УДК 330.341.1:330.47
JEL Classification: D83, L20, L86, M10
DOI: *http://doi.org/10.34025/2310-8185-2023-4.92.03*

Юрій Королюк, д.н.д.у., професор,
https://orcid.org/0000-0001-8732-3731
Валентина Чичун, к.е.н., доцент,
https://orcid.org/0000-0003-0032-9757
Чернівецький торговельно-економічний інститут ДТЕУ,
м. Чернівці

МЕНЕДЖМЕНТ КІБЕРБЕЗПЕКИ В СИСТЕМІ ЛОЯЛЬНОСТІ ПОКУПЦІВ

Анотація

Актуальність. Постановка проблеми. Інформатизація процесів життєдіяльності суспільства набула глобальних масштабів. Однак, окрім позитивних наслідків, інформатизація принесла глобальні загрози, пов'язані із безпекою суспільних відносин. Не винятком є торговельно-економічні процеси, які становлять основу економіки будь-якої країни. Важливим елементом таких процесів є лояльність покупця, що є основою прибутків продавця і запорукою його економічного розвитку. Функціонуючи в інформаційному полі товарно-грошових відносин, лояльність є привабливим об'єктом кібератаки, адже може бути суттєво зменшена внаслідок тільки одного кіберінциденту. Усунення наслідків втрати лояльності може займати роки і вимагати суттєвих ресурсів. Саме тому сучасні виклики до формування лояльності покупців ставлять її кіберзахист на перше місце. Система лояльності є кібернетичною за своїм змістом, що вимагає кіберзахисту усіх складових такої системи: об'єкта, суб'єкта, інформаційних зв'язків. Дієвий інформаційний захист такої системи повинен забезпечуватися відповідними механізмами, ресурсами, регламентуватися формально і документально. Крім цього, такий захист повинен бути постійним і гнучким з позицій виявлення нових кіберризиків. Зважаючи на зазначене, надзвичайної актуальності набуває потреба пошуку нових методів менеджменту торгівельних підприємств, де управління кібербезпекою торгівельних операцій повинне займати ключову позицію. Пошук і впровадження зазначених методів є пріоритетним завданням для практиків і теоретиків менеджменту, фахівців публічного управління.

Мета статті – пошук і дослідження ефективних методів менеджменту кібербезпеки в системі лояльності покупців вітчизняних підприємств, побудова дієвої організаційної схеми механізму управління кібербезпекою лояльності покупця, що базується на захисті усіх складових товарно-економічної взаємодії та її належному ресурсному забезпеченні. **Методологія**. В рамках дослідження використано такі загальнонаукові теоретичні методи:

системний аналіз та синтез – для побудови схеми управління системою кіберзахисту лояльності; метод індукції – для накопичення, узагальнення й обробки інформації актуальності і невирішених проблем дослідження; метод дедукції – для виокремлення головних складових проблеми; методи абстрагування та конкретизації – для схематичного і практично орієнтованого опису проблем кіберзахисту підприємств торгівлі; абстрактно-логічний метод – для виявлення логічних проблем системи кіберзахисту лояльності, оцінки ризиків кіберінцидентів, виявлення ресурсних потреб кіберзахисту.

Результати. За результатами дослідження безпеки інформатизації торговельно-економічних процесів, підтверджено вагомий вплив кіберінцидентів на зниження лояльності покупців торговельних підприємств. Однак у випадку вітчизняних продавців і покупців спостерігається низький інтерес до питань інформаційної та кібербезпеки торговельних операцій. Головною проблемою залишається відсутність єдиного підходу до управління кібербезпекою лояльності покупця. В роботі запропоновано схему кіберзахисту лояльності покупців, яка передбачає цілісний механізм оцінки, моніторингу і розв'язання кіберризиків і кіберінцидентів. Головною складовою ефективності такої схеми є Політика інформаційної безпеки і оперативність реагування на кіберінциденти. **Практичне значення** одержаних результатів полягає у тому, що рекомендації і пропозиції, викладені у дослідженні, передбачають обґрунтування впровадження дієвої системи кіберзахисту лояльності покупців вітчизняних торговельних підприємств. **Перспективами подальших досліджень** у цьому напрямі є сегментація організаційної схеми механізму управління кібербезпекою лояльності покупця для випадків вітчизняних підприємств торгівлі різних типів і розмірів.

Ключові слова: лояльність покупця; кібербезпека; кіберризики; менеджмент кібербезпеки; система лояльності.

Кількість джерел: 22; кількість рисунків: 2.

Yurii Koroliuk, Doctor of Science in Public Administration, Professor,
https://orcid.org/0000-0001-8732-3731
Valentyna Chychun, Candidate of Economic Sciences, Associate Professor,
https://orcid.org/0000-0003-0032-9757
Chernivtsi Institute of Trade and Economics of SUTE, Chernivtsi

CYBER SECURITY MANAGEMENT IN THE BUYER LOYALTY SYSTEM

Summary

The need to find new methods of management of trading enterprises, where the management of cyber security of trading operations should occupy a key position, is becoming highly relevant. The search and implementation of these methods is a priority

task for management practitioners and theoreticians, public administration specialists. That is why the purpose of the article is to find and research effective methods of cyber security management in the customer loyalty system of domestic enterprises, to build an effective organizational chart of the customer loyalty cyber security management mechanism, which is based on the protection of all components of the commodity-economic interaction and its proper resource provision. As part of the study, the following general scientific theoretical methods were used: system analysis and synthesis - to build a management scheme for the loyalty cyber protection system; induction method - for accumulation, generalization and processing of information of relevance and unsolved research problems; the method of deduction - to distinguish the main components of the problem; methods of abstraction and concretization - for a schematic and practically oriented description of the problems of cyber protection of trade enterprises; abstract logical method - for identifying logical problems of the loyalty cyber protection system, assessing the risks of cyber incidents, identifying resource needs of cyber protection. As a result of research on the security of informatization of trade and economic processes, the significant impact of cyber incidents on the decrease in customer loyalty of trade enterprises has been confirmed. However, in the case of domestic sellers and buyers, there is a low interest in issues of information and cyber security of trade operations. The main problem remains the lack of a unified approach to managing customer loyalty cyber security. The paper proposes a scheme for cyber protection of customer loyalty, which provides for a comprehensive mechanism for assessing, monitoring and solving cyber risks and cyber incidents. The main component of the effectiveness of such a scheme is the Information Security Policy and the prompt response to cyber incidents. The practical significance of the obtained results lies in the fact that the recommendations and proposals outlined in the study provide justification for the implementation of an effective system of cyber protection of the loyalty of buyers of domestic trade enterprises. Prospects for further research in this direction are the segmentation of the organizational chart of the buyer's loyalty cyber security management mechanism for the cases of domestic trade enterprises of various types and sizes.

Keywords: customer loyalty; cyber security; cyber risks; cyber security management; loyalty system.

Number of sources – 22; number of drawings – 2.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Лояльність покупця є надзвичайно актуальним явищем у ракурсі здійснення ним повторних покупок. Нещодавні статистичні дослідження [1] виявили, що в середньому половина нових клієнтів протягом 90 днів не здійснює повторні купівлі в магазинах різних типів і на різних платформах. Такі дані створюють два виклики менеджменту торговельного підприємства: потребу збільшення частки лояльних клієнтів за рахунок зазначеного нереалізованого потенціалу;

утримання наявних лояльних покупців, зважаючи на посилення конкуренції, зокрема з боку онлайн торговельних платформ.

Сучасна економічна наука ґрунтовно описує феномен лояльності покупця в рамках двох підходів: емоційного та когнітивного. Так, під емоційною лояльністю розуміють почуття клієнта від продукту чи продавця [2]. В сенс когнітивної лояльності науковці закладають раціональні чисельні чинники поведінки покупця: ціна, час очікування, розташування продавця. Не менш відомою є модель лояльності Діка-Базу, яка розподіляє лояльність на справжню і фіктивну [2]. Справжня лояльність підтверджується повторними покупками. Фіктивна виникає, коли в покупця відсутні альтернативи і він змушений йти на повторні покупки до нелояльного постачальника. Універсальним є визначення лояльності як міри здійснення споживачем повторних покупок з позитивним ставленням до їх постачальника і розгляд тільки його для подальшої взаємодії [3].

Лояльність покупця є головною і невід'ємною частиною бренду постачальника товару чи послуги [4]. У свою чергу, брендова репутація є дуже вразливою складовою розвитку торгівельної економічної системи [5]. Розвиток мережево-комунікаційних технологій та онлайн-торгівлі дозволив отримати точні статистичні дані впливу лояльних до бренду покупців на прибуток продавця. Так, нещодавні дослідження М. Муліки [6] встановили, що лояльні покупці витрачають в середньому на 67% більше, ніж нові покупці і навіть залучення тільки 20% лояльних покупців приносить 80% доходу продавцю. З іншого боку, мережеві технології дають нові можливості продавцю із просування свого товару. Онлайн-методи торгівлі створили нові комерційні поняття, зокрема е-сервіс, який містить такі компоненти [7]: е-задоволення та е-довіра клієнта бренду. Останній параметр, який характеризує безпеку та приватність, сьогодні є ключовим у ланцюжку: е-безпека – е-довіра – лояльність – бренд – прибуток. Статистичні дослідження [8] доводять, що клієнт передає свій негативний досвід (зокрема пов'язаний із порушенням особистої інформаційної безпеки) в

середньому 11 людям, тоді як задоволений клієнт передає його тільки 3. Тому сучасні виклики в утриманні лояльних клієнтів потребують нових методів менеджменту торгівельних підприємств, де управління кібербезпекою торгівельних операцій повинне займати ключову позицію.

Аналіз останніх досліджень та публікацій. Питанням розвитку товарно-грошових відносин та різноманітним аспектам їх інформаційного та безпекового забезпечення приділяли увагу багато вітчизняних та закордонних науковців. Так, А. Вдовічен та О. Вдовічена [9] розглянули питання неконтрольованих глобальних інформаційних викликів в умовах стабілізації діяльності торговельних підприємств України. І. Лошенюк та ін. [10] дослідили дилемні питання безпеки цифрового маркетингу. В. Кифяк та К. Паламарек [11] оцінили інформаційні аспекти розвитку послуг в умовах кризових явищ безпеки. О. Хитрова досліджувала взаємозв'язок безпеки брендових технологій і розвитку торговельних підприємств [12].

Однак нестача досліджень в царині механізмів забезпечення інформаційної безпеки лояльності споживачів на рівні і на базі ресурсів торговельного підприємства все ж дуже відчутна.

Формулювання цілей. Метою статті є пошук і дослідження ефективних методів менеджменту кібербезпеки в системі лояльності покупців вітчизняних підприємств. Для досягнення мети в роботі вирішено наступні завдання: оцінено вплив лояльності покупця на доходи і розвиток торговельного підприємства; встановлено кіберризики та кіберзагрози лояльності покупців; сформовано організаційну схему механізму управління кібербезпекою лояльності покупця та обґрунтовано її ефективність.

Виклад основного матеріалу. Оксфордський тлумачний словник визначає безпеку як «стан, у якому об'єкт є вільним від небезпеки чи загрози», а інформаційну безпеку як «стан, у якому об'єкт захищений від злочинного чи несанкціонованого використання його електронних даних, або заходи, вжиті для досягнення такого стану» [13]. Певні галузі піддаються більшому

ризику стати об'єктом кібератак. Наприклад, компанії, що надають медичні та фінансові послуги, набагато частіше зазнають атак, ніж компанії в інших галузях. Інтернет речей також викликає підвищення занепокоєння через його взаємопов'язаність і низькі засоби захисту кінцевого споживача. Так, зростання побутових приладів із доступом в мережу Інтернет і зовнішнім управлінням загострює питання кібербезпеки на побутовому рівні [14].

Інформатизація сфер життєдіяльності суспільства суттєво посилює ризики і наслідки порушення інформаційної безпеки. Не винятком є торговельні операції. Взаємодія продавця з клієнтом є, значною мірою, інформатизованим процесом. Тому багато вчених розглядають кібербезпеку як ефективний маркетинговий інструмент, використовуючи заходи з її вдосконалення для зміцнення довіри споживачів [15], оскільки навіть один випадок порушення безпеки торгівельної операції може призвести до різкого падіння витрат споживачів на купівлю товарів і послуг у такого продавця [16]. Крім цього, ефект впливу порушення безпеки торгівельних операцій є довготривалим і масштабним. Так, за даними опитування FireFly [17] 72% покупців припинять покупки в продавця, який не забезпечив належним чином кібербезпеку торговельних операцій. Інші вчені [18] оцінюють прямі і непрямі втрати прибутку торговельного підприємства від втрати кібербезпеки до 90 відсотків, які будуть розтягнуті на два роки і є наслідком втрати лояльності покупців.

У сучасній Україні питання кібербезпеки торговельних підприємств набуває ролі виживання малого і середнього торговельного бізнесу, зважаючи на військову агресію росії, спрямовану на всі сфери життєдіяльності українського суспільства. З метою оцінки активності і зацікавленості учасників торговельних процесів питанням кібербезпеки нами було проведено аналіз пошукових трендів в мережі Інтернет за останні два роки із відповідними запитами стосовно безпеки і кібербезпеки (рис. 1).

Як інструмент аналізу пошукових трендів було використано онлайн-сервіс Google Trends (trends.google.com.ua).

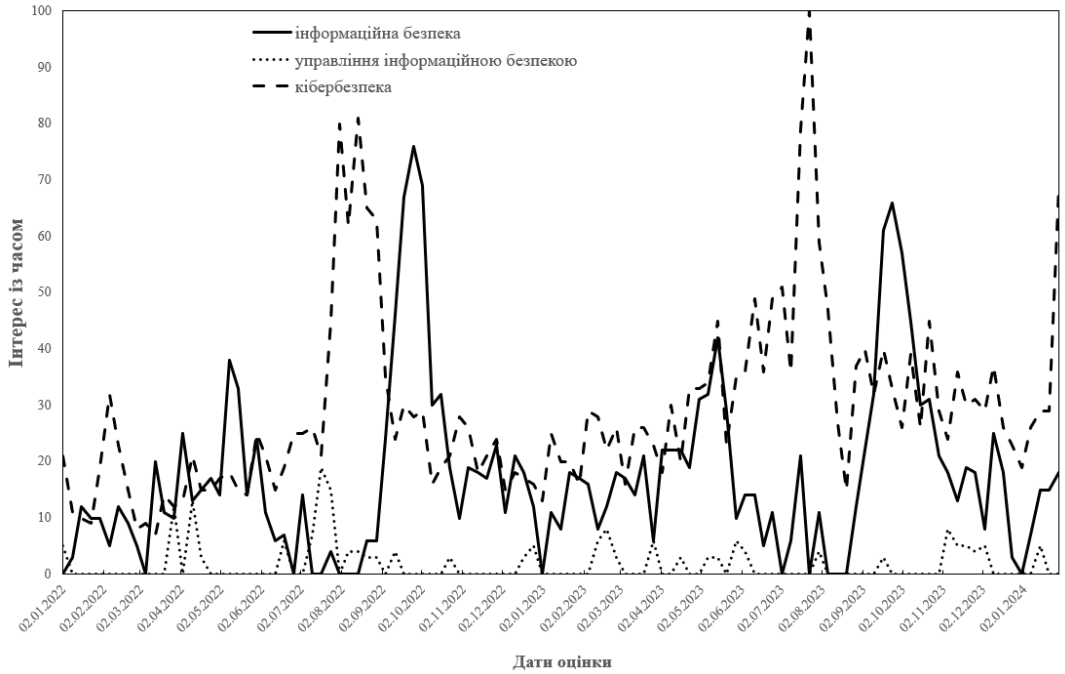

Рис. 1. Динаміка показників «Інтерес з часом» сервісу Google Trends (02.01.2022 р. – 02.01.2024 р.)

Ключові фрази пошуку: «інформаційна безпека», «кібербезпека», «управління інформаційною безпекою». Період аналізу – діапазон 02.01.2022–02.01.2024 з кроком один місяць. Сегмент аналізу пошукових запитів – сфера торгівлі. Регіоном оцінки була вся Україна, а вимірюваним показником – параметр «Інтерес із часом». Вказаний параметр показує популярність пошукового запиту (терміну) стосовно максимальної точки запитів для певного регіону та часового періоду. Параметр вимірюється в межах від 100 (пік максимальної популярності терміну) до 0 (термін не популярний).

Як свідчать результати аналізу активності пошукових запитів за 2022-2023 рр., юридичних та фізичних осіб України при здійсненні торговельних операцій питання безпеки та інформаційної безпеки цікавлять фрагментарно. Піками уваги до питань такої безпеки була зима 2022 та 2023 року. Крім цього, виявлено вкрай низьку зацікавленість питаннями управління інформаційною безпекою і

кібербезпекою торговельних операцій, незважаючи на військовий стан і реальні загрози з боку агресора. Зазначене є свідченням несформованості механізмів управління кібербезпекою торговельних підприємств, малій увазі таким проблемам як з боку продавця, так і покупця. Ускладнює ситуацію затримка із виявлення порушення кібербезпеки навіть в добре захищених підприємств. За даними Ponemon Institute і корпорації IBM [5], середній час виявлення порушення кібербезпеки на торговельних підприємствах США є 201 день після інциденту і 70 днів потрібно для оцінки збитків.

З технічної точки зору кожна кібератака містить комбінацію чотирьох складових [5]: актора (хто буде здійснювати атаку), цілі (на які складові спрямована кібератака), ефекту (які прямі наслідки атаки передбачаються) і практики (які опосередковані і довготривалі наслідки атаки). Сучасними методами кібератак є окреме або комбіноване використання [5]: порушення даних, фішингові атаки, шкідливе програмне забезпечення, програми-вимагачі, соціальний інжиніринг.

Складність і множина методів кібератак вимагає від керівництва організації адекватної системи кіберзахисту. Очевидно, що тотальний захист від усіх можливих типів кіберзагроз є неможливим з позиції обмежених ресурсів малих і навіть середніх підприємств. У випадку ж великих підприємств відбувається фактична порівняльна оцінка вартості від потенційної шкоди кібератаки і вартості засобів чи заходів її захисту. Тому побудова системи кіберзахисту є вирішенням задачі оптимального й ефективного менеджменту наявних ресурсів підприємства з метою максимально можливої мінімізації кіберзагроз. Головним об’єктом захисту такої системи повинна бути лояльність покупця, зважаючи на її важливу роль в прибутку, описану вище, і подальший розвиток торговельного підприємства.

Згідно з моделлю Олівера [19], лояльність покупця, як динамічне явище, містить чотири послідовних ступені (стадії життєвого циклу), розташованих в ієрархічному порядку: когнітивну лояльність; емоційну або афективну лояльність; вольову лояльність; активну, дієву лояльність. Формування кожного етапу

здійснюється в рамках програм лояльності згідно з циклом [2]: клієнтська база даних (ідентифікація клієнта); комплекс комунікацій з клієнтами (утримання клієнта); пакет привілеїв (матеріальне і нематеріальне стимулювання потрібної поведінки клієнта); аналітичне ядро, що дозволяє спрогнозувати те, як клієнт поведе себе завтра, а також те, яким чином його поведінка позначиться на показниках бізнесу. Головним об'єктом лояльності такого циклу є якість продукту та послуг, якість обслуговування клієнтів, а іноді й ціноутворення, щоб вплинути на сприйняту цінність. Однак ціни не мають значного впливу порівняно з процесами та процедурою [20].

Ефективні системи кібербезпеки ґрунтуються на моніторингу вимірюваних показників об'єкта захисту. У випадку лояльності таким показником визначимо широко поширений індекс підтримки споживача (англ. Net Promoter Score – NPS) Фреда Райчхелда [21]. Індекс розраховується шляхом опитування в межах від -100 (відсутня лояльність) до +100 (максимально можлива лояльність клієнтів).

Менеджмент кібербезпеки торговельного підприємства – це, перш за все, побудова ефективної динамічної системи оцінки ризиків кіберзагроз. Вчасний моніторинг таких ризиків у просторі і часі дозволить встановлювати рівні прийнятної безпеки для підприємства, забезпечувати їх дотримання, приймаючи рішення за наявних ресурсів та управлінських інструментів. Обов'язковим для такої системи є врахування кіберпрецендентів безпеки, досвіду минулих подій.

Використовуючи методи системного аналізу і синтезу, опрацьовані вище підходи і теоретичні концепти, нами було запропоновано схему менеджменту кібербезпеки лояльності покупців торговельного підприємства (рис. 2).

Система лояльності покупців формується в процесі їх взаємодії з торговельним підприємством. Головними складовими такої взаємодії є товарно-речовий обмін, валютно-грошові операції і просування товару. Такі складові є кібернетичними за своєю природою.

Кіберзагрози лояльності мають відношення до усіх частин такої кібернетичної системи:

- на рівні торговельного підприємства виникають загрози цілісності даних клієнтів, систем управління підприємством (логістика, облік, засоби внутрішньої комунікації), цілісність даних про бізнес-процеси підприємства з метою їх зупинення чи зменшення ефективності;

- на рівні взаємодії клієнтів з підприємством виникають загрози взлому каналів комунікації та валютно-грошового обміну з метою шахрайства, підміни чи кібердиверсії;

- на рівні покупця виникають загрози спотворення інформації про продавця, просування негативного псевдодосвіду купівлі інших клієнтів з метою його дискредитації і зменшення лояльності.

Початковим етапом протидії кіберінцидентам є два одночасних процеси: раннє виявлення кіберзагроз і моніторинг стану кібербезпеки. Перший процес є оцінкою ризиків, тоді як оцінка стану системи лояльності – це процес виявлення наявних кіберінцидентів. І в першому, і в другому випадку обов'язковим є подальший аналіз потенційного чи явного збитку від кіберінциденту. Регламентація початкового етапу й аналіз збитків відбувається відповідно до Політики інформаційної безпеки торговельного підприємства і чітко описується її положеннями (рис. 2).

Наступним етапом механізму кіберзахисту лояльності є оцінка спроможності і необхідності подолати кіберзагрозу. Оцінка здійснюється на підставі наявних ресурсів підприємства передбачених Політикою інформаційної безпеки на такі цілі. У разі спроможності подолати кіберзагрозу застосовуються передбачені заходи на всю кібернетичну систему взаємодії з клієнтом. У разі неспроможності відбувається циклічна переоцінка наслідків ризиків чи події, перегляд Політики інформаційної безпеки, у т.ч. з метою збільшення ресурсів, допоки підприємство не буде спроможне ефективно вирішити проблеми кібербезпеки (рис. 2).

Важливим аспектом такої схеми механізму управління кібербезпе-кою лояльності покупця є повідомлення останніх про кіберінцидент.

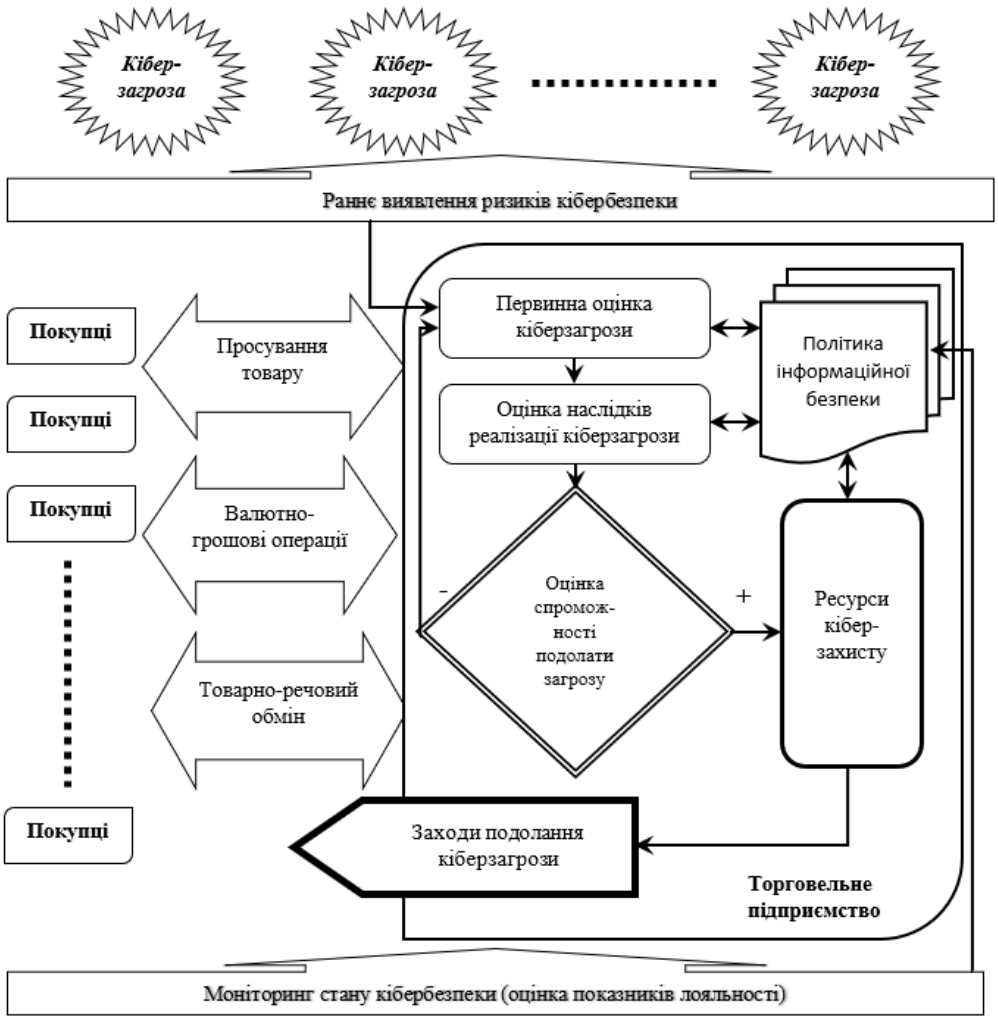

*Рис. 2. Організаційна схема механізму управління кібербезпекою лояльності покупця**

*Джерело: сформовано авторами.

Ефективне спілкування із зацікавленими сторонами є невід'ємною частиною успішного відновлення лояльності після кіберінциденту.

Однак часто підприємству, яке зламали, може знадобитися багато часу, щоб виявити порушення та згодом публічно оголосити про порушення даних. Час між моментом, коли відбулося

порушення даних, і моментом, коли його виявила зламана компанія, може призвести до того, що клієнти втратять довіру до бренду [22]. Саме тому важливим є оперативність проходження усіх етапів схеми кіберзахисту лояльності покупця.

Кіберзахист лояльності покупців - це безперервний та унікальний в кожному випадку процес, де головним аспектом є налагодження дієвого механізму виявлення кіберзагроз, розробки і застосування нових методів протидії ним.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямку. Інформатизація усіх процесів життєдіяльності суспільства набула глобальних масштабів. Однак, окрім позитивних наслідків, інформатизація принесла глобальні загрози, пов'язані із безпекою суспільних відносин. Не винятком є торговельно-економічні процеси, які становлять основу економіки будь-якої країни.

За результатами дослідження безпеки інформатизації торговельно-економічних процесів, підтверджено вагомий вплив кіберінцидентів на зниження лояльності покупців торговельних підприємств. Однак у випадку вітчизняних продавців і покупців спостерігається низький інтерес до питань інформаційної та кібербезпеки торговельних операцій. Головною проблемою залишається відсутність єдиного підходу до управління кібербезпекою лояльності покупця. Для розв'язання вказаної проблеми в роботі запропоновано схему кіберзахисту лояльності покупців, яка передбачає цілісний механізм оцінки, моніторингу і протидії кіберризикам і кіберінцидентам. Головною складовою ефективності такої схеми є Політика інформаційної безпеки і оперативність реагування на кіберінциденти.

Напрямами подальших досліджень є сегментація організаційної схеми механізму управління кібербезпекою лояльності покупця для випадків вітчизняних підприємств торгівлі різних типів і розмірів.

Список використаних джерел:

1. Amatus, A., & Gisip, I. A. Effects of Website Appearance, Security and Electronic Word-of-Mouth (EWOM) on Online Customer Loyalty: Trust as Mediating Factor. *International Journal of Academic Research in Business and Social Sciences*. 2022. No. 12(12). Pp. 818–840.

2. Кляченко І. О., Зозульов О. В. Програми лояльності споживачів до бренду. *Актуальні проблеми економіки та управління : збірник наукових праць молодих вчених.* 2012. № 5. URL: https://ela.kpi.ua/handle/123456789/12367 (дата звернення: 01.12.2023).

3. Ferguson R., Hlavinka K. Loyality trends 2006: Three evolutionary trends to transform your loyalty strategy. *Journal of Consumer Marketing*. 2007. No. 23 (5). Pp. 292-299.

4. Kirk G. & Noguera J. Strategic marketing and cybersecurity: the case of data breaches. *Issues in Information Systems.* 2019. No. 20(3). Pp. 165–174.

5. DiStaso M. W. Communication challenges in cybersecurity. *Journal of Communication Technology.* 2018. No. 1(1). Pp. 43-60.

6. Muliki M. A importância da lealdade do cliente [The importance of customer loyalty]. 2021. URL: https://after.sale/importancia-da-lealdade-do-cliente/ (дата звернення: 01.12.2023).

7. Ghali Z. Motives of customers' e-loyalty towards e-banking services: a study in Saudi Arabia. *Journal of Decision Systems.* 2021. Pp. 172-193.

8. Pereira H. G., Cardoso M. and Dionísio P. The determinants of website purchases: The role of e-customer loyalty and word-of-mouth. *International Journal of Electronic Marketing and Retailing.* 2017. Pp. 135-156.

9. Вдовічен А. А., Вдовічена О. Г. Триєдиний вектор стабілізації економіки України в умовах неконтрольо-ваних глобальних викликів. *Вісник Чернівецького тоговельно-економічного інституту. Серія: Економічні науки.* 2020. Вип. I (77). С. 12–30.

10. Лошенюк І. Р., Кірєєва К. О., Мілашовська О. І. Дилемні питання розвитку цифрового маркетингу в реаліях масштабної військової агресії. *Академічні візії.* 2023. №. 21.

11. Паламарек К. В., Кифяк В. Ф. Розвиток готельного бізнесу м. Чернівці в умовах кризових явищ. *Вісник Чернівецького торговельно-економічного інституту*. 2021. № 1 (81). С. 25-39.

12. Хитрова О.А. Брендингові технології як спосіб популяризації товарів. *Економіка та управління підприємствами.* 2019. Випуск II (74). С. 116 – 125.

13. Oxford Living Dictionary (n.d.). URL: https://en.oxforddictionaries.com/ (дата звернення: 01.12.2023).

14. Stavridis, J., & Weinstein, D. (2016, November 3). The Internet of Things is a cyberwar nightmare. Foreign Policy (FP). URL: http://foreignpolicy.com/2016/11/03/the-internet-of-things-is-a-cyber-war-nightmare/ (дата звернення: 01.12.2023).

15. Lucas, J., Minsky, L., & DiSanti, B. Good cybersecurity can be good marketing. *Harvard Business Review Digital Articles*. 2016. No. 9(23). Pp. 2-4.

16. Janakiraman, Ramkumar, Lim, Joon Ho, Rishika, Rishika The effect of a data breach announcement on customer behavior: evidence from a multichannel retailer. *Journal of Marketing*. 2018. No. 82(2). Pp. 85-105.

17. Muncaster, P. (2016, May 13). Brits shun brands following breaches. InfoSecurity. URL: https://www.infosecurity-magazine.com/news/brits-shun-brands-following/ (дата звернення: 01.12.2023).

18. Mossburg, E., Fancher, D., Gelinne, J., & Calzada, H. Beneath the surface of a cyberattack. 2016. URL: https://www2.deloitte.com/us/en/pages/risk/articles/hidden- business-impact-of-cyberattack.html (дата звернення: 01.12.2023).

19. Duffy, Dennis L. Customer loyalty strategies. *Journal of Consumer Marketing*. 1998. Vol. 15. Iss. 5. Pp. 435-448.

20. Alharbi A. H., Alhider I. H. The impact of customer satisfaction and loyalty on e-marketing: Moderating effect of perceived value. *Journal of Marketing and Consumer Research*. 2018. No. 46. Pp. 70–77.

21. Reichheld Fred, Markey Rob. The Ultimate Question 2.0: How Net Promoter Companies Thrive in a Customer-Driven World. Boston, Mass.: *Harvard Business Review Press*. 2011. P. 52.

22. Wang, P. & Johnson, Ch. Cybersecurity incident handling: A case study of the Equifax data breach. *Issues in Information Systems*. 2018. No. 19(3). Pp. 150-159.

References:

1. Amatus, A., & Gisip, I.A. (2022). Effects of Website Appearance, Security and Electronic Word-of-Mouth (EWOM) on Online Customer Loyalty: Trust as Mediating Factor. *International Journal of Academic Research in Business and Social Sciences*, no. 12(12), pp. 818–840.

2. Klyachenko, I.O., Zozulyov, O.V. (2012). Consumer brand loyalty programs. Actual problems of economics and management: *a collection of scientific works of young scientists,* № 5. URL: https://ela.kpi.ua/handle/123456789/12367 (Accessed 01.12.2023) (in Ukr.).

3. Ferguson, R., Hlavinka, K. (2007). Loyality trends 2006: Three evolutionary trends to transform your loyalty strategy. *Journal of Consumer Marketing*, no. 23 (5), pp. 292-299.

4. Kirk, G. & Noguera, J. (2019). Strategic marketing and cybersecurity: the case of data breaches. *Issues in Information Systems*, no. 20(3), pp. 165–174.

5. DiStaso, M.W. (2018). Communication challenges in cybersecurity. *Journal of Communication Technology*, no. 1(1), pp. 43-60.

6. Muliki, M. (2021). A importância da lealdade do cliente [The importance of customer loyalty]. URL: https://after.sale/importancia-da-lealdade-do-cliente/ (Accessed 01.12.2023).

7. Ghali, Z. (2021). Motives of customers' e-loyalty towards e-banking services: a study in Saudi Arabia. *Journal of Decision Systems*, pp. 172-193.

8. Pereira, H.G., Cardoso, M. and Dionísio, P. (2017). The determinants of website purchases: The role of e-customer loyalty and word-of-mouth. *International Journal of Electronic Marketing and Retailing*, pp. 135-156.

9. Vdovichen, A.A., Vdovichena, O.G. (2020). The triple vector of stabilization of the economy of Ukraine in the conditions of uncontrollable global challenges. *Visnyk Chernivetskoho torhovelno-ekonomichnoho instytutu [Bulletin of the Chernivtsi Trade and Economic Institute],* Iss. I (77), pp. 12–30 (in Ukr.).

10. Loshenyuk, I.R., Kireeva, K.O., Milashovska, O.I. (2023). Dilemma issues of digital marketing development in the realities of large-scale military aggression. *Akademichni vizii. [Academic Visions]*, no. 21 (in Ukr.).

11. Palamarek, K.V., Kyfyak, V.F. (2021). Development of hotel business in Chernivtsi in the conditions of crisis phenomena. *Visnyk Chernivetskoho torhovelno-ekonomichnoho instytutu [Bulletin of the Chernivtsi Trade and Economic Institute]*, no. 1 (81), pp. 25-39 (in Ukr.).

12. Khitrova O.A. (2019). Branding technologies as a way to popularize goods. *Ekonomika ta upravlinnia pidpryiemstvamy [Economics and business management],* Iss. II (74), pp. 116–125 (in Ukr.).

13. Oxford Living Dictionary (n.d.). URL: https://en.oxforddictionaries.com/ (Accessed 01.12.2023).

14. Stavridis, J., & Weinstein, D. (2016, November 3). The Internet of Things is a cyberwar nightmare. Foreign Policy (FP). URL: http://foreignpolicy.com/2016/11/03/the- internet-of-things-is-a-cyber-war-nightmare/ (Accessed 01.12.2023).

15. Lucas, J., Minsky, L., & DiSanti, B. (2016). Good cybersecurity can be good marketing. *Harvard Business Review Digital Articles*, no. 9(23), pp. 2-4.

16. Janakiraman, Ramkumar, Lim, Joon Ho, Rishika, Rishika (2018). The effect of a data breach announcement on customer behavior: evidence from a multichannel retailer. *Journal of Marketing*, no. 82(2), pp. 85-105.

17. Muncaster, P. (2016, May 13). Brits shun brands following breaches*. InfoSecurity*. URL: https://www.infosecurity-magazine.com/news/brits-shun-brands-following/ (Accessed 01.12.2023).

18. Mossburg, E., Fancher, D., Gelinne, J., & Calzada, H. (2016). Beneath the surface of a cyberattack. URL: https://www2.deloitte.com/us/en/pages/risk/articles/hidden- business-impact-of-cyberattack.html (Accessed 01.12.2023).

19. Duffy, Dennis L. (1998). Customer loyalty strategies. *Journal of Consumer Marketing*, vol. 15, Iss. 5, pp. 435-448.

20. Alharbi A. H., Alhider I. H. (2018). The impact of customer satisfaction and loyalty on e-marketing: Moderating effect of perceived value. *Journal of Marketing and Consumer Research,* no. 46, pp. 70–77.

21. Reichheld, Fred, Markey, Rob (2011). The Ultimate Question 2.0: How Net Promoter Companies Thrive in a Customer-Driven World. Boston, Mass.: *Harvard Business Review Press*. 52 p.

22. Wang, P. & Johnson, Ch. (2018). Cybersecurity incident handling: A case study of the Equifax data breach. *Issues in Information Systems*, no. 19(3), pp. 150-159.

УДК 659.1:658.8:330.3
JEL Classification:M31,M37,M38
DOI: *http://doi.org/10.34025/2310-8185-2023-4.92.04*

Вардан Вардеванян, к.е.н., асистент,
https://orcid.org/0000-0002-3642-6164
Чернівецький національний університет ім. Ю. Федьковича,
м. Чернівці

РИНОК РЕКЛАМИ В УКРАЇНІ: КРИЗОВІ ТА ПОСТКРИЗОВІ ПЕРІОДИ

Анотація

Актуальність. Постановка проблеми. Ринок реклами в Україні за останні 10 років доволі часто перебував у кризовому стані, але завжди знаходив можливості для початку відновлення. Знання про ситуацію на ринку важливі для прийняття адекватних рішень при оцінці конкурентних можливостей, перегляду рекламних бюджетів та рекламних стратегій. Достовірну інформацію про ринок отримують, використовуючи різні методики розрахунку показників ринку. В умовах частих криз важливо адекватно оцінювати ситуацію, що склалася на ринку, розуміти амплітуду коливань та регенеративні можливості ринку.

Мета дослідження полягає у вивченні динаміки рекламного ринку України у його кризові та посткризові періоди розвитку. **Методологія.** Методичною основою написання статті служили методи наукової абстракції – при визначенні концепції дослідження, статистичний – при формуванні вибірки показників рекламного ринку, аналізу та синтезу – при співставленні отриманих показників ринку.

Результати. У статті досліджено динаміку показників рекламного ринку України, розрахованих у фактично діючих цінах, в цінах попереднього року та цінах 2013 року.