УДК 336.717
DOI https://doi.org/10.32782/npnuola.v33.2023.13

Р. С. Южека

КІБЕРБЕЗПЕКА НАЦІОНАЛЬНОГО БАНКУ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ

Постановка проблеми. У сучасному світі, де цифрові технології все більше проникають у різні сфери життя, кібербезпека стає однією з найбільш актуальних проблем, з якими стикаються уряди, організації та приватні особи. В умовах постійного розвитку та застосування інформаційно-комунікаційних технологій, кіберзагрози стають все більш складними та небезпечними.

Одним з ключових гравців, який потребує особливої уваги з точки зору кібербезпеки, є Національний банк України (далі – НБУ). Як центральний банк країни, НБУ відіграє критичну роль у забезпеченні стабільності фінансової системи та збереженні довіри громадян до банківської сфери.

Проте, в умовах воєнного стану, кіберзагрози для НБУ стають ще більшим викликом. Ворогів необхідно вдосконалювати свої методи атак, використовуючи нові технології та підходи для здійснення кібернетичних нападів. Напади на фінансову систему можуть мати катастрофічні наслідки для економіки країни, викликаючи паніку серед населення та порушуючи стабільність фінансових ринків [1, с. 45].

Тому, наукова стаття має на меті дослідити проблему кібербезпеки НБУ в умовах воєнного стану. Вона спрямована на аналіз ризиків та загроз, з якими стикається НБУ, а також на пошук ефективних заходів та рекомендацій щодо зміцнення кібербезпеки цього важливого інституту. Дослідження такого важливого аспекту забезпечення безпеки фінансової системи в умовах воєнного стану може мати практичне значення для НБУ та сприяти розробці ефективних стратегій захисту від кібернетичних загроз.

Стаття базується на системному аналізі та науковому підході до вивчення проблеми кібербезпеки. Вона складається з аналізу поточного стану кібербезпеки НБУ, ідентифікації основних загроз та ризиків, а також розгляду різних стратегій та технологій, які можуть бути використані для підвищення рівня захисту.

Мета цієї статті полягає в тому, щоб виявити слабкі місця та ризики в кібербезпеці НБУ в умовах воєнного стану та запропонувати рекомендації та стратегії для їх запобігання та мінімізації наслідків можливих кібератак. В результаті цього дослідження, ми сподіваємося сприяти зміцненню кібербезпеки Національного банку України та підвищенню стійкості фінансової системи країни в умовах воєнного стану.

Виклад основного матеріалу. Загрози кібербезпеці в умовах воєнного стану можуть бути серйозним викликом для Національного банку України (НБУ). До основних загроз варто віднести наступні:

1. Фішинг.
2. Віруси та шкідливі програми.
3. DDoS атаки.
4. Атаки на інфрастуктуру.

Фішинг є одним з найпоширеніших видів кібератак, які становлять серйозну загрозу для кібербезпеки в умовах воєнного стану. Основна мета фішингової атаки полягає в тому, щоб зловмисники отримали конфіденційну інформацію, таку як паролі, номери карток або особисті дані користувачів [2, с. 187].

Умови воєнного стану можуть створювати напружену атмосферу та збільшувати небезпеку фішингових атак. Зловмисники можуть використовувати цей час, щоб маскуватися під НБУ або банки та надсилати електронні листи з виглядом офіційних повідомлень. Ці листи можуть містити посилання на підроблені веб-сайти, які створені з метою викликати довіру інших осіб і отримати їхні конфіденційні дані.

Для захисту від фішингу в умовах воєнного стану, НБУ може вживати такі заходи:

– Спільне навчання та інформування. НБУ повинен проводити постійне навчання своїх співробітників та клієнтів щодо методів виявлення фішингових атак і практик безпеки. Це допоможе підвищити усвідомленість і здатність виявляти підозрілі електронні листи та веб-сайти.

– Фільтрація спаму. НБУ може використовувати спеціалізовані програми фільтрації спаму, які допомагають виявляти та блокувати фішингові листи, перед тим як вони досягнуть адресатів.

– Багатофакторна аутентифікація. НБУ може впровадити систему багатофакторної аутентифікації, яка вимагає додаткових перевірок, крім введення паролю, для підтвердження ідентифікації користувача. Це може включати використання одноразових паролів, біометричних даних або фізичних пристроїв аутентифікації.

– Система сповіщень. НБУ може встановити систему сповіщень, яка повідомляє клієнтів про потенційно шкідливі або підозрілі активності. Клієнти можуть бути попереджені про підроблені електронні листи або підроблені веб-сайти, щоб запобігти їх використанню.

– Моніторинг та виявлення. НБУ повинен мати механізми моніторингу та виявлення фішингових атак, які допомагають вчасно виявляти та реагувати на підозрілі активності. Це може включати використання систем виявлення і запобігання вторгнень, аналіз логів та інші методи контролю [3, с. 167].

Дані заходи допоможуть НБУ зменшити ризик фішингових атак та забезпечити більшу безпеку в умовах воєнного стану. Однак, важливо пам'ятати, що постійне оновлення заходів безпеки та своєчасне реагування на нові загрози є необхідними для забезпечення ефективного захисту.

Також в умовах воєнного стану загроза від вірусів та шкідливих програм значно зростає, оскільки зловмисники використовують цей час для збільшення своєї активності та поширення шкідливих програм. Надамо деталізований опис цих загроз:

1. Віруси. Віруси є програмами, які розповсюджуються шляхом зараження інших файлів або програм. Вони можуть завдати шкоди інформаційним системам, виконуючи різноманітні шкідливі дії, включаючи знищення даних, блокування доступу до ресурсів або отримання нелегального доступу до конфіденційної інформації.

2. Трояни. Троянські програми представляють собою шкідливі програми, які приховані під надійними або корисними додатками. Після встановлення троян може здійснювати шпигунські дії, збирати конфіденційну інформацію, таку як паролі або банківські реквізити, або навіть надавати зловмиснику дистанційний доступ до інформаційних систем [4, с. 77].

3. Шпигунське програмне забезпечення. Шпигунське програмне забезпечення або шпигунські програми приховано встановлюються на системі з метою збору конфіденційної інформації без відома користувача. Вони можуть перехоплювати введені дані, переглядати веб-сторінки або перехоплювати комунікацію, що загрожує безпеці інформації.

4. Інші шкідливі програми. Окрім вірусів, троянів та шпигунського програмного забезпечення, існує багато інших видів шкідливих програм, таких як рандомізатори, шифрувальники, ботнети тощо. Вони можуть використовуватися для злому систем, збирання інформації або виконання розподілених атак, таких як DDoS-атаки [5, с. 21].

Для захисту від цих загроз, НБУ повинен вживати наступні заходи:

– Встановлення та оновлення антивірусного програмного забезпечення. Антивірусне програмне забезпечення допомагає виявляти та блокувати шкідливі програми, включаючи віруси, трояни та шпигунське програмне забезпечення. Регулярне оновлення антивірусного ПЗ дозволяє виявляти нові загрози та забезпечувати оптимальний рівень захисту.

– Файрвол. Встановлення та налаштування файрволу допомагає контролювати мережевий трафік і блокувати небажану активність, включаючи спроби нелегального доступу до систем.

– Регулярні оновлення програмного забезпечення. Важливо встановлювати всі необхідні патчі та оновлення для операційних систем, браузерів, програм та інших компонентів, що використовуються в інформаційних системах НБУ. Це дозволить усунути вразливості, які можуть бути використані зловмисниками.

– Перевірка на виявлення шкідливого програмного забезпечення. Регулярне проведення сканування систем на наявність вірусів, троянів та інших шкідливих програм допомагає виявити та видалити їх з комп'ютерів та мережі.

– Контроль прав доступу. НБУ повинен встановити строгий контроль прав доступу до своїх інформаційних систем. Це означає встановлення індивідуальних облікових записів для співробітників, обмеження прав доступу до конфіденційної інформації та впровадження принципу найменшого доступу (Least Privilege), щоб мінімізувати ризики несанкціонованого доступу.

– Системи виявлення вторгнень. Використання систем виявлення вторгнень (Intrusion Detection Systems, IDS) та систем виявлення та запобігання вторгнень (Intrusion Detection and Prevention Systems, IDPS) дозволяє виявляти та реагувати на вторгнення та атаки шкідливого ПЗ.

– Користувацька освіта. Важливо проводити навчання та нагадування співробітникам про ризики вірусів та шкідливих програм, а також про необхідність дотримання безпечних практик використання комп'ютерів та мережі.

Вважаємо, що саме ці заходи допоможуть зменшити ризик від вірусів та шкідливих програм і забезпечити більшу кібербезпеку в умовах воєнного стану. Проте, важливо пам'ятати, що кіберзагрози постійно еволюціонують, тому необхідно постійно оновлювати та підтримувати високий рівень захисту інформаційних систем.

DDoS-атаки (розподілений деніал сервісу) є серйозною загрозою для кібербезпеки фінансових установ, включаючи Національний банк України (НБУ), особливо в умовах воєнного стану [6, с. 130].

DDoS-атака полягає в намаганні перевантажити цільовий сервер або мережу шляхом надсилання великого обсягу запитів з багатьох джерел одночасно. Це призводить до перевантаження мережевих ресурсів та відмови в обслуговуванні легітимних користувачів.

В умовах воєнного стану загострюється кібербойова активність, оскільки зловмисники можуть сприймати цей час як період зниженої обороноздатності та збільшувати свою активність. Це може призвести до зростання кількості та інтенсивності DDoS-атак на фінансові установи, включаючи НБУ.

DDoS-атаки можуть мати серйозні наслідки для фінансових установ. Вони можуть призвести до перешкоджання нормальному функціонуванню інтернет-сервісів, зниження доступності веб-сайтів, онлайн-банкінгу та інших систем, що використовуються для фінансових операцій. Це може порушити роботу клієнтів та викликати негативний вплив на довіру до фінансової установи [7, с. 334].

Заходи захисту від DDoS-атак: Для захисту від DDoS-атак фінансові установи, включаючи НБУ, повинні вживати наступні заходи:

– Використання систем виявлення та запобігання DDoS (DDoS Detection and Prevention Systems): Ці системи дозволяють виявляти атаки та блокувати шкідливий трафік, перешкоджаючи його надходженню до цільових серверів.

– Резервне копіювання та масштабування інфраструктури: Забезпечення наявності резервних серверів та мережевих ресурсів допомагає розподілити навантаження та забезпечити нормальне функціонування в разі атаки.

– Фільтрація мережевого трафіку: Використання фільтрів мережевого трафіку дозволяє блокувати шкідливий трафік, що міститься у DDoS-атаках, тим самим зменшуючи їх вплив.

– Використання розподілених CDN-систем (Content Delivery Network): CDN-системи допомагають розподілити навантаження на різні сервери та мережеві вузли, забезпечуючи швидку доставку контенту та знижуючи вразливість до DDoS-атак.

– Співпраця з провайдерами мережевого зв'язку: Важливо підтримувати контакт з провайдерами мережевого зв'язку та виявляти атаки DDoS. Провайдери можуть надавати підтримку та допомогу у виявленні та мінімізації впливу атаки.

Саме ці заходи допоможуть зменшити ризик від DDoS-атак та забезпечити більшу стійкість фінансових установ, включаючи Національний банк України, під час воєнного стану.

Атаки на інфраструктуру, включаючи центри обробки даних та комунікаційні вузли Національного банку України (НБУ), є серйозною загрозою в умовах воєнного стану. Надамо детальний опис цієї загрози:

1. Фізичні атаки. Умови воєнного стану можуть сприяти зростанню фізичних атак на інфраструктуру НБУ. Це можуть бути напади на фізичну безпеку, злам замків, вторгнення до приміщень або знищення обладнання. Зловмисники можуть мати за мету зупинити або пошкодити роботу систем НБУ, перервати фінансове обслуговування або спричинити втрату важливих даних [8, с. 147].

2. Вплив на функціонування. Атаки на інфраструктуру можуть призвести до зупинки або обмеження функціонування інформаційних систем НБУ. Це може перешкоджати виконанню фінансових операцій, обробці та передачі даних, а також забезпеченню зв'язку з іншими фінансовими установами та клієнтами.

3. Втрати даних. Атаки на інфраструктуру можуть призвести до втрати важливих даних НБУ. Це може мати серйозні наслідки для фінансової стабільності та безпеки. Втрата даних може включати фінансову інформацію, конфіденційну інформацію клієнтів, резервні копії та інші важливі дані, які є необхідними для нормального функціонування НБУ [9, с. 641].

Для захисту від атак на інфраструктуру НБУ під час воєнного стану необхідно вживати наступні заходи:

– Фізична безпека. Забезпечення належної фізичної безпеки приміщень та інфраструктури НБУ, включаючи системи контролю доступу, відеоспостереження та охорону.

– Резервне копіювання даних. Регулярне резервне копіювання важливих даних та зберігання їх на захищених місцях. Це допоможе відновити дані у разі їх втрати або пошкодження.

– Захист мережі. Використання захисних механізмів, таких як мережеві брандмауери, інтра- та інтернет-периметри, що дозволять контролювати трафік та виявляти потенційно шкідливі активності.

– Фізична резервування. Резервування критичних систем та обладнання, таких як сервери та комунікаційні вузли, для забезпечення неперервного функціонування в разі атаки або пошкодження.

– Спостереження та виявлення інцидентів. Використання систем моніторингу та виявлення інцидентів для раннього виявлення атак і швидкого реагування на них.

– Контроль доступу. Забезпечення контролю доступу до критичних систем та обмеження привілеїв користувачів, щоб унеможливити несанкціонований доступ [10, с. 733].

Тому, вважаємо, що дані заходи допоможуть зменшити ризик атак на інфраструктуру Національного банку України та забезпечити надійний захист в умовах воєнного стану.

Висновки. Отже, кібербезпека НБУ в умовах воєнного стану є критично важливою задачею для забезпечення безпеки фінансових систем та функціонування економіки країни. Умови воєнного стану створюють нові виклики і загрози, які можуть призвести до збільшення кількості та складності кібератак на НБУ.

Загрози кібербезпеці включають фішинг, віруси, DDoS-атаки та атаки на інфраструктуру. Ці атаки можуть мати наслідки, такі як крадіжка конфіденційної інформації, перешкоджання роботі фінансових систем, вплив на грошові потоки та навіть зруйнування інфраструктури.

Для ефективного захисту кібербезпеки НБУ в умовах воєнного стану необхідно вживати цілісний набір заходів. Це включає використання сучасних технологій та рішень для виявлення, запобігання та реагування на кібератаки. Також необхідно забезпечити фізичну безпеку приміщень та інфраструктури, резервне копіювання даних, захист мережі та спостереження за інцидентами.

Співпраця з провайдерами мережевого зв'язку та залучення експертів з кібербезпеки також мають велике значення для успішної боротьби з кіберзагрозами.

Забезпечення кібербезпеки НБУ в умовах воєнного стану є невід'ємною частиною загальної безпекової стратегії країни. Тільки за умови ефективного захисту від кіберзагроз можна забезпечити нормальне функціонування фінансових систем та зберегти довіру громадськості до банківської системи.

Перспективи подальших досліджень. Національний банк України повинен приділити належну увагу кібербезпеці та вжити всіх необхідних заходів для запобігання та виявлення кібератак в умовах воєнного стану. Це має включати планування, навчання персоналу, впровадження технічних та організаційних заходів, а також постійний моніторинг та оновлення кібербезпекових заходів. Тільки таким шляхом можна забезпечити стійкість фінансової системи в умовах загострення конфлікту та воєнного стану.

Література

1. Гаруст Ю. В. Фінансово-економічна безпека як запорука сталого розвитку банківської установи. *Форум права*. 2019. № 1. С. 42–48.

2. Кравчук Н. Я. Фінансова безпека: Навчально-методичний посібник. Тернопіль: Вектор, 2018. 277 с.

3. Кириченко О. А. Вплив зовнішніх боргів на економічну безпеку українських банків. *Механізм регулювання економіки*. 2018. № 1. С. 160–169.

4. Зачосова Н. В. Особливості забезпечення фінансової безпеки комерційних банків в Україні. *Науковий вісник: Фінанси, банки, інвестиції*. 2021. № 4. С. 74–78.

5. Барановський О. Специфіка фінансової безпеки в банківській сфері. Вісник Національного банку України. 2018. № 9. С. 17–23.

6. Дмитрова О. С. Класифікація загроз та ризиків економічної безпеки. *Ефективна економіка*. 2019. № 11. С. 124–132.

7. Горалько О. В. Фінансова безпека банків у системі забезпечення фінансової безпеки держави. Науковий вісник Львівського державного університету внутрішніх справ. 2021. Вип. 2. С. 328–337.

8. Вартість банківського бізнесу : монографія. А. О. Єпіфанов, С. В. Лєонов, Й. Хабер та ін; за заг. ред. д-ра екон. наук А. О. Єпіфанова та д-ра екон. наук С. В. Лєонова. Суми : ДВНЗ "УАБС НБУ", 2020. 295 с.

9. Василик О. Фінансова безпека. Економічна енциклопедія: у 3 т. Т. 3 О. Василик, С. Мочерний. Київ: Вид.центр «Академія», 2018. 952 с.

10. Шаповал Л.П. Напрями оптимізації менеджменту фінансової безпеки комерційного банку. *Глобальні та національні проблеми економіки*. 2019. Вип. 9. С. 730–736.

Анотація

Южека Р. С. **Кібербезпека Національного банку України в умовах воєнного стану. – Стаття.**

Визначено, що кібербезпека Національного банку України в умовах воєнного стану є актуальним дослідженням, котре демонструє вплив воєнного стану на кібербезпеку банківської системи України. У статті розглядається важливість забезпечення надійності та захисту інформаційно-комунікаційних систем Національного банку України у складних умовах збройного конфлікту.

Автор аналізує загрози, з якими стикається Національний банк України під час воєнного стану, такі як кібератаки, розповсюдження зловмисного програмного забезпечення, соціальний інжиніринг та інші. Також у статті аналізуються та розкриваються основні проблеми, з якими стикається кібербезпека Національного банку України, і пропонуються ефективні стратегії та рішення для підвищення рівня захисту.

Стаття також оглядає сучасні практики кібербезпеки, включаючи впровадження мультифакторної аутентифікації, шифрування даних, моніторинг та виявлення вторгнень, а також навчання персоналу щодо кібербезпеки. Автор звертає увагу на важливість співпраці з іншими банками, урядовими органами та кібербезпековими компаніями для обміну інформацією та координації дій.

Дана робота наголошує на тому, що воєнний стан створює нові виклики для кібербезпеки Національного банку України, але водночас відкриває можливості для впровадження нових технологій, поліпшення захисту та вдосконалення кібербезпеки Національного банку України. Подолання цих викликів вимагає постійного оновлення кібербезпекових політик та стратегій, а також залучення ресурсів та експертизи для ефективного реагування на загрози.

Дана стаття являє собою корисне джерело інформації для фахівців з кібербезпеки, керівників банків та урядових органів, а також для всіх, хто цікавиться захистом фінансової системи в умовах воєнного стану. Автор надає практичні поради та рекомендації, які можуть бути використані для підвищення кібербезпеки Національного банку України та забезпечення стабільності фінансової системи в умовах кризи.

Ключові слова: кібербезпека, Національний банк України, воєнний стан, інформаційно-комунікаційні системи, кібератаки, шкідливе програмне забезпечення, соціальна інженерія.

Summary

Yuzheka R. S. **Cyber security of the NBU under the conditions of marital state. –** Article.

It has been determined that cyber security of the National Bank of Ukraine (NBU) in the conditions of a state of war is a relevant research topic that showcases the impact of the state of war on the cyber security of Ukraine's banking system. The article discusses the importance of ensuring the reliability and protection of NBU's information and communication systems in complex conditions of armed conflict.

The author analyzes the threats faced by the NBU during a state of war, such as cyber-attacks, proliferation of malicious software, social engineering, and others. The article also examines and elucidates the main challenges encountered by NBU's cyber security and proposes effective strategies and solutions to enhance the level of protection.

The article further reviews contemporary cyber security practices, including the implementation of multi-factor authentication, data encryption, monitoring and intrusion detection, as well as personnel training in cyber security. The author draws attention the significance of collaboration with other banks, government agencies, and cyber security companies for information exchange and coordination of actions.

This work highlights that a state of war presents new challenges for NBU's cyber security but also opens up opportunities for the adoption of new technologies, improvement of defense, and enhancement of NBU's cyber security. Overcoming these challenges requires continuous updating of cyber security policies and strategies, as well as mobilization of resources and expertise for effective response to threats.

This article serves as a valuable source of information for cyber security professionals, bank executives, government agencies, and anyone interested in safeguarding the financial system in the context of a state of war. The author provides practical advice and recommendations that can be utilized to enhance NBU's cyber security and ensure stability of the financial system in crisis conditions.

Key words: cyber security, National Bank of Ukraine, state of war, information and communication systems, cyber-attacks, malicious software, social engineering.