УДК 338.2 doi: 10.20998/2519-4461.2023.3.64

О.І. МАСЛАК, Я.Ю. ЯКОВЕНКО

ЗАБЕЗПЕЧЕННЯ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ В УМОВАХ ЦИФРОВОЇ ЕКОНОМІКИ

Цифровізація бізнес-процесів полегшила клієнтам самообслуговування, що також зменшує витрати на оплату праці. Однак із зростанням популярності онлайн-транзакцій фінансова та економічна безпека стала актуальною проблемою. Оскільки все більше транзакцій переміщується в діджитал-середовище, фінансово-економічна безпека стає все більш важливою, бо її основною метою є захист бізнес-структур від загроз і викликів, у тому числі тих, що випливають із тенденцій Індустрії 5.0. Основні виклики фінансово-економічній безпеці в цифровій економіці включають необхідність вдосконалення електронних систем безпеки. Одним із таких заходів є інвестування в надійне програмне забезпечення для кібербезпеки, наприклад брандмауери та шифрування. Керівники також повинні бути в курсі потенційних загроз і вразливостей. Хоча нові технології, такі як блокчейн і штучний інтелект, створюють нові виклики, важливо знайти способи протистояти цим загрозам, не стримуючи інновації. Стрімке впровадження інформаційних технологій і поява криптовалют призвели до проблем кібербезпеки. У дослідженні акцентовано увагу на тому, що інноваційний характер цифрових технологій, таких як хмарні обчислення, штучний інтелект та Інтернет речей, вимагає посилення регуляторних і правових систем для захисту від кіберризиків і загроз. Крім того, в епоху великих даних існує потреба в моделях кількісного аналізу для оцінки та прогнозування ризиків фінансового ринку, забезпечуючи основу для технологічного регулювання. Також потребує вирішення проблема загроз і викликів, що виникають у зв'язку з людино-цифровою взаємодією у фінансовій сфері. У дослідженні наголошується, що кібератаки та витоки даних стають все більшою загрозою для компаній та їхніх клієнтів. Відповідно, для захисту інформації від несанкціонованого витоку та різного роду впливів необхідні заходи безпеки. Наголошується на тому, що підтримання надійної кібергігієни має вирішальне значення для будь-якого бізнесу, щоб уникнути руйнівних наслідків кібератак: важливо мати надійну політику зберігання і оновлення паролів, оновлене програмне забезпечення та регулярне резервне копіювання. Крім того, регулярне навчання співробітників найкращим практикам кібербезпеки може допомогти запобігти порушенням. Подано алгоритм реагування на загрози фінансово-економічній безпеці підприємства в умовах цифрової економіки. У статті містяться заходи щодо підвищення фінансово-економічної безпеки в умовах цифрової економіки та подано основні проблеми, з якими стикаються підприємства на шляху адаптації до цифрової економіки.

Ключові слова: фінансово-економічна безпека; діджиталізація; цифрова економіка

O.I. MASLAK, YA.YU.YAKOVENKO

ENSURING FINANCIAL AND ECONOMIC SECURITY IN THE DIGITAL ECONOMY

Digitization of business processes has made self-service easier for customers, which also reduces labor costs. However, with the growing popularity of online transactions, financial and economic security has become a pressing issue. As more and more transactions are moving to the digital environment, financial and economic security is becoming increasingly important because its primary goal is to protect business structures from threats and challenges, including those arising from Industry 5.0 trends. The main challenges of financial and economic security in the digital economy include the need to improve electronic security systems. One such measure is investing in robust cybersecurity software like firewalls and encryption. Managers also need to stay informed about potential threats and vulnerabilities. While new technologies like blockchain and artificial intelligence bring new challenges, finding ways to counter these threats without stifling innovation is important. The rapid introduction of information technologies and the emergence of cryptocurrencies have led to cyber security problems. The study emphasizes that the innovative nature of digital technologies such as cloud computing, artificial intelligence, and the Internet of Things requires strengthening regulatory and legal systems to protect against cyber risks and threats. In addition, in the era of big data, there is a need for quantitative analysis models to assess and forecast financial market risks, providing a basis for technological regulation. The problem of threats and challenges arising in connection with human-digital interaction in the financial sphere also needs to be solved. The study highlights that cyber-attacks and data breaches increasingly threaten companies and their customers. Accordingly, security measures are necessary to protect information from unauthorized leakage and various types of influences. It emphasizes that maintaining strong cyber hygiene is critical for any business to avoid the devastating effects of cyber-attacks: having robust password storage and update policy, up-to-date software and regular backups is essential. Additionally, regularly training employees on cybersecurity best practices can help prevent breaches. The algorithm for responding to threats to the financial and economic security of the enterprise in the conditions of the digital economy is also presented. The article contains steps to increase financial and economic security in the conditions of the digital economy. It presents the main problems enterprises face when adapting to the digital economy.

Keywords: financial and economic security; digitization; digital economy

У часи цифрової економіки новітні технології активно використовуються для підвищення ефективності операцій та зниження витрат: коли споживачі переходять на онлайн-банкінг, банки закривають філії; зручність онлайн-шопінгу зумовила зменшення площ роздрібних торгівельних організацій; майже усі бізнес-процеси оцифровуються та спрощуються, щоб підвищити ефективність - клієнтам надається можливість самообслуговування і тим самим зменшуються витрати на робочу силу.

Разом з цим, у сучасній цифровій економіці актуальність імперативу забезпечення фінансово-економічної безпеки загострюється, оскільки зі зростаючою популярністю здійснення ділових операцій в Інтернеті, пропорційно зросла й уразливість до небезпек кібератак та навіть витоку конфіденційних даних.

Під фінансово-економічною безпекою розуміють умови та заходи, що вживаються для забезпечення сталого функціонування підприємницьких структур та захисту їх інтересів. Відповідно, для суб'єктів господарювання вкрай важливо вживати профілактичних заходів, щоб захистити себе, своїх клієнтів і контрагентів від цих загрозливих загроз. Однією з ключових стратегій є інвестування в надійне програмне забезпечення для кібербезпеки (у якості прикладу можна навести брандмауери, шифрування та регулярні чекпоінти поточного стану фінансово-економічної безпеки).

Крім того, вкрай важливо, щоб управлінці були поінформованими та обізнаними з виявленими у ході останніх перевірок загрозами та вразливими місцями, щоб бути готовими до проактивного реагування в разі кібератаки. Ще один аспект, який заслуговує на увагу, — це вплив нових технологій, таких як блокчейн і штучний інтелект, на фінансову та економічну безпеку [6, 9, 10].

Незважаючи на те, що ці технології мають багато переваг, вони також призвели до появи нових викликів, проте основне завдання полягає не в тому, щоб перешкоджати інноваціям через можливі загрози, а в тому, щоб удосконалювати методи протидії їм.

Аналіз останніх досліджень та публікацій свідчить, що до основних викликів забезпечення фінансово-економічної безпеки в умовах цифрової економіки відноситься необхідність вдосконалення електронних систем безпеки – з цим погоджуються Дж.Марен [1] та І. Яковюк [4], а стрімке впровадження інформаційних технологій і поява криптовалют призвели до проблем кібербезпеки [2]. Як зазначають науковці Д. Павловіч [5] та Кім Донг [3], існує дефіцит фахівців із сучасних інформаційних технологій, що заважає зрозуміти поточні зміни, пов'язані з цифровізацією.

Крім того, цифрова економіка спровокувала появу нових типів ризиків, тому забезпечення економічної безпеки в цифровій економіці потребує розробки та реалізації функціональних стратегій, які враховують цифровий розвиток бізнес-середовища [7, 8].

Відповідно, в умовах сьогодення слід прагнути до балансу між ринковими та неринковими інструментами для досягнення безпеки, мінімізації несприятливих наслідків та врахування компромісів між безпекою та ефективністю, глобалізацією, справедливістю та свободою.

Виклад основного матеріалу. В епоху цифрової економіки важливого значення набуває потреба визначення факторів ризику фінансово-економічній безпеці, оцінки їхніх наслідків та заходів, які можна вжити для забезпечення не лише безпеки цифрових фінансових транзакцій, а й економічної діяльності загалом.

Зі збільшенням обсягів даних про клієнтів, що обробляються, і зростаючою роллю інтелектуальної власності в успіху продуктів не дивно, що з'являються нові форми крадіжки інформації. Конкуренти все більше цікавляться інформацією про внутрішні процеси компанії, даними про співробітників, фінансовою інформацією, інтелектуальною власністю та даними корпоративних банківських рахунків. Важливо вживати необхідних заходів для захисту конфіденційної інформації.

Перш за все, варто відзначити, що існують загальноприйняті заходи, які однаково ефективні як для фізичних осіб, так і для суб'єктів господарювання. Такі заходи включають рекомендації використовувати надійні та чіткі паролі для всіх облікових записів і регулярно їх змінювати або, наприклад, активувати двофакторну автентифікацію, якщо це можливо, щоб забезпечити додатковий рівень безпеки.

Крім того, важливо використовувати лише надійні та безпечні веб-сайти та програми для фінансових операцій, уникаючи доступу до конфіденційної інформації через загальнодоступні мережі Wi-Fi.

Суб'єктам господарювання доцільно постійно контролювати діяльність банківських рахунків і своєчасно повідомляти банк або фінансову установу про будь-які підозрілі операції. Такий підхід може допомогти запобігти шахрайству. Нарешті, підтримка програмного забезпечення та систем безпеки в актуальному стані також є ефективним профілактичним заходом.

Серед банківських установ до числа тих, хто запустив успішну практику фінансового онлайн-менеджменту, американський банк Simple (викуплений пізніше іспанським BBVA), який ще з моменту появи на ринку позиціонував себе як альтернативу традиційному банкінгу. Онлайн-банкінг від Simple став еволюційним поєднанням діджитал-інструментів економічної та фінансової безпеки для фізичних і юридичних осіб.

По-перше, дані про клієнта використовуються для моментальної звірки із закономірностями його витрат.

По-друге, є можливість скористатися функцією «безпечних витрат», що включає в себе співставлення здійснених транзакцій та майбутніх рахунків з поставленими фінансовими цілями (додатково інша функція - «цілі» - слугує для врівноваження прибутку зі здійсненими витратами).

Сьогодні спектр цифрових послуг Інтернет-банкінгу для підвищення рівня економічної та фінансової безпеки ще ширший: мобільний застосунок Allpoint за допомогою геолокації допомагає знайти найближчий банкомат для безпечного зняття готівкових коштів; для швидкого депонування чеків є утиліта Photo Check Deposit; для перерахування коштів чи миттєвого блокування викрадених карток - SendMoney тощо.

Що стосується технічного боку забезпечення фінансово-економічної безпеки, то важливо переконатися, що для захисту конфіденційної інформації баз даних підприємств (як, наприклад, найбільш небезпечні для витоку даних номери облікових записів і паролі), використовуються новітні протоколи шифрування.

Більш того, впровадження багатофакторної автентифікації може підвищити рівень безпеки та протидіяти несанкціонованому доступу до облікового запису. Ось чому регулярний моніторинг активності, що здається підозрілою, а також швидке вирішення будь-яких проблем на етапі проходження багатоступеневої автентифікації зможе допомогти запобігти підозрілим або шахрайським транзакціям. Вживаючи превентивних заходів можна попередити шпигунські, фішингові та інші спроби несанкціонованого доступу.

Суб'єкти господарювання різних рівнів щорічно стикаються з зовнішніми атаками або внутрішніми інцидентами порушення інформаційної безпеки. Приголомшлива швидкість, з якою створюється нове зловмисне програмне забезпечення, є свідченням того, наскільки складно випереджати ці загрози. Чорний

ринок вірусів величезний, і навіть невеликі проекти можуть стати чутливими до випадкових DDoS-атак. Тому активний підхід до кібербезпеки має вирішальне значення, а для запобігання потенційним загрозам необхідно постійно оцінювати та оновлювати заходи безпеки.

У той час як зручність може допомогти оптимізувати процеси та покращити взаємодію з клієнтами, ризики безпеки можуть розкрити конфіденційні дані та завдати шкоди репутації компаній, тому після інформування про витік даних (якщо такий стався), варто перейти до детального аналізу його причин.

Оскільки компанії продовжують впроваджувати нові принципи роботи та використовувати новітні технології, кожен компонент їхніх бізнес-процесів стає окремою ланкою у взаємопов'язаному ланцюжку елементів, що робить виявлення критичних точок і вразливостей, через які вони взаємодіють із зовнішнім середовищем, складнішим, ніж будь-коли.

Таким чином, оскільки бізнес все більше переходить на цифрові транзакції, стає вкрай важливо збалансувати потребу в зручності та потребу в безпеці (рис.1).

Рис. 1 - Основні етапи алгоритму реагування на загрози фінансово-економічній безпеці підприємства в умовах цифрової економіки

Джерело: розробка авторів

У разі атаки важливо провести ретельне розслідування, щоб визначити походження зламу та виявити будь-які слабкі місця в системі, які могли сприяти поширенню зловмисного програмного забезпечення.

При аналізі кіберзагроз підприємствам важливо враховувати їхню орієнтацію на сьогодення, минуле чи майбутнє. Ті, хто адаптується з поточною орієнтацією (інактивна позиція), можуть мати обмежену перспективу і, отже, нижчу ефективність адаптації. З іншого боку, суб'єктам господарювання із реактивною орієнтацією (на минуле) може бути складно синхронізуватися із існуючим кіберсередовищем, яке швидко змінюється.

Підприємства, які орієнтуються на майбутнє (інтерактивна позиція), мають два варіанти: керувати змінами або передбачати їх. Активно впливаючи на зовнішнє середовище або готуючись до майбутніх змін, підприємства можуть краще адаптуватися до кіберзагроз і захистити свої активи.

Отримавши чітке розуміння проблеми, простіше впровадити заходи, які дозволять швидко визначати індикатори кіберзагроз. Варто зазначити, що універсального рішення щодо кібербезпеки не існує, тому необхідний проактивний підхід, щоб мінімізувати виникнення подібних інцидентів у майбутньому.

На етапах відновлення та оцінки захист інформаційних систем є головним пріоритетом. Щоб досягти цього, важливо враховувати кілька ключових факторів, таких як безпека систем, ефективне вирішення інцидентів, надійне управління безперервністю бізнесу, постійний моніторинг і аудит, дотримання міжнародних стандартів, а також ретельне розслідування та судове переслідування будь-яких порушень безпеки. Вкрай важливо визначити потенційні ризики та вразливі місця.

Крім того, варто постійно оцінювати ефективність заходів кібербезпеки та узгоджувати бізнес-цілі з проблемами безпеки. Запроваджуючи чіткі політики та регулярно оновлюючи інструменти безпеки, підприємства можуть ефективно зменшити ризики кіберзагроз і захистити конфіденційні дані та операції.

Зловмисники продовжують знаходити способи використовувати вразливості в інформаційних системах, що ускладнює захист і ефективне функціонування. Усі без виключення суб'єкти господарювання повинні знати, що вони не застраховані від цих загроз, і повинні вживати відповідних заходів, щоб захистити себе.

Оскільки тактика та методи кіберзлочинців постійно розвиваються, компанії повинні застосовувати проактивний підхід, щоб запобігати атакам і захищати свої операції та інформацію. Щодо превентивних заходів, то компанії повинні застосувати багатофакторну автентифікацію, шифрування та інші заходи безпеки для забезпечення безпеки транзакцій.

При цьому повністю уникнути підприємницького ризику у контексті фінансово-економічної безпеки неможливо, оскільки бізнес- процесам є притаманні: конфліктність, невизначеність, відсутність повної та симетричної інформації, неможливість точного передбачення параметрів економічних процесів.

Разом з цим, оцінка величини та структури активів і пасивів, дозволить відповісти на питання щодо того, наскільки підприємство незалежне з фінансової точки зору; наскільки зростає чи зменшується рівень фінансової незалежності підприємства і чи відповідає стан активів і пасивів фірми завданням її фінансово-господарської діяльності.

Що стосується цифрового аспекту, то низька зацікавленість як з боку підприємств, так і споживачів, застаріла матеріальна база, відтік капіталу, низький рівень кібербезпеки та корупція в регіональних і

національних органах влади – усе це ускладнює адаптацію до умов діджитал-економіки.

Іншими проблемами виступають: відсутність нормативно-правової бази для впровадження цифрових трендів, дефіцит спеціалістів із цифровізації та труднощі з аудитом процесів впровадження. Разом з тим, незважаючи на ці проблеми, важливо продовжувати процес адаптації, щоб забезпечити довгостроковий успіх і конкурентоспроможність підприємств.

Висновки. Вплив цифровізації на усі аспекти безпеки, у тому числі фінансово-економічні, може бути як позитивним, так і негативним: підвищення прибутковості та інноваційного підприємництва, з одного боку, і збільшення монополізації та звільнення працівників, з іншого.

Однак завдяки розробці кращого механізму забезпечення фінансової та економічної безпеки менеджери підприємства можуть виявити нові загрози та сприяти довгостроковому зростанню.

Тому варто інвестувати в зручні для користувача інтерфейси та надавати чіткі інструкції, щоб допомогти клієнтам орієнтуватися в процесі цифрових транзакцій. Віддаючи перевагу як зручності, так і безпеці, компанії можуть зміцнити довіру своїх клієнтів і залишатися попереду в сучасній цифровій економіці.

Адаптувавшись до цифрового середовища, підприємства можуть поліпшити показники операційної діяльності та ефективніше використовувати інноваційні технології та залучити інвестиції для подальшого успіху.

Список літератури

1. Maren, Andrea, Jimenez., Marta, Roig. (2021). A New Global Deal Must Promote Economic Security. doi: 10.18356/27081990-90
2. Sandeep, Gogineni, Ravindrababu., Jim, Alves-Foss. (2020). Automated Detection of Configured SDN Security Policies for ICS Networks. doi: 10.1145/3442144.3442148
3. Dong, Won, Kim., Hyun, Jin, Kim., Seunghwan, Myeong. (2020). The Cloud System of Futuristic Vehicles and Security Policies. doi: 10.1109/BIGCOMP48618.2020.00-15
4. I. V. Yakoviyk., A. Yu. Turenko. (2021). Економічна безпека України як передумова забезпечення її суверенітету. Problems of Legality, doi: 10.21564/2414-990X.154.238747
5. Dejan, Pavlović., Vilmoš, Tot. (2020). Economic security as a function of corporate security: A stakeholders' perspective. doi: 10.5937/CIVITAS2001159P
6. O. I. Maslak, M. V. Maslak, N. Y. Grishko, O. O. Hlazunova, P. G. Pererva and Y. Y. Yakovenko, "Artificial Intelligence as a Key Driver of Business Operations Transformation in the Conditions of the Digital Economy," 2021 IEEE International Conference on Modern Electrical and Energy Systems (MEES), Kremenchuk, Ukraine, 2021, pp. 1-5, doi: 10.1109/MEES52427.2021.9598744.
7. Petra, Maresova., Ivan, Soukal., Libuše, Svobodová., Martina, Hedvicakova., Ehsan, Javanmardi., Ali, Selamat., Ondrej, Krejcar. (2018). Consequences of Industry 4.0 in Business and Economics. Economies, doi: 10.3390/ECONOMIES6030046
8. Безручко О.О. Управління економічним потенціалом підприємства на різних стадіях його життєвого циклу / О.І. Маслак, О.О. Безручко // *Маркетинг і менеджмент інновацій*. - 2014. - № 1. - С. 201-212.
9. Маслак О.І. Диверсифікація інноваційного розвитку промисловості в контексті перспективної інвестиційної політики / О.І. Маслак // *Інвестиції: практика та досвід*. Науково-практичний журнал. - 2010. -№4 (лютий). - С. 13-16.
10. Maslak O. Intellectual capital as a factor of economic development of Ukraine/ Maslak O. Grishko N., Hlazunova O., Maslak M.// Journal of Turiba University "Acta Prosperitatis". – 2016. – No. 7. – P. 104–118.

References (transliterated)

1. Maren, Andrea, Jimenez., Marta, Roig. (2021). A New Global Deal Must Promote Economic Security. doi: 10.18356/27081990-90
2. Sandeep, Gogineni, Ravindrababu., Jim, Alves-Foss. (2020). Automated Detection of Configured SDN Security Policies for ICS Networks. doi: 10.1145/3442144.3442148
3. Dong, Won, Kim., Hyun, Jin, Kim., Seunghwan, Myeong. (2020). The Cloud System of Futuristic Vehicles and Security Policies. doi: 10.1109/BIGCOMP48618.2020.00-15
4. I. V. Yakoviyk., A. Yu. Turenko. (2021). Економічна безпека України як передумова забезпечення її суверенітету [Economic security of Ukraine as a prerequisite for ensuring its sovereignty]. Problems of Legality, doi: 10.21564/2414-990X.154.238747
5. Dejan, Pavlović., Vilmoš, Tot. (2020). Economic security as a function of corporate security: A stakeholders' perspective. doi: 10.5937/CIVITAS2001159P
6. O. I. Maslak, M. V. Maslak, N. Y. Grishko, O. O. Hlazunova, P. G. Pererva and Y. Y. Yakovenko, "Artificial Intelligence as a Key Driver of Business Operations Transformation in the Conditions of the Digital Economy," 2021 IEEE International Conference on Modern Electrical and Energy Systems (MEES), Kremenchuk, Ukraine, 2021, pp. 1-5, doi: 10.1109/MEES52427.2021.9598744.
7. Petra, Maresova., Ivan, Soukal., Libuše, Svobodová., Martina, Hedvicakova., Ehsan, Javanmardi., Ali, Selamat., Ondrej, Krejcar. (2018). Consequences of Industry 4.0 in Business and Economics. Economies, doi: 10.3390/ECONOMIES6030046
8. Bezruchko O.O. Upravlinnya ekonomichnym potentsialom pidpryyemstva na riznykh stadiyakh yoho zhyttyevoho tsyklu [Management of the economic potential of the enterprise at various stages of its life cycle]/ O. I. Maslak, O. O. Bezruchko // *Marketynh i menedzhment innovatsiy* [Marketing and innovation management]. – 2014. - no 1. – pp. 201–212.
9. Maslak O.I. (2010) Dyversyfikatsiia innovatsiinoho rozvytku promyslovosti v konteksti perspektyvnoi investytsiinoi polityky [Diversification of innovative industrial development in the context of long-term investment policy] *Investytsii: praktyka ta dosvid.* [Investments: practice and experience] Naukovo-praktychnyi zhurnal. - 2010. –Vol. 4. - pp. 13-16.
10. Maslak O. Intellectual capital as a factor of economic development of Ukraine/ Maslak O. Grishko N., Hlazunova O., Maslak M.// Journal of Turiba University "Acta Prosperitatis". – 2016. – No. 7. – pp. 104–118.

Надійшла(received) 04.05.2023

Відомості про авторів / About the Authors

Маслак Ольга Іванівна (Maslak Olga Ivanivna) – доктор економічних наук, професор, завідувачка кафедри економіки Кременчуцького національного університету імені Михайла Остроградського; м. Кременчук, Україна; ORCID:0000-0001-6793-4367; e-mail: oimaslak2017@gmail.com

Яковенко Ярослава Юріївна (Yakovenko Yaroslava Yuriivna) – PhD з економіки, Кременчуцький національний університет імені Михайла Остроградського, старший викладач кафедри економіки; м. Кременчук, Україна, ORCID: https:// orcid.org/0000-0001-5042-2701; e-mail: yaroslavayakovenko@gmail.com