УДК: 004.056 DOI 10.33111/mise.102.3

Бєгун А.В., к.е.н., професор
кафедри комп'ютерної математики та інформаційної безпеки,
Київський національний економічний університет
імені Вадима Гетьмана

Шкоденко Т.В., магістр економічної кібернетики,
аспірант денної форми навчання,
Київський національний економічний університет
імені Вадима Гетьмана

Begun A.V., Philosophy Doctor,
Professor of the Department of Computer Mathematics
and Information Security,
KNEU named after Vadim Hetman
Shkodenko T.V., master of economic cybernetics,
full-time graduate student,
KNEU named after Vadim Hetman

АНАЛІЗ ОСОБЛИВОСТЕЙ СИСТЕМ ЗАХИСТУ ВЕЛИКИХ ДАНИХ В ЕЛЕКТРОННОМУ БІЗНЕСІ

ANALYSIS FEATURES OF BIG DATA PROTECTION SYSTEMS IN ELECTRONIC BUSINESS

***Анотація**. Ефективність захисту великих даних електронного бізнесу забезпечує високу конкурентоспроможність підприємницької діяльності на сучасному ринку. За останнє десятиліття термін «електронний бізнес» дістав широку популярність серед населення у сучасному світі, що і викликає певні загрози з боку зовнішніх чинників та формує актуальність розвитку сучасного програмного та технологічного забезпечення захисту великих даних електронного бізнесу в цілому. Актуальність обраної тематики обґрунтована підвищенням значимості електронної ролі комерції у сфері бізнес-діяльності, а також зростаючою потребою захисту учасників електронної комерції від шахрайських дій. У статті автори аналізують особливості систем захисту інформації бізнесових структур цифрової економіки. Висвітлено основні елементи сучасних технологій в контексті рівнів безпеки великих даних у сфері електронного бізнесу. Розглянуто основні проблеми, з якими стикається електронний бізнес у сфері захисту персональних і прихованих даних. Проаналізовано основні погляди провідних учених, які займалися і займаються питаннями захисту великих даних. Надано характеристику основним напрямам, з якими стикається електронний бізнес у сучасному середовищі. Запропоновано головні шляхи подолання проблеми підвищення рівня захисту даних. Визначено основні етапи використання сучасного програмного забезпечення, спрямованого на захист неструктурованих даних електронного бізнесу.*

***Ключові слова:** електронний бізнес, програми захисту, методи захисту, сучасний рівень, персональні дані, приватні дані, прихована інформація, системи злому, комп'ютерні технології.*

Abstract. *The effectiveness of the protection of big data of e-business ensures high competitiveness of entrepreneurial activity in the modern market. Over the last decade, the term "electronic business" has gained wide publicity and popularity among the population in the modern world, which in turn causes certain threats from external factors and shapes the relevance of the development of modern software and technological support for the protection of big data of electronic business as a whole. The relevance of the chosen topic is justified by the increasing importance of the electronic role of commerce in the field of business activities, as well as the growing need to protect participants of electronic commerce from fraudulent actions. In this article, the authors analyze the features of information protection systems of business structures of the digital economy. The main elements of modern technologies in the context of security levels of big data in the field of e-business are highlighted. The main problems faced by e-business in the field of protection of personal and hidden data are considered. The main views of leading scientists and researchers who were and are dealing with issues of big data protection are analyzed. The main directions faced by e-business in the modern environment are characterized, the main ways to overcome the problem of increasing the level of data protection are proposed, and the main stages of using modern software aimed at protecting unstructured e-business data are defined.*

Keywords: *electronic business, protection programs, protection methods, state of the art, personal data, private data, hidden information, hacking systems, computer technology.*

Постановка проблеми. Період XXI століття — особливий час переходу до цифрового ведення підприємницької діяльності, яка передбачає електронне виробництво послуг та товарів, що у свою чергу вимагає ефективного захисту особистих великих даних у сфері ведення електронного бізнесу в сучасних умовах. Ефективність захисту великих даних електронного бізнесу забезпечує високу конкурентоспроможність підприємницької діяльності на сучасному ринку. За останнє десятиліття термін «електронний бізнес» здобув широку популярність серед населення в сучасному світі, що спричинює певні загрози з боку зовнішніх чинників та формує актуальність розвитку сучасного програмного та технологічного забезпечення захисту великих даних електронного бізнесу в цілому.

Сьогодні значним попитом користується надійна та ефективна система захисту великих даних електронного бізнесу, як важлива складова та запорука успішності ведення електронної підприємницької діяльності в сучасному світі, який з кожним роком все більше розвивається та йде вперед за допомогою сучасних високотехнологічних винаходів та їх впровадженням в повсякденне життя кожної людини. Інформаційні технології та мережа Інтернет стають невід'ємною частиною життя економічних агентів, у зв'язку з цим створюються нові умови для здійснення бізнесу: розробка вебпропозицій, виникнення принципово нових ринків, формування ринку інноваційних товарів та послуг. Комерційна

діяльність активно переноситься в середовище Інтернету та залучає дедалі більше учасників електронних бізнес-операцій. Цей факт підтверджується активністю наукових публікацій про електронний бізнес та сучасних систем захисту великих даних.

Однак, незважаючи на зростання масштабів електронного бізнесу, як і під час здійснення будь-якої діяльності, можуть виникнути загрози несанкціонованого доступу, що може призвести до серйозних збитків.Отже, онлайн-бізнесу загрожують усі внутрішні та віддалені атаки, властиві будь-яку розподілену комп'ютерну систему, що взаємодіє за допомогою передачі даних по відкритих мережах. Тому потрібно відшукувати шляхи та методи вирішення проблем безпеки в електронному бізнесі. Актуальність обраної тематики обґрунтована підвищенням значимості електронної ролі комерції у сфері бізнес-діяльності, а також зростаючою потребою захисту учасників електронної комерції від шахрайських дій.

Аналіз останніх досліджень і публікацій. Серед провідних українських науковців та спеціалістів, які займалися дослідженням поставленого питання сучасних проблем та особливостей захисту великих даних електронного бізнесу, слід виділити таких, як З. І. Віновський, Р. М. Бліхарський, Д. О. Еймор [2], Т. М. Горний, Т. М. Харик, А. І. Соболевський, В. О. Заблоцький, Є. С. Єпіфанов [3], І. Р. Микитчин, А.І. Барбуляк та П. Р. Швед, М. Б. Клімковський, І. О. Кусий, Р. А. Озарків, Р. Р. Дубина, А. М. Кармінський [4], М. І. Макар, І. П. Війтишин, В. Р. Войтович та В. Л. Матвіїв, Н. М. Крейніна, Є. С. Стоянова, А. П. Манюшис [5], І. Т. Балабанов, В. М. Родіонова, А. Д. Шеремет, А. А. Паскова [6], О. В. Єфімова та інші.

Слід виділити також і зарубіжних науковців, які зробили значний внесок у розвиток і дослідження питань захисту особистих даних у системі електронного бізнесу та методів протидії за допомогою сучасного програмного забезпечення різним кібератакам для захисту даних. Серед провідних зарубіжних науковців, в більшості американських та європейських, слід виділити таких як: Akter S.I. [7], Altman, E.I., Tishaw, J.R., Taffler, A.A., Van Horn, P.R., Alvin, E.R., Bertil, O.P., Thorstein, B.W., Walras, J.M., Alfred A.O., Schumpeter, J.A., Wilson, J.N., Bunge, M.H., Gattenberger, K.C., Scheimin, J.P., Forrester, J.A., Weitzecker, E.E., Lovins, L. W, Smith AR, Griffin NR, Damodaran AD, McCarthy MW, Gruening JM, Monahan GI, Flynn JS, Griffin RR., Zaman D.H., Andersen T.R., Bedford J.D., Watson H.J. [8], Tsai C.W. [8], Lai C. F. [8], Chao H. C. [8] і низка інших науковців, які зробили значний вклад у розвиток поставленого питання.

Невирішені проблеми. Серед основних питань, які досі потребують подальшого розв'язання, слід виділити такі, як недосконаліть сучасного програмного забезпечення спрямованого на захист великих даних у сфері ведення електронного бізнесу, брак кваліфікованих кадрів, спроможних протистояти діючим проблемам ззовні та проблеми правильного використання сучасних інструментів Big Data у процесі ведення електронного бізнесу.

Цілі статті

1. Провести аналіз існуючого сучасного програмного забезпечення спрямованого на захист великих даних електронного бізнесу.

2. Описати особливості функціонування програм та технологій спрямованих на безпосередній захист великих даних електронного бізнесу від зовнішніх та внутрішніх чинників.

3. Запропонувати перспективні шляхи застосування сучасного технологічного та програмного забезпечення для безпосереднього захисту великих даних у сфері електронного бізнесу, як одного з основних та важливих важелів збереження високої конкурентоспроможності підприємницької діяльності на ринку.

Виклад основного матеріалу. Електронний бізнес як сфера цифрової економіки включає фінансові, торгові та усі пов'язані з іншими бізнес-транзакціями операції, які проводяться за допомогою Інтернету [2, с. 106]. Розвиток такого сучасного кластеру економічної діяльності, що являє собою інноваційно насичену галузь, створює нові економічні бізнес-моделі, надає сучасні умови ведення підприємницької діяльності, а також змінює підхід до традиційних способів продажів і стає однією з сфер, яка найбільш активно розвивається у різноманітних напрямах економіки [1]. Про це свідчать показники, подані на рис. 1.

У визначенні до електронної комерції відносять електронний обмін інформацією, електронний рух капіталу, електронні гроші, електронну торгівлю, електронний маркетинг, електронний банкінг [6, с. 173]. На сьогодні на українському сегменті під електронною комерцією у вузькому розумінні прийнято розуміти електронну торгівлю. За даними компанії «Statista», роздрібні продажі онлайн-торгівлі у всьому світі склали 1,3 трлн дол.

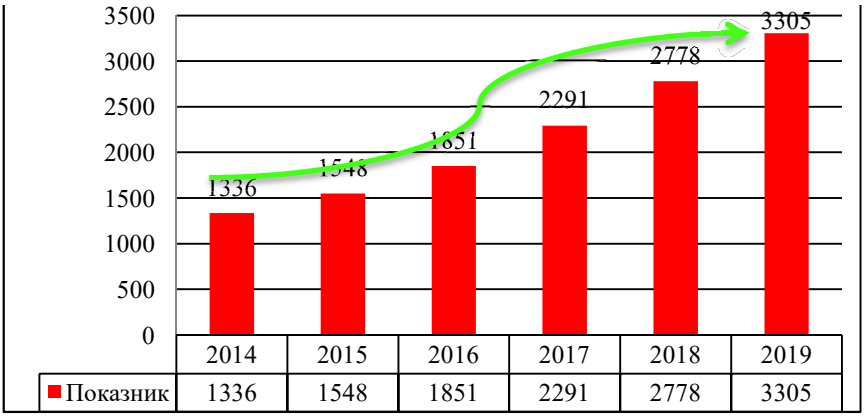

Рис. 1. Динаміка розвитку електронного бізнесу у світі, трлн дол. США

Досить поширена не до кінця правильна думка, що онлайн-бізнес почати легше, ніж традиційний. Проте це твердження дискусійного характеру, оскільки, з одного боку, немає потреби використовувати такі ресурси, як оренда приміщення (а складом для зберігання товару може бути будь-яка частина квартири, невеликого приміщення) або можна виключити користування послугами продавця та спростити логістику. Але, з другого боку, зберігають серйозність і вагомість такі види діяльності, як своєчасна та по можливості безкоштовна доставка, забезпечення оплати товару або послуги (онлайн- та офлайн-транзакції) [1, с. 43]. І тут варто приділяти увагу настройкам і забезпеченню безпеки оплати онлайн через банківські картки або електронні гаманці.

Отже, з погляду початкових інвестицій, можна виділити кілька видів електронної комерції:

1) не вимагають вкладень (дропшипінг, перепродаж за партнерською програмою);

2) які вимагають мінімальних капіталовкладень (покращений дропшипінг, продаж партнерських товарів, але на власних сайтах);

3) потребують середнього рівня інвестицій (будь-який онлайн-магазин);

4) вимагають серйозних інвестицій на введення в електронний бізнес (онлайн-магазини з великим асортиментом за суміжними лініями) [2, с. 107—108].

Між цими категоріями існують перехідні форми. Зазначимо, що онлайн-бізнес вимагає певної кваліфікації, і тут у конкурент-

ній боротьбі перемагають лише професійні гравці. Актуальність розвитку бізнесу на просторах всесвітнього павутиння вкрай висока, оскільки на даний момент кількість підприємців, задіяних у ньому, зростає в геометричній прогресії, а отже, необхідно усвідомлювати, що розвиток комерційної діяльності в Інтернеті пов'язаний як з її перевагами, так і має властиві їй ризики [6, с. 174].

Електронний бізнес пропонує низку переваг та можливостей для учасників ринку:

1) скорочення витрат з допомогою виключення чи заміни раніше значимих ресурсов. Наприклад, втрата необхідності найму штату співробітників чи оренди приміщення тощо;

2) можливість невеликих компаній досягти глобального ринку, оскільки перспективи електронної комерції настільки серйозні, що бізнес не має географічних обмежень;

3) можливість конкурувати з великими світовими компаніями;

4) можливість цілодобового зворотного зв'язку з клієнтом [2, с. 44-45].

Електронний бізнес не є єдиною можливістю для отримання прибутку, і все ж таки ніяка інша модель бізнесу не запропонує подібних переваг. До того ж надається можливість розвивати бізнес у вільний від основної роботи час або фрилансом.

Активне нарощування темпів та обсягів електронного бізнесу розширює і можливості для покупців, а саме [3, с. 220]:

• великий асортимент продукції та послуг;

• можливість цілодобової покупки;

• комфортні умови купівлі, оформлення замовлення без відвідування магазинів та супермаркетів;

• здійснення купівлі товарів із різних країн світу;

• вплив на стратегію та поведінку виробника шляхом формування відгуків та пропозицій [2, с. 109].

На тлі активного розвитку електронного бізнесу основним питанням, яке потребує підвищеної уваги з боку як вчених, так і професіоналів, залишається безпека захисту великих даних електронного бізнесу. Нині ключовою перешкодою розвитку онлайн-платежів став психологічний чинник. Так, результати опитувань показують, що розвитку інтернет-торгівлі перешкоджає недовіра безпеки онлайн-середовища та підвищені ризики потенційного шахрайства з персональними даними, зокрема і з реквізитами платіжних карток та гаманців [6, с. 175].

Прийнято виділяти кілька видів ризиків від шахрайства у віртуальній мережі:

– дублювання технічного пристрою (електронного гаманця або жорсткого диска комп'ютера);

– зміна або дублювання відомостей, повідомлень чи програм;

– крадіжка персональних даних та платіжних реквізитів;

– відмова у проведенні операцій;

– «соціальна інженерія» [3, с. 221–222].

Одним із найбільш популярних інноваційних методів підвищення безпеки систем захисту великих даних, що застосовуються учасниками електронного бізнесу, є перевірка використання сертифікованих протоколів інтернет-ритейлером. Найбільш широко застосовувані методи забезпечення безпеки онлайн-комерції можна звести до наступних [1, с. 46]:

• Secure Socket Layer (SSL) під час здійснення інтернет-банкінгу передбачає шифрування даних у разі спроби перехоплення даних, що передаються; і тут важливим стає забезпечення захисту безпосередньо сервера, у якому проводиться відповідна платіжна транзакція;

• різні способи ідентифікації власників платіжних інструментів (карт, гаманців та ін.); тут особливо виділимо перевірку кодів для карток Visa CV2, і для MasterCard — CVK2; перевірка справжності відбувається на підставі перевірки адреси (AVS);

• одноразові паролі, які отримуються в SMS або безпосередньо в банкоматі, які надсилаються на мобільний телефон для проведення конкретної транзакції;

• криптографія, що використовує асиметричні методи шифрування — системи з відкритим ключем — мають два ключі, які не можуть бути розраховані один від одного;

• ЦЕП (цифровий електронний підпис), що дозволяє легко ідентифікувати відправника запиту;

• генератори одноразових паролів, які є зовнішніми відносно комп'ютери пристрою, що підключаються за допомогою USB-порту;

• зовнішній електронний ключ, який генерується та записується на зовнішній диск при першому вході до системи та використовується надалі для здійснення платіжних транзакцій [2, с. 110].

На додаток до цього економічні агенти часто роблять додаткові заходи для забезпечення безпечного проведення інтернет-платежів під час здійснення електронного бізнесу:

1. *Обмеження використання особистого сертифіката*. Система деяких банків дозволяє використовувати електронний ключ або електронний сертифікат лише на тому комп'ютері, на якому він був створений. Через це ви можете здійснювати платежі тіль-

ки через інтернет-банкінг зі свого комп'ютера, хоча ви можете переглядати виписки на інших пристроях [3, с. 223].

2. *Віртуальна клавіатура*, щоб шахраї не могли читати дані реєстру під час набору тексту на стандартній клавіатурі з комп'ютерними вірусами.

3. Історія підключень — ця функція дозволяє користувачеві інтернет-банку визначати підключення до системи будь-кого та відстежувати несанкціоновані події.

На думку експертів, захист корпоративних інформаційних систем залежить від ряду факторів: 30 % — від технічних рішень, що застосовуються; 40 % — від інституціональних механізмів в установі; і 30 % — від морального стану суспільства та загального культурного рівня користувача [2, с. 111].

Станом на 2022 р. одними із найбільш використовуваних програм для захисту великих даих електронного бізнесу в сучасному світі є такі: «Serial Port Control», «Bitdefender», «Symantec Corporation», «TrustPort a.s.», «McAfee, Inc.» та «G DATA Software AG». Сьогодні в період XXI століття, розвитку технологій дані програми використовуються в найбільших інтернет-корпораціях сучасності [6, с. 176]. До прикладу програма для захисту великих даних «G DATA Software AG» використовується в компанії «Amazon», яка дозволяє ретельно дотримувати основні вимоги безпеки для захисту великих даних зазначенної компанії, яка є найбільшим представником сучасносі у сфері електронного бізнесу. Наприклад, одна з найбільших біотехнологічних інтернет-компаній світу «Life Technologies» використовує декілька програм захисту особлистих даних, серед яких є програма «TrustPort a.s.», яка дозволяє наперед виявляти та знешкоджувати загрози від зовнішніх чинників за допомогою раптового виявлення вірусної інформації в системі.

Висновки. На підставі проведеного дослідження зазначимо, що електронний бізнес вже тенденційно стає сучасним затребуваним та перспективним напрямом цифрової економіки, у якому економічні агенти не лише розвивають свій бізнес, але отримують можливість отримати передові знання та набути професійних навичок у різних сферах. Вихід на простори електронної комерції може забезпечити успішний старт для розвитку власного бізнесу, який пропонує комфортні умови як для продавця, так і покупця.

Однак як і будь-яка економічна діяльність, електронна комерція не захищена від загрози втручання в галузь шахраїв. Маючи широкий асортимент методів, що використовуються для забезпечення безпеки великих даних в інтернет-середовищі, учаснику

електронного бізнесу доцільно пам'ятати, що багато залежить безпосередньо від користувача. Найчастіше причиною шахрайського доступу до облікового запису учасника операції може стати його неуважність або недбалість.

Отже, щоб уникнути потенційних ризиків власнику облікового запису слід обмежити доступ до платіжних реквізитів та персональних даних шляхом регулярної зміни паролів до систем та проведення операцій лиш тільки на попередньо перевірених пристроях. Проте основне вирішення проблеми інформаційної безпеки великих даних електронного бізнесу залишається в основному за апаратним та програмним забезпеченням.

Бібліографічні посилання

1. Бєгун А.В.,Плахтій М.О., Осипова О.І., Урденко О.Г. Аналіз зовнішніх і внутрішніх загроз функціонування електронного квитка видовищних заходів. *Моделювання та інформаційні технології в економіці*. 2021. № 101. С. 20–31.
2. Еймор Д.О. Електронний бізнес. Еволюція та революція. Харків: Вільямс, 2021. 320 с.
3. Єпіфанов Є.С., Атаров Н. З. Основні етапи розвитку електронного бізнесу. *Запитання регіональної економіки*. 2020. № 3. Т. 28. С. 106-111.
4. Кармінський А.М. Інформатизація бізнесу: концепція, технології, системи захисту великих даних. Київ: Фінанс та статистика, 2020. 623 с.
5. Манюшіс А.П., Смольянінов В., Тарасов В. Віртуальне підприємство як ефективна форма організації зовнішньоекономічної діяльності. *Проблем теорії та практики управління*. 2020. № 4. С. 3-27.
6. Паскова А.А. Технології «Big Data» в автоматизації технологічних і бізнес-процесів. *Науковий огляд. Технічні науки*. 2019. № 4. С. 23-27.
7. Akter S.I. Big data analytics in E-commerce: a systematic review and agenda for future research. Shahriar Akter, Samuel Fosso Wamba. *Electronic Markets*. Vol. 26, Issue 2. Springer International Publishing AG. 2019. P. 173-194.
8. Big data analytics: a survey. Tsai C.-W., Lai C.-F., Chao H.-C. and Vasilakos A.V. *Journal of Big Data*. 2021. Vol. 2. № 1. P. 29-32.
9. Watson H.J. Tutorial: Big Data analytics: Concepts, technologies, and applications. Comm. of the Association for Information Systems. 2019. Vol. 34. Article 65. P. 1247-1268.

Статтю подано до редакції 21.11.2022