систему.

Такі дані, як місце розташування військових підрозділів, яким адресована допомога, детальний опис закуповуваного майна, місце роботи волонтерів тощо, не слід розміщувати у відкритому вигляді на інформаційних ресурсах організації, або опубліковувати їх вже після того, як інформація втратила актуальність. Слід використовувати шифрування даних – як під час передачі, так і на фізичних носіях, щоб у випадку отримання несанкціонованого доступу запобігти заволодіння цими даними у відкритому вигляді.

Іншим вразливим місцем волонтерських інформаційних систем може стати слабке управління аутентифікацією та авторизацією. Для запобігання несанкціонованого доступу до файлів системи слід використовувати двофакторну аутентифікацію. Права доступу повинні бути чітко розмежовані: волонтери та випадкові користувачі не повинні мати доступу до всього об'єму інформації про роботу організації. Менеджери паролів, своєю чергою, зменшують ризик соціальної інженерії, витоку облікових записів та зловживань через слабкі або повторно використані паролі.

Через відсутність можливості найму висококваліфікованих спеціалістів з адміністрування інформаційних систем та забезпечення захисту інформації, слід покладатись на періодичне оновлення програмного забезпечення від його виробників. Застаріле устаткування або таке, виробник якого припинив його підтримку, з часом стає все більш вразливим до нових загроз.

Брандмауери та системи сканування в режимі реального часу забезпечують захист від атак на мережевому рівні, миттєво реагуючи на підозрілу активність. Вони дозволяють виявити зловмисників ще до того, як ті отримають доступ до системи. Доступ до системи слід організовувати за допомогою списків дозволених IP- або MAC-адрес (whitelist).

На ринку програмного забезпечення для захисту інформації існує велика кількість продуктів, що своїм функціоналом забезпечують виконання потреб волонтерських організацій. Компанія «Bitdefender SRL» пропонує певний вибір програмних продуктів свого виробництва, орієнтованих на корпоративне використання в неприбуткових організаціях. Існують й інші програмні рішення, розроблені спеціально для потреб НУО, у тому числі й волонтерських організацій [12-24].

Таблиця 1. **Відповідність програмних продуктів до критеріїв захисту інформації**

Продукт	Брандмауер	Аналіз у РРЧ	Шифрування під час передачі	Шифрування на фізичному носії	Менеджер паролів
Bitdefender GravityZone	вбудований фаєрвол IDS/IPS	поведінковий аналіз і моніторинг	захист трафіку	–	–
pfSense	повноцінний firewall	–	VPN-функції (OpenVPN, IPsec)	–	–
CrowdStrike Falcon	–	виявлення загроз у РРЧ	захищені канали	–	–
ProtonMail / Drive	–	–	end-to-end шифрування	–	–
OpenVPN / WireGuard	–	–	тунелювання і шифрування	–	–
VeraCrypt	–	–	–	повне або часткове шифрування	–
BitLocker	–	–	–	повне шифрування диска (Windows)	–
FileVault	–	–	–	повне шифрування (macOS)	–
Bitwarden	–	–	Bitwarden Send (зашифрована передача)	–	менеджер паролів Zero-Knowledge
KeePassXC	–	–	–	–	локальний менеджер паролів

У таблиці 1 наведені програмні продукти для захисту інформації та досліджено їх функціонал. Знаючи ефективність засобів, які пропонує кожен окремий застосунок, волонтерська організація може сформувати такий стек, що буде задовольняти описані вище проблеми.

Висновки. У зв'язку зі зростанням обсягів конфіденційної інформації, яку обробляють волонтерські організації в Україні, захист інформаційних систем стає критично важливим завданням. Для ефективного захисту необхідно впроваджувати шифрування, багаторівневу автентифікацію, чітке розмежування прав доступу та використання актуальних версій програмного забезпечення. Через обмежені ресурси НУО мають орієнтуватися на програмні продукти, розроблені спеціально для неприбуткових організацій.

1. Кондратенко, О. (2023). Взаємовідносини влади та неурядових організацій в Україні : Витоки та сучасний стан. Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління, 3(69), 31-41. DOI: 10.32689/2523-4625-2023-3(69)-4.

2. Звітність фонду: надходження/ Благодійний фонд “Повернись живим”. URL: https://savelife.in.ua/reporting/?reportingType=%22income%22.

3. Звітність фонду: закупівлі. Благодійний фонд “Повернись живим” URL: https://savelife.in.ua/reporting/?reportingType=%22purchase%22&date_from=%222021-12-31T22%3A00%3A00.000Z%22&date_to=%222025-05-31T17%3A59%3A59.999Z%22.

4. Ситник Н., Половчак І. Цифровізація та кібербезпека у забезпеченні фінансової безпеки банків в умовах війни. Галицький економічний вісник. 2024. №4 (89). С. 70-81. DOI: 10.33108/galicianvisnyk_tntu2024.04.070.

5. Логачова, Є., Єсіна, М., Бобух, В. Аналіз особливостей забезпечення кібербезпеки у банківських мобільних додатках. Комп’ютерні науки та кібербезпека Computer science and cybersecurity (CS&CS), 2023. 1(23). С. 63.

6. Ліпінський В. В., Застосування стандартів НАТО при створенні систем захисту інформації в сфері національної безпеки. Телекомунікаційні та інформаційні технології. 2018. №3(60). С. 88–93. DOI: 10.31673/2412-4338.2018.038893.

7. Шпак О. І. Юришинець М. М. Розробка мобільного додатку для організації збору волонтерської допомоги. Актуальні проблеми сучасної науки та освіти : Матеріали VIII міжнародної науково-практичної конференції, м. Львів, 29–30 травня 2023 р. / Львівський науковий форум. С. 66–68.

8. Парфило О. А. Кібератаки як одна із складових російської агресії проти України. Державна безпека України в умовах Російської агресії: актуальні питання експертно-криміналістичного науково-технічного забезпечення : Збірник матеріалів Всеукраїнської науково-практичної конференції. м. Київ, 22 серпня 2023 р. Том 2. С. 91–94 / Український науково-дослідний інститут спеціальної техніки та судових експертиз служби безпеки України.

9. Lee, E. Rice & Syed (Shawon), M. Rahman,. Non-profit organizations’ need to address security for effective government contracting. International Journal of Network Security & Its Applications. 4(4), July 2012. P 53–71.

10. Mierzwa, S., & Scott, J. (2017). Cybersecurity in non-profit and non-governmental Organizations. Institute for Critical Infrastructure Technology.

11. Imboden, T. R., Phillips, J. N., Seib, J. D., & Fiorentino, S. R. (2013). How are nonprofit organizations influenced to create and adopt information security policies. Issues in Information Systems, 14(2), 166-173.

12. TechSoup. Сторінка продукту Bitdefender для некомерційних організацій. URL: https://www.techsoup.org/bitdefender.

13. Офіційний вебсайт продукту “Bitdefender GravityZone”. URL: https://www.bitdefender.com/en-us/ business/gravityzone-platform/.

14. Офіційний вебсайт продукту “pfSense”. URL: https://www.pfsense.org.

15. Офіційний вебсайт продукту “The CrowdStrike Falcon”. URL: https://www.crowdstrike.com/platform/.

16. Офіційний вебсайт продукту “Proton Mail”. URL: https://account.proton.me/mail.

17. Офіційний вебсайт продукту “Proton Drive”. URL: https://account.proton.me/drive.

18. Офіційний вебсайт продукту “OpenVPN”. URL: https://openvpn.net.

19. Офіційний вебсайт продукту “WireGuard”. URL: https://www.wireguard.com.

20. Офіційний вебсайт продукту “VeraCrypt”. URL: https://veracrypt.eu/en/Home.html.

21. Офіційний вебсторінка продукту “Microsoft BitLocker”. URL: https://support.microsoft.com/en-us/windows/bitlocker-overview-44c0c61c-989d-4a69-8822-b95cd49b1bbf.

22. Офіційний вебсторінка продукту “FileVault”. URL: https://support.apple.com/en-gb/guide/mac-help/mh11785/mac.

23. Офіційний вебсайт продукту “BitWarden”. URL: https://bitwarden.com.

24. Офіційний вебсайт продукту “KeePassXC”. URL: https://keepassxc.org.

---

1. Kondratenko, O. (2023). Relations between the government and non-governmental organizations in Ukraine: Origins and current state. Scientific works of the Interregional Academy of Personnel Management. Political Science and Public Administration, 3(69), 31-41. DOI: 10.32689/2523-4625-2023-3(69)-4.

2. Fund reporting: income. Charitable fund “Return Alive”. URL: https://savelife.in.ua/reporting/?reportingType=%22income%22.

3. Fund reporting: purchases. Charitable Foundation "Return Alive" URL: https://savelife.in.ua/reporting/?reportingType=%22purchase%22&date_from=%222021-12-31T22%3A00%3A00.000Z%22&date_to=%222025-05-31T17%3A59%3A59.999Z%22.

4. Sytnyk N., Polovchak I. Digitalization and cybersecurity in ensuring the financial security of banks in wartime. Galician Economic Bulletin. 2024. No. 4 (89). P. 70-81. DOI: 10.33108/galicianvisnyk_tntu2024.04.070.

5. Logachova, E., Yesina, M., Bobukh, V. Analysis of the features of ensuring cybersecurity in banking mobile applications. Computer science and cybersecurity (CS&CS), 2023. 1(23). P. 63.

6. Lipinsky V. V., Application of NATO standards in the creation of information protection systems in the sphere of national security. Telecommunications and information technologies. 2018. №3(60). P. 88–93. DOI: 10.31673/2412-4338.2018.038893.

7. Shpak O. I. Yurishynets M. M. Development of a mobile application for organizing the collection of volunteer assistance. Current problems of modern science and education: Materials of the VIII international scientific and practical conference, Lviv, May 29–30, 2023 / Lviv scientific forum. P. 66–68.

8. Parfilo O. A. Cyberattacks as one of the components of Russian aggression against Ukraine. State security of Ukraine in the conditions of Russian aggression: current issues of expert and forensic scientific and technical support: Collection of materials of the All-Ukrainian scientific and practical conference. Kyiv, August 22, 2023. Volume 2. P. 91–94 / Ukrainian Research Institute of Special Equipment and Forensic Examinations of the Security Service of Ukraine.

9. Lee, E. Rice & Syed (Shawon), M. Rahman,. Non-profit organizations' need to address security for effective government contracting. International Journal of Network Security & Its Applications. 4(4), July 2012. P 53–71.

10. Mierzwa, S., & Scott, J. (2017). Cybersecurity in non-profit and non-governmental Organizations. Institute for Critical Infrastructure Technology.

11. Imboden, T. R., Phillips, J. N., Seib, J. D., & Fiorentino, S. R. (2013). How are nonprofit organizations influenced to create and adopt information security policies. Issues in Information Systems, 14(2), 166-173.

12. TechSoup. Bitdefender product page for nonprofit organizations. URL: https://www.techsoup.org/bitdefender.

13. Official website for the product "Bitdefender GravityZone". URL: https://www.bitdefender.com/en-us/business/gravityzone-platform/.

14. Official website for the product "pfSense". URL: https://www.pfsense.org.

15. Official website for the product "The CrowdStrike Falcon". URL: https://www.crowdstrike.com/platform/.

16. Official website for the product "Proton Mail". URL: https://account.proton.me/mail.

17. Official website of the product "Proton Drive". URL: https://account.proton.me/drive.

18. Official website of the product "OpenVPN". URL: https://openvpn.net.

19. Official website of the product "WireGuard". URL: https://www.wireguard.com.

20. Official website of the product "VeraCrypt". URL: https://veracrypt.eu/en/Home.html.

21. Official website of the product "Microsoft BitLocker". URL: https://support.microsoft.com/en-us/windows/bitlocker-overview-44c0c61c-989d-4a69-8822-b95cd49b1bbf.

22. Official website of the product "FileVault". URL: https://support.apple.com/en-gb/guide/mac-help/ mh11785/mac.

23. Official website of the product "BitWarden". URL: https://bitwarden.com.

24. Official website of the product "KeePassXC". URL: https://keepassxc.org.