Використання стеганографії для забезпечення безперервності бізнес-процесів у банківських системах: аналіз ризиків і стратегій захисту

УДК 004.056.5

Олександр Уманський[1], Олександр Мілов[2]

Національний Технічний Університет «Харківський політехнічний інститут»
[1]oleksandr.umanskyi@cs.khpi.edu.ua, [2]oleksandr.milov@khpi.edu.ua

У сучасному цифровому світі значення безперервності бізнес-процесів у банківському секторі важко переоцінити, особливо для України, яка зіткнулася з викликами воєнного часу. Регулярні кібератаки, які веде країна-агресор, ставлять під загрозу стабільність не лише окремих фінансових установ, а й усієї економічної системи країни. В таких умовах, кібербезпека перетворюється з одного з аспектів банківської діяльності на основу її стійкості та надійності. Стеганографія, як метод приховування інформації у цифрових зображеннях, пропонує витончений і ефективний спосіб захисту даних. Ця техніка не лише дозволяє зберігати конфіденційність інформації, але й виступає як додатковий бар'єр на шляху несанкціонованого доступу до неї. У цьому контексті, застосування стеганографії у банківській сфері України відкриває нові можливості для забезпечення неперервності бізнес-процесів, підвищуючи захист від кіберзагроз, які постійно еволюціонують і стають все більш складними.

Мета роботи – продемонструвати потенціал стеганографії як інструменту кіберзахисту, з огляду на її здатність приховувати важливу інформацію від потенційних загроз. Необхідно у теоретичному плані оцінити ефективність стеганографії та на практиці перевірити її можливості через розробку моделей і методів, які можуть бути впроваджені у банківські системи для посилення їх безпеки. З огляду на постійно зростаючі кіберзагрози, особливо в контексті військових дій, такий підхід не просто покращує захист інформації, але й створює стратегічну основу для забезпечення довгострокової стійкості та надійності фінансової системи України. Важливість стеганографії в контексті забезпечення кібербезпеки банківських систем України є незаперечною. Вивчення та впровадження стеганографії не тільки відповідає на потребу в захисті від нинішніх кіберзагроз, але й відкриває нові шляхи для зміцнення національної безпеки в умовах цифрової ери.

В контексті забезпечення безперервності банківських процесів значну увагу приділяється аналізу вразливості інформаційних систем і ефективності механізмів захисту перед обличчям постійно еволюціонуючих кіберзагроз. Серед таких загроз виділяються розширені постійні загрози (APT), які вимагають від системи інформаційної безпеки не лише реактивних, але й прогностичних здібностей. Дослідження, як от робота Islam та ін. (2022), демонструють, що DDoS-атаки є значною загрозою для інформаційної безпеки в банках, акцентуючи на важливості розробки машинного навчання моделей для їх виявлення в моніторингових системах банківського сектору [1].

З іншого боку, Zimba (2022) вказує на шкідливе програмне забезпечення (malware) як на один із найбільш пріоритетних способів кібератак проти банків та

інших фінансових інституцій, зазначаючи, що malware досягло нових рівнів еволюції, включно з використанням шифрованих вантажів та технік обфускації, що ускладнює його виявлення [2].

Надзвичайно популярні кібератаки в банківській сфері – це фішинг, кіберсталкінг, хакінг, XSS та DDoS. Hasan та Al-Ramadan (2021) підкреслюють розмаїття методів, якими користуються кіберзлочинці для порушення безпеки фінансових установ [3]. Водночас, Revenkov та ін. (2021) та Tariq (2018) підтверджують, що фішинг залишається одним із найпоширеніших методів вчинення шахрайських дій, оскільки він дозволяє красти паролі та інші конфіденційні дані, обманом виманюючи їх у жертв [4, 5].

Зазначені дослідження наголошують на важливості не лише реагування на вже відомі загрози, але й на необхідності розвитку новітніх технологій для прогнозування та запобігання майбутнім атакам, підкреслюючи складність та динамічність кіберзагроз, з якими зіштовхуються банківські системи.

Для аналізу можливостей застосування стеганографії у забезпеченні безперервності банківських бізнес-процесів необхідно, перш за все, використовувати релевантний теоретичний підхід. Основою методології є критичний огляд існуючих досліджень у галузі кібербезпеки та стеганографії, з метою ідентифікації найефективніших стеганографічних методів, які можуть бути адаптовані для захисту інформаційних ресурсів в банківській сфері.

Аналіз літератури необхідно поєднати з математичним моделюванням, що дозволиять визначити потенційні сценарії використання стеганографії в рамках банківських систем. Такий підхід включає оцінку сумісності стеганографічних методів з існуючими технологіями та їх потенціал для зниження ризику втрати даних або несанкціонованого доступу.

Для підтвердження теоретичних припущень слід розглянути використання сценарного аналізу, що допомагає моделювати реакцію банківської системи на введення стеганографічних елементів захисту. Сценарний аналіз спрямований на ідентифікацію можливих викликів та переваг використання стеганографії, з урахуванням різних рівнів загроз та атак.

Важливою частиною методології є також розробка рекомендацій щодо інтеграції стеганографії у комплексні системи захисту інформації банківських інституцій. Ці рекомендації базуватимуться на аналізі отриманих теоретичних та модельних даних, з метою надання практичних напрямків для ефективної реалізації стеганографії як частини загальної стратегії кіберзахисту [6,7].

Таким чином, методологія передбачає використання інтегрованого підходу, що поєднує теоретичне дослідження та аналітичне моделювання, з метою визначення найбільш перспективних шляхів використання стеганографії у банківській сфері. Цей підхід дозволяє не лише виявити потенційні переваги та обмеження стеганографії, але й розробити конкретні рекомендації щодо її ефективного впровадження та використання як інструменту підвищення безпеки банківських інформаційних систем.

Такий підхід вимагає ретельного вибору джерел, а також критичного аналізу існуючих досліджень у цій області, щоб забезпечити актуальність і об'єктивність рекомендацій. Врахування широкого спектру думок і досліджень сприятиме глибшому розумінню теми та забезпеченню високої якості кінцевих висновків.

Попередні дослідження показують, що впровадження стеганографічних механізмів може значно ускладнити виявлення конфіденційної інформації з боку неавторизованих осіб. Використання вейвлет-перетворень для застосування цифрових водяних знаків прогнозується ефективним в запобіганні несанкціонованого доступу до даних без істотного впливу на продуктивність системи. Однак, важливим є додатковий аналіз можливості адаптації таких методів до масштабних реальних банківських систем і визначення оптимального балансу між ступенем приховування інформації та легкістю її регулярного використання системами банку. Необхідно враховувати, що збільшення складності процедур захисту не має заважати ефективності та швидкості банківських операцій.

В подальшому дослідження покликані зосередитися на ретельному аналізі стеганографічних технік з точки зору стійкості до сучасних методів криптоаналізу. Зокрема, необхідно проаналізувати вплив квантових обчислень та машинного навчання на здатність стеганографії приховувати дані, а також розробляти стратегії адаптації та вдосконалення відповідно до нових викликів. Окрім того, слід розглянути імплементацію стеганографії у багатошарову модель безпеки, де вона виступає як один із елементів комплексного захисту інформаційних активів.

При інтеграції стеганографії в системи банківської безпеки необхідно враховувати не тільки технічні, але й соціальні та організаційні аспекти. Стеганографія може вимагати значних змін у корпоративних стандартах та навчанні персоналу для ефективного впровадження. Правові аспекти, такі як дотримання GDPR та інших нормативно-правових актів, також відіграють ключову роль у процесі адаптації стеганографії.

Необхідно прийняти до уваги потенційні ризики, такі як використання стеганографії для неетичних цілей, і необхідність розробки ефективних засобів виявлення таких зловживань. Важливо обговорити стратегії забезпечення прозорості та підзвітності при використанні стеганографії у фінансових системах, щоб гарантувати, що ці технології використовуються на користь організації та її клієнтів.

Загальний висновок щодо запропонованого підходу полягає у наступному. Стеганографія пропонує обнадійливий підхід до забезпечення безпеки банківських бізнес-процесів, вносячи новий вимір у захист конфіденційної інформації. Її здатність приховувати існування даних може стати вирішальним фактором у протидії розширеним кіберзагрозам, що цілеспрямовано шукають цінну інформацію. Дослідження підтверджують, що, незважаючи на певні виклики в імплементації та потенційні ризики, інтеграція стеганографічних методів у систему загальної кібербезпеки може значно посилити захист інформації.

Враховуючи швидкий розвиток кіберзагроз, робота над вдосконаленням і адаптацією стеганографічних технік повинна тривати. Важливо проводити подальші дослідження щодо стійкості цих методів перед лицем квантових обчислень та розвинутих методів криптоаналізу. Разом із тим, необхідно забезпечити баланс між секретністю і відкритістю, належно розглядаючи етичні, правові та організаційні аспекти стеганографії. Можна константувати, що міцна база наукових знань та добре обґрунтовані стратегії впровадження можуть дозволити стеганографії зайняти міцне місце у відповідях на сучасні та майбутні кіберзагрози в банківській сфері.

1. Islam, U., Muhammad, A., Mansoor, R., Hossain Md, S., Ahmad, I., Eldin, E.T., Khan, J.A., Rehman, A.U., Shafiq, M. Detection of distributed denial of service (DDoS) attacks in IOT based monitoring system of banking sector using machine learning models. Sustainability, 2022, 14(14): 8374.
2. Zimba, A. A Bayesian attack-network modeling approach to mitigating malware-based banking cyberattacks. International Journal of Computer Network & Information Security, 2022, 14(1): 25-39.
3. Hasan, M.F., Al-Ramadan, N.S. Cyber-attacks and cyber security readiness: iraqi private banks case. Social Science and Humanities Journal, 2021, 5(8): 2312-2323.
4. Revenkov, P.V., Oshmankevich, K.R., Berdyugin, A.A. Phishing schemes in the banking sector: Recommendations to internet users on protection and development of regulatory tasks. Finance: Theory and Practice, 2021, 25(6): 212-226.
5. Tariq, N. Impact of cyberattacks on financial institutions. Journal of Internet Banking and Commerce, 2018, 23(2): 317.
6. Hryshchuk, R., Yevseiev, S. The synergetic approach for providing bank information security: the problem formulation. Ukrainian Scientific Journal of Information Security, 2016, 22(1): 64-74.
7. Yevseiev, S., Milov, O., Aleksiyev, V., Berdnik, P., Voitko, O., Dyptan, V., Ivanchenko, Y., Pavlenko, M., Salii, A., Yarovyy, S. Development of the interacting agents behavior scenario in the cyber security system. Eastern-European Journal of Enterprise Technologies, 2019, 5/9(101): 46–57.
8. Construction methodology of information security system of banking information in automated banking systems : monograph – Vienna.: Premier Publishing s.r.o., 2018. – 284 p.