Громадська організація “Міжнародна асоціація науковців”

Національний університет “Полтавська політехніка імені Юрія Кондратюка”

кафедра економіки, підприємництва та маркетингу

Київський національний університет

імені Тараса Шевченка

кафедра ядерної фізики та високих енергій

Національний університет харчових технологій

кафедра жирів, хімічних технологій харчових добавок та косметичних засобів

Громадська організація

“Європейська Асоціація Економістів”

Лодзький університет (Польща)

Варшавська школа економіки (Польща)

Національний технологічний інститут Мотилала Неру Аллахабад (Індія)

Батумський державний університет імені Шота Руставелі (Грузія)

Університет менеджменту безпеки в Кошицях (Словаччина)

МАТЕРІАЛИ
IV заочної Міжнародної
науково-практичної конференції
“АКТУАЛЬНІ ПРОБЛЕМИ НАУКИ ТА ОСВІТИ: РЕАЛІЇ ТА ПЕРСПЕКТИВИ”

11 листопада 2025 року,
м. Київ

2025

УДК 004.738.5:004.056.5:330

Григор'єва Олеся Володимирівна
к.е.н., доц.,
Національний університет "Полтавська політехніка імені Юрія Кондратюка",
м. Полтава
ORCID ID: https://orcid.org/0000-0001-7524-7161

ЗАХИСТ ДАНИХ У СИСТЕМАХ ЕЛЕКТРОННОГО БІЗНЕСУ: ЕКОНОМІЧНІ ТА ОРГАНІЗАЦІЙНІ АСПЕКТИ

Olesya Hryhoryeva

DATA PROTECTION IN ELECTRONIC BUSINESS SYSTEMS: ECONOMIC AND ORGANIZATIONAL ASPECTS

Електронний бізнес відіграє ключову роль у розвитку підприємницької діяльності, набуваючи особливого значення в умовах війни в Україні та для мікро й малого підприємництва. Особливістю електронного бізнесу, є залучення до діяльності постачальника послуг проміжного характеру в інформаційні й сфері, якій у відповідності із Законом України "Про електронну комерцію" не несе відповідальності за автоматичне, тимчасове та проміжне зберігання інформації і за шкоду, завдану внаслідок використання результатів таких послуг [1]. Тож питання захисту інформаційних даних цілком та повністю є завданням власників електронного бізнесу, а в сучасних умовах – це не просто вимога цифрового світу, а базис, від якого залежить саме його існування.

Основні ризики втручання у інформаційні системи електронного бізнесу полягають у наступному:

- ✓ втручання в систему електронної документації, що може призвести до порушення конфіденційності, втрати комерційної інформації та конфіденційних даних;
- ✓ фінансові збитки через заміну маршруту транзакцій, створення хибних платежів, злом захисту інформації підприємства або переадресації масивів даних;
- ✓ втручання у робочі системи електронного бізнесу через блокування роботи систем, шифрування чи знищення даних та резервних копій, наслідком чого є неможливість належного користувача користування системою
- ✓ витік бізнес інформації у зовнішнє середовище через електронні мережі, зараження вірусами цифрових систем тощо.

Витік інформації, що має статус комерційної таємниці, може коштувати бізнесу занадто дорого через заподіяння шкоди його репутації, призвести до додаткових витрат або навіть стати причиною ліквідації бізнесу.

До комерційної таємниці, відповідно до законодавства України [2] відносять специфічну інформацію, яка має комерційну цінність для бізнесу та

недоступна для загалу. Її ключова ознака – цінність для підприємства та потенційна шкода у разі розголошення, тобто це відомості, що мають реальну або потенційну комерційну цінність; які невідомі третім особам та підлягають захисту за допомогою правових, організаційних чи технічних заходів.

З економічної точки зору система даних електронного бізнесу також слід віднести до комерційної таємниці з поширенням всіх аспектів її захисту.

Безумовно, нормативно-правова база створюю юридичне підґрунтя захисту даних електронного бізнесу. Але для запобігання їх витоку слід забезпечити належний рівень захисту інформації від загроз, які можуть виникати як із середини роботи електронного бізнесу, так і ззовні.

Провадження електронного бізнесу суттєвим чином підвищує ризики кіберзлочинів через використання шкідливого програмного забезпечення (віруси, трояни); фішингові атаки для отримання паролів чи іншої чутливої інформації; злом систем електронного бізнесу з метою заволодіння даними; атаки на партнерів електронного бізнесу, які мають доступ до її конфіденційної інформації, хакери можуть атакувати саме їх.

Усвідомлення цих ризиків – перший крок до створення ефективної системи захисту.

Перш за все, необхідно розробити чітку політику доступу до даних електронного бізнесу та окреслити коло тих осіб, які мають доступ до бази даних. При цьому ефективним буде створення системи багаторівневого доступу, у якій кожен рівень має свої обмеження та права.

Обов'язковим заходом забезпечення безпеки електронного бізнесу стає шифрування даних, яке перетворює інформацію в код, який неможливо прочитати без спеціального ключа. Таким чином, у випадку, якщо зловмисники отримають доступ до даних, вони не зможуть їх використати.

Ще одне простий, проте ефективний спосіб убезпечення даних електронного бізнесу – створення резервних копій, тому іноді навіть найнадійніші системи захисту можуть не спрацювати. Саме тому резервне копіювання даних – ключовий елемент у забезпеченні інформаційної безпеки. Втрата інформації може бути катастрофічною для бізнесу, але якщо у є резервні копії, завжди є можливість відновлення та продовження роботи без значних втрат. Головне, щоб резервні копії зберігалися у безпечному місці, бажано у хмарному сховищі або на віддалених серверах.

Створення антивірусних програм та міжмережевих екранів створюють досить надійний захист бази даних через блокування шкідливих програм та вірусів та запобігання несанкціонованого доступу через аналіз внутрішнього трафіку електронного бізнесу та швидкого усунення спроб витоку даних.

Важливим організаційним заходом захисту даних електронного бізнесу є створення та впровадження системи управління інформаційною безпекою (ISMS – Information Security Management System) та хмарних технологій. Система аналізує інформаційні потоки бізнесу, бази даних та пропонує для

реалізації ефективні заходи щодо виявлення, оцінки та зменшення ризиків, формуючи надійний бар'єр проти кіберзагроз.

Хмарні технології забезпечують надійне зберігання інформації та доступ до неї з будь-якого місця, а також надають додаткові засоби захисту, такі як шифрування та резервне копіювання. В поєднанні з системою управління інформаційною безпекою ISMS хмарні технології можуть значно підвищити рівень безпеки електронного бізнесу, ефективність управління інформаційними ресурсами, знижувати ризики втрати даних [3].

Отже, інформаційна безпека та захист даних електронного бізнесу вимагають комплексного підходу з моніторингом стану інформаційної системи, регулярного оновлення програмного забезпечення, та превентивних заходів запобігання новим загрозам ти викликам кіберпростору. Система інформаційної безпеки має бути гнучкою та динамічною, здатною швидко реагувати на будь-які зміни.

Список використаних джерел

1. Закон України "Про електронну комерцію". *Відомості Верховної Ради (ВВР), 2015, № 45, ст.410.* URL: https://zakon.rada.gov.ua/laws/show/675-19#Text

2. Цивільний кодекс України. Відомості Верховної Ради України (ВВР), 2003, №№ 40-44, ст.356. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text

3. URL: https://gigatrans.ua/ua/news/nformac-yna-bezpeka-p-dpri-mstva-ta-osnovn-zasadi-zahistu-danih