

КІБЕРБЕЗПЕКА ЯК ДЕТЕРМІНАНТА ОБАЧЛИВОЇ ФІНАНСОВОЇ ПОВЕДІНКИ ДОМОГОСПОДАРСТВ

Вовченко Оксана Сергіївна 

канд. екон. наук, доцент,
доцент кафедри фінансів, банківського бізнесу та оподаткування
Національний університет «Полтавська політехніка
імені Юрія Кондратюка», Україна

Анотація. В роботі автором запропоновано підхід до дослідження кібербезпеки як інструменту вдосконалення особистої фінансової поведінки домогосподарств. Охарактеризовано спектр кіберзагроз, типи загроз фінансовій безпеці домогосподарств в онлайн-середовищі та обґрунтовано важливість протидії фінансовим втратам від них в умовах цифровізації. Запропоновано напрями підвищення рівня кібербезпеки та окреслено особливості формування обачливої фінансової поведінки домогосподарств з урахуванням сучасних тенденцій.

Ключові слова: фінансова поведінка, кібербезпека, домогосподарство, кіберзагроза, цифровізація, мережа «Інтернет», особиста фінансова безпека.

В сучасному цифровому світі, де передові фінансові інновації та технології розвиваються в геометричній прогресії, питання кібербезпеки набуває надзвичайно важливого значення. У рамках Програми фінансової допомоги Україні від ЄС Ukraine Facility на 2024–2027 рр. передбачено реалізацію реформ у секторі цифрової трансформації, зокрема: інтеграцію з цифровим ринком ЄС, поширення швидкого та захищеного зв'язку, створення умов для розвитку екосистеми стартапів та «держави в смартфоні» [1]. Проте цифровізація не лише створює нові можливості для її розвитку та покращення якості життя, а також несе в собі нові ризики, особливо для особистої фінансової безпеки домогосподарств, що проявляються у погіршенні здатності до стійкої протидії впливу внутрішніх і зовнішніх загроз стану їх життєдіяльності. Застосування fintech у фінансовій сфері, враховуючи тренди та перспективи фінтех-галузі, забезпечує вищий рівень обслуговування домогосподарств і полегшує доступ до фінансової інформації, проте значно розширює спектр кіберзагроз. Збільшення кількості та складності кібератак, зростання залежності від онлайн-банкінгу в умовах пандемії COVID-19, а потім і повномасштабного вторгнення, а також зростання фінансових втрат від перелічених чинників, роблять захист домогосподарств від кіберзлочинців все більш складним завданням. Згідно з даними компанії IBM [2], середня вартість витоку даних досягла максимуму у 2023 році та становила 4,45 млн доларів (рис. 1), тобто в порівнянні з 2022 роком, коли вартість витоку була 4,35 млн доларів США, показник збільшився на 2,3%.

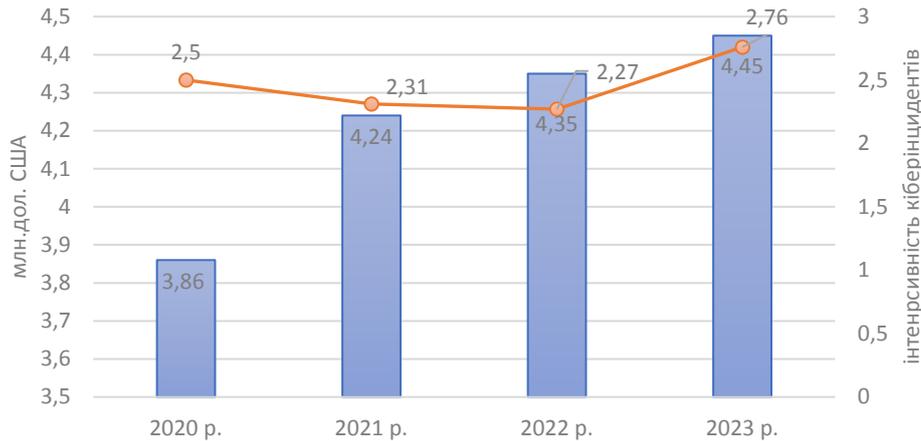


Рис. 1. Динаміка вартості витоку даних та інтенсивності кібератак протягом 2020-2023 років

Джерело: дані сформовано з [2, 3]

Варто відмітити, що інтенсивність кібератак (яка оцінюється European Repository of Cyber Incidents (EuRepoC) за шкалою від 1 до 15 балів, виходячи з фактичних наслідків та соціально-політичної серйозності кіберінциденту), в Україні за 2023 рік зросла до показника 2,76 [3].

Аналіз наукового інтересу в світовому масштабі до проблем забезпечення особистої фінансової безпеки було проведено за допомогою системи Google Trends. В якості пошукових запитів використані пов'язані з даною тематикою терміни: «Financial security», «Personal financial security», «Digitalization». Згідно з одержаними результатами, за останні 5 років інтерес до проблем забезпечення фінансової безпеки стабільно зростає, досягнувши свого максимуму в березні 2024 року. При цьому така ж тенденція спостерігається й з питаннями цифровізації, зацікавленість якою у серпні 2023 року навіть перевищила фінансову безпеку. Важливо, що все частіше користувачі починають цікавитися особистою фінансовою безпекою, адже з поширенням цифровізації і комп'ютеризації як у виробництві, так і у побуті, масштаби кіберзагроз зростають пропорційно розширенню спектру продуктів і послуг, у яких застосовуються інформаційні технології, та кількості їх споживачів.

Тенденцію до підвищення рівня кібершахрайства підтверджують статистичні дані Національного банку України щодо незаконних дій з платіжними картками: кількість незаконних дій з платіжними картками, за якими були понесені збитки, протягом двох років зросла на 45,5%; сума збитків надавачів платіжних послуг, торговців, клієнтів від незаконних дій з платіжними картками за минулий рік становила майже 833 млн гривень, що більш ніж у 3 рази перевищує показник 2021 року; середня сума однієї незаконної операції зросла на 90% (табл.1).

Таблиця 1

Динаміка платіжного шахрайства в Україні протягом 2021-2023 років

Показник	2021 рік	2022 рік	2023 рік
Сума збитків від незаконних дій з платіжними картками, млн.грн.	260	481	833
Кількість незаконних дій з платіжними картками, за якими були понесені збитки, тис.шт.	187	204	272

Продовження табл. 1

Показник	2021 рік	2022 рік	2023 рік
Середня сума однієї незаконної операції	1640	2200	3065
Частка шахрайства з платіжними картками через мережу Інтернет (від загальної кількості випадків), %	70%	86%	83%

Джерело: дані сформовано з [4]

Варто відмітити, що шахрайство з платіжними картками найчастіше відбувалося через мережу Інтернет – 83% від загальної кількості випадків у 2023 році. Водночас лише 17% – через фізичні пристрої (торговельна мережа, банкомати, пристрої самообслуговування). Крім платіжного шахрайства до основних типів загроз фінансовій безпеці домогосподарств в онлайн-середовищі можна віднести:

1. Кіберзлочини: крадіжки особистих даних, фішингові атаки, шкідливе програмне забезпечення.

2. Фінансові піраміди та шахрайські схеми: фейкові інвестиційні пропозиції, шахрайські схеми з працевлаштуванням, залежність від онлайн-кредитування, онлайн-казино та азартних ігор.

3. Необережне використання онлайн-платежів: перекази коштів невідомим особам, оплата за неіснуючі товари або послуги, незахищені онлайн-платежі.

4. Необізнаність та недостатня фінансова грамотність: незнання основ онлайн-безпеки: принципів захисту особистих даних, використання надійних паролів та розпізнавання ознак шахрайства; нерозуміння фінансових продуктів та послуг, відсутність навичок планування бюджету та контролю витрат.

Щоб забезпечити особисту фінансову безпеку, домогосподарства повинні впевнено користуватися фінансовими послугами та ухвалювати відповідальні фінансові рішення, тобто мати високий рівень фінансових знань. Попередні дослідження рівня фінансової грамотності серед дорослого населення України у 2018 та 2021 роках показали, що найменш фінансово обізнаною є молодь віком 18-19 років. Цей висновок підтверджується результатами опитування з фінансової грамотності серед підлітків, проведеного Національним банком України у 2023 році [5].

Тож цифровізація суспільства створює нові виклики для особистої фінансової безпеки, особливо молоді. Проте, враховуючи ці виклики та вживаючи відповідних заходів, можна захиститися від фінансових втрат. Особливу увагу слід приділити підвищенню фінансової грамотності серед підлітків, наприклад, шляхом включення модулів із фінансової грамотності до шкільних навчальних програм, проведення просвітницьких кампаній та заходів для молоді, створення онлайн-ресурсів та мобільних додатків з фінансової освіти та залучення до роботи з молоддю фінансових установ та фахівців. В загальному, можна запропонувати наступні напрями підвищення кібербезпеки домогосподарств:

1. Освіта та обізнаність: підвищення обізнаності домогосподарств про онлайн-шахрайство та кіберзлочини; роз'яснення користувачам яким чином розпізнавати фейкові веб-сайти, електронні листи та SMS-повідомлення; навчання їх безпечно здійснювати онлайн-покупки та оплачувати послуги.

2. Батьківський контроль та моніторинг: використання відповідного програмного забезпечення, відслідковування онлайн-активності підлітків, щоб виявити підозрілу активність; використання програмного забезпечення для батьківського контролю, щоб обмежити доступ підлітків до шкідливих веб-сайтів; постійне спілкування з дітьми про їхню онлайн-активність та навчання відповідальному використанню мережі.

3. Законодавство та правозастосування: необхідність вдосконалення законодавства для захисту домогосподарств від онлайн-шахрайства та кіберзлочинів; підвищення кваліфікації правоохоронних органів для розслідування та запобігання онлайн-шахрайству.

4. Співпраця з державними та приватними організаціями: зі сторони державних органів, шкіл та громадських організацій – для підвищення обізнаності про фінансову безпеку; зі сторони банків, фінансових установ та інтернет-магазинів – для розробки безпечних онлайн-платформ, проведення роз'яснювальних занять; підтримки досліджень та розробок нових технологій для захисту домогосподарств від онлайн-шахрайства.

5. Розвиток цифрової грамотності: навчання домогосподарств критичному мисленню та навичкам оцінки інформації в Інтернеті, розвиток їхніх навичок розпізнавання фейкових новин та пропаганди, покращення навичок використання мережі «Інтернет» для пошуку достовірної інформації та ресурсів.

Висновки. У сучасному світі, де все більше фінансових операцій здійснюється онлайн, кібербезпека стає критичним фактором для захисту фінансового благополуччя домогосподарств. Зростання кіберзлочинності, зокрема, у вигляді крадіжок особистих даних, шахрайства з кредитними картками та фішингу, робить домогосподарства більш вразливими до фінансових втрат. Обачлива фінансова поведінка домогосподарств передбачає вжиття ними заходів для захисту своєї кібербезпеки, таких як: використання надійних паролів та їх регулярна зміна, встановлення антивірусного програмного забезпечення та брандмауерів, оновлення програмного забезпечення та операційної системи, уникання кліків на підозрілі посилання та вкладення файлів, здійснення онлайн-платежів лише на надійних чи перевірених сайтах, повідомлення про підозрілу активність у банку або фінансовій установі та інше. Підвищення фінансової грамотності та кібербезпеки домогосподарств допоможе їм покращити своє фінансове становище, захистити себе від фінансових втрат та збудувати більш стійке та успішне майбутнє.

Список використаних джерел:

- [1] Цифрова трансформація економіки України в умовах війни. (2024). Вилучено з <https://niss.gov.ua/news/komentari-ekspertiv/tsyfrova-transformatsiya-ekonomiky-ukrayiny-v-umovakh-viyny-berezen-2024>.
- [2] Cost of a Data Breach Report. (2023). *IBM Security*. Вилучено з <https://www.ibm.com/downloads/cas/E3G5JMBP>.
- [3] Overview of cyber incidents against Ukraine between 01-01-2020 and 01-01-2023. *European Repository of Cyber Incidents (EuRepoC)*. Вилучено з <https://www.swp-berlin.org/en/swp/about-us/organization/swp-projects/european-repository-on-cyber-incidents-eurepos>.

- [4] Причиною більшості шахрайських випадків з платіжними картками стало розголошення даних їхніми користувачами. (2024). *Офіційне Інтернет-представництво Національного банку України*. Вилучено з <https://bank.gov.ua/ua/news/all/prichinoyu-bilshosti-shahrayskih-vipadkiv-z-platijnimi-kartkami-stalo-rozgoloshennya-danih-yihnimi-koristuvachami>.
- [5] Войтицька, Л., & Ролік, В. (2023). Опитування з фінансової грамотності серед підлітків 11-18 років в Україні. НБУ. Вилучено з <https://talan.bank.gov.ua/uploads/ekspertyza/files/gmw-2023-survey-teens-64707f2a6d2d4221260570.pdf>.

CYBERSECURITY AS A DETERMINANT OF PRUDENT FINANCIAL BEHAVIOR OF HOUSEHOLDS

Vovchenko Oksana

Ph.D., associate professor,

Associate Professor of the Department of Finance, Banking and Taxation

Poltava National Technical University, Ukraine

***Summary.** The author proposes an approach to the study of cybersecurity as a tool for improving personal financial behavior of households. The spectrum of cyber threats and types of threats to the financial security of households in the online environment are characterized and the importance of counteracting financial losses from them in the context of digitalization is substantiated. The ways to improve the level of cybersecurity and the features of the formation of prudent financial behavior of households, taking into account current trends, are outlined.*

***Keywords:** financial behavior, cybersecurity, household, cyber threat, digitalization, Internet, personal financial security.*