ГОСПОДАРСЬКЕ ПРАВО; ГОСПОДАРСЬКО-ПРОЦЕСУАЛЬНЕ ПРАВО

УДК 347.77:004.738.5
DOI https://doi.org/10.32844/2618-1258.2024.4.10

ВОЛИНЕЦЬ В.В.

ПОЛІТИКА КОНФІДЕНЦІЙНОСТІ В ЕЛЕКТРОННІЙ КОМЕРЦІЇ: НАЙКРАЩІ ПРАКТИКИ ТА ПРАВОВІ ВИМОГИ

E-COMMERCE PRIVACY POLICY: BEST PRACTICES AND LEGAL REQUIREMENTS

Стаття присвячена дослідженню питання політики конфіденційності в електронній комерції, кращі практичні та правові аспекти. Електронна комерція це економічно вигідна сфера, оскільки вона не має прив'язки до територіальності і часових бар'єрів, має широкий спектр послуг, які можуть надаватися будь коли і будь куди. Успіх електронної комерції важко переоцінити, однак зовнішні регулятори, які прагнуть удосконалити цю галузь, досить часто зіштовхуються з проблемами, які потребують невідкладного вирішення. Однією із таких проблем є збереження конфіденційності власних даних і даних споживачів. Успішні компанії вже давно переглянули власну політику конфіденційності, яка б задовольняла вибагливих клієнтів. Сюди відноситься насамперед дотримання законодавства у сфері захисту персональних даних, а також розробку прозорих і зрозумілих умов збирання та обробки інформації. Прискорення цього процесу пов'язують із вибагливістю споживачів, оскільки вони прагнуть придбати товар або послугу, не відкривши при цьому конфіденційні дані третім особам.

Варто зазначити, що втрата конфіденційних даних майже у всі випадках призводить до фінансових втрат, тому саме на рітейлерах лежить відповідальність забезпечити захист даних і врегулювати свою діяльність таким чином, щоб мати змогу й надалі отримувати прибутки й підтримувати репутацію. Серед відомих стандартів збереження конфіденційності варто назвати інноваційні технології, зокрема шифрування та двофакторну аутентифікація, регулярне оновлення сайтів, навчання персоналу з метою зниження витоку інформації і сприяння її захищеності. У багатьох країнах світу вже діють або впроваджуються нові закони, які регулюють захист конфіденційних даних. Визначений крок вимагає від компаній переглянути свою політику конфіденційності, з метою відповідності законодавчим вимогам та уникненню штрафів.

Наразі перегляд і вдосконалення політики конфіденційності є невід'ємною частиною успішного розвитку кожної компанії, яка працює у сфері цифрової економіки. Цей процес здатний зміцнити довіру споживачів і сформувати конкурентні переваги на ринку електронної комерції. Практика містить чимало успішних компаній, які розробили власні програми захисту конфіденційних даних.

Ключові слова: *конфіденційність даних, електронна комерція, двофакторна аутентифікація, витік інформації, кіберзагроза, кібератака.*

The article is devoted to researching the issue of privacy policy in electronic commerce, the best practical and legal aspects. E-commerce is an economically profitable field, as it is not tied to territoriality and time barriers, has a wide range of services that can be

© ВОЛИНЕЦЬ В. В. – доктор юридичних наук, професор кафедри готельно-ресторанної справи (Київський університет туризму економіки і права) ORCID ID: 0009-0003-0714-236X

provided anytime and anywhere. The success of e-commerce can hardly be overstated, but external regulators seeking to improve the industry are often faced with problems that require urgent solutions. One of these problems is maintaining the confidentiality of one's own data and data of consumers. Successful companies have long revised their privacy policies to satisfy demanding customers. This primarily includes compliance with legislation in the field of personal data protection, as well as the development of transparent and understandable conditions for the collection and processing of information. The acceleration of this process is associated with the fastidiousness of consumers, as they seek to purchase a product or service without revealing confidential data to third parties.

It is worth noting that the loss of sensitive data almost always leads to financial losses, so it is the responsibility of retailers to ensure that data is protected and to regulate their operations in such a way that they can continue to generate profits and maintain reputation. Among the well-known privacy standards, it is worth mentioning innovative technologies, in particular encryption and two-factor authentication, regular updating of sites, training of personnel with the aim of reducing information leakage and promoting its security. Many countries around the world already have or are implementing new laws that regulate the protection of confidential data. The specified step requires companies to revise their privacy policies in order to comply with legal requirements and avoid fines.

Currently, reviewing and improving the privacy policy is an integral part of the successful development of every company in the field of the digital economy. This process can strengthen consumer confidence and create competitive advantages in the e-commerce market. The practice includes many successful companies that have developed their own data protection programs.

Key words: *data privacy, e-commerce, two-factor authentication, information leak, cyber threat, cyber attack.*

Вступ. Політика конфіденційності в електронній комерції набуває ширшого значення в умовах стрімкого розвитку цифрових технологій та збільшення обсягів персональних даних, які обробляють компанії. Захист конфіденційних даних користувачів є ключовим чинником, який впливає на підтримку довіри клієнтів і запобігає наявним юридичним ризикам. Актуальність цієї теми обумовлена складністю цього питання та жорсткими правовими вимогами у сфері обробки й збереження персональних даних. Компанії які не мають достатнього рівня захисту не можуть здійснювати економічну діяльність, оскільки мають значний ризик того, що їхніми даними чи даними їхніх клієнтів заволодіють треті особи. В рамках цього законотворці продовжують працювати ад процесами законотворчого і технічного захисту конфіденційності даних.

Постановка завдання. Мета дослідження полягає у комплексному окресленні питання політики конфіденційності в електронній комерції, спираючись на досвід провідних компаній та правові вимоги.

Аналіз останніх досліджень і публікацій. Дослідженням питання політики конфіденційності в електронній комерції займалася низка вітчизняних науковців, зокрема Ю. О. Шкригун [1], О. Є. Мервінський [2], О. В. Булах [5], Є. Гурчунова [7] та інші. Однак незважаючи на розробленість теми, питання залишається невирішеним і потребує детального опрацювання, оскільки сфера електронної комерції продовжує інтенсивно розвиватися й надалі.

Результати дослідження. Електронний бізнес доцільно розглядати як діяльність, що охоплює електронну комерцію, тобто електронну торгівлю, яка має ширший функціональний та загальний напрямок розвитку. Електронна комерція є різновидом комерційної діяльності, що здійснюється шляхом електронної взаємодії між економічними суб'єктами. Водночас, електронна торгівля є конкретною формою підприємницької діяльності, яка спрямована на продаж товарів і послуг через мережу Інтернет. Ці поняття взаємодоповнюють одне одного, формуючи сучасну структуру електронного бізнесу та забезпечуючи його ефективну функціональність у цифровому середовищі [1, с. 315].

Захист конфіденційних даних є пріоритетом діяльності будь-якої компанії. Сфера електронної комерції є тим осередком, в якому цей захист особливо цінний, оскільки фізична комунікація між сторонами відсутня або зведена до мінімуму. Електронна комерція це стійка економічна галузь, яка досить успішно показала себе на практиці. Успіх цієї галузі полягає в тому, що за досить короткий проміжок часу споживач може задовольнити власні потреби, обрати потрібний товар чи скористатися послугою, не виходячи із дому.

Вітчизняний дослідник О. Мервінський зазначає, що масовий характер використання персональних даних у сфері електронної комерції формує підґрунтя для низки порушень при їх обробці, особливо в процесі збирання, накопичення, зберігання, оновлення та використання. Цей процес значно підсилює ризик незаконного втручання третіх осіб у приватне життя людини. Загалом, ризики у сфері електронної комерції пов'язані насамперед із ймовірністю нанесення шкоди через розповсюдження недостовірної чи неналежної реклами, ризики пов'язані із незаконною обробкою даних, в тому числі їх втрати чи випадкового знищення, збереження від незаконного доступу до них [2, с. 36].

Діяльність суб'єктів господарювання в сфері електронної комерції повинна відповідати чітким і дієвим вимогам законодавства у сфері захисту персональних даних, оскільки обробка та зберігання конфіденційної інформації клієнтів є важливою складовою електронного бізнесу. Компанії зобов'язані забезпечувати належний рівень захисту споживачів задля уникнення їх неправомірного використання, витоку чи викрадення. Одним із нормативно-правових документів у сфері регулювання онлайн торгівлі, в тому числі й захисту персональних даних є GDPR (General Data Protection Regulation) – Загальний регламент захисту даних, який набрав чинності 25 травня 2018 року. Зміст регламент визначає правила щодо захисту персональних даних фізичних осіб та регулює їх вільний рух у межах Європейського Союзу. Основна мета GDPR полягає в забезпеченні високого рівня захисту даних і підвищення довіри до цифрових послуг. Вказаний регламент встановлюють чіткі правила щодо збору, обробки та зберігання персональних даних [3].

Порушення цих норм може призвести до великих штрафів та репутаційних втрат для суб'єктів господарювання. Зокрема, компанії повинні інформувати користувачів про те, які дані збираються, з якою метою і як вони будуть використовуватись. Не менш важливим аспектом є надання користувачам права доступу до своїх даних, можливості їх редагування або видалення, у випадках, якщо це передбачено законодавством.

Компанії також мають право запроваджувати сучасні технічні та організаційні заходи для захисту персональних даних, зокрема шифрування, багаторівневу аутентифікацію та регулярні перевірки систем безпеки. Необхідно забезпечити прозорість та доступність політики конфіденційності для споживачів аби ті могли легко знайомитися з умовами обробки їхніх даних. Прозорість і чіткість є запорукою успішного бізнесу.

Відповідно до статті 1 ст. 4 Загального регламенту захисту даних (GDPR), поняття «захист персональних даних» охоплює «будь-яку інформацію, яка стосується ідентифікованої або такої, що може бути ідентифікована фізичної особи (суб'єкта даних)». Основним елементом цього визначення є процес «ідентифікації», який передбачає зв'язок інформації з конкретною фізичною особою. Ідентифікаційні дані мають суто індивідуальний характер і є унікальними для кожної особи, що, в свою чергу, дозволяє відрізнити її від інших осіб. Таким чином, інформація, яка може використовуватися для ідентифікації особи, належить до персональних даних.

Згідно з вимогами GDPR, власники електронних магазинів повинні забезпечити комерційну діяльність нормам захисту персональних даних за трьома основними напрямами. Перш за все, це адаптація «Умов надання послуг» (Terms of service), де необхідно чітко регламентувати взаємодію з користувачами. Далі слід забезпечити наявність «Політики конфіденційності» (Privacy Policy), яка містить детальний опис способів збору, обробки та зберігання персональних даних. Також важливим аспектом є розробка «Політики використання файлів cookie» (Cookies Policy), яка регламентує роботу з файлами cookie для збору інформації про поведінку користувачів на вебсайті.

Комерційна діяльність повинна забезпечуватися захистом внутрішніх документів і даних відповідно до вимог, визначених регламентом ЄС. Для цього необхідно, щоб налаштування процесів обробки персональних даних здійснювався таким чином, щоб структурні підрозділи комерційних компаній відповідали за певну частину цього процесу в межах своїх функціональних обов'язків. Наступним важливим кроком є налагодження співпраці з контрагентами та іншими суб'єктами, яким можна передавати дані клієнтів, з впевненістю, що інформація не буде втрачена або несанкціоновано доступна третім особам.

Крім цього, необхідно привести вебсайти, на яких функціонує Інтернет-магазин, у відповідність до вимог, визначених GDPR. Впровадження таких процесів буде значно складнішим без належно підготовленого персоналу, тому одним із ключових завдань керівників є забезпечення навчання співробітників, надання їм необхідних знань та навичок, що стосуються обробки та захисту персональних даних. Лише системний підхід до організації захисту даних зможе забезпечити належне виконання вимог GDPR та надійний рівень захисту конфіденційної інформації клієнтів [4].

Шлях розвитку електронної комерції характеризується загрозою надмірної інтенсифікації конкуренції всередині ринку, оскільки споживачі, зважаючи на розвиток сучасних бізнес-моделей мають низку переваг вибору та керуються в першу чергу ціновим фактором в процесі вибору. У зв'язку з цим компанії змушені шукати нові способи залучення клієнтів задля підтримки власної конкурентоспроможності. Використання значного обсягу даних є головним інструментом, який сприяє швидкій адаптації до мінливих умов на цифровому ринку. Таким чином, розвиток електронної комерції сьогодні збільшується не лише на основі розширення асортименту товарів, але й за умови ефективного використання аналітичних інструментів, що сприяють оптимізації їх діяльності [5].

Всі електронні трансакції в Інтернеті супроводжуються передачею даних, тому дотримання їх конфіденційності є важливим завданням для компанії. У випадку втрати конфіденційності даних під час купівлі товарів через інтернет, це значно підриває довіру споживачів і може серйозно вплинути на розвиток бізнесу ритейлерів. Саме тому переважна більшість ритейлерів вживає заходів для захисту конфіденційних даних. Одним із таких заходів є систематичні тренінги щодо захисту персональних даних. Зміст тренінгів полягає у зобов'язанні навчати своїх співробітників захищати конфіденційні дані компанії, незалежно від того кому вони належать. Підготовлені працівники можуть виявити і зменшити потенційні ризики, пов'язані із витоком даних та фішингом. Навчання дає змогу співробітникам розпізнати та уникнути певних пасток, зменшуючи ймовірні порушення. Наступним кроком в системі захисту конфіденційних даних в е-комерції є мінімізація цих даних. Компанії, які займаються е-комерцією повинні уникати збору надмірної чи неревалентної інформації, оскільки чим її буде більше, тим важче її контролювати, а відтак, і захищати. Збір лише важливої інформації зменшує ризики витоку даних та покращує захист конфіденційності. Тому компанії повинні звернути увагу на те, який об'єм інформації збирається і як він використовується.

Наступним кроком захисту конфіденційних даних є клієнтоорієнтованість. Її зміст полягає у визначенні самими клієнтами переваг захисту конфіденційних даних тією чи іншою компанією. Надання пріоритету клієнтам у сфері безпеки є не лише юридичною вимогою, але й визначальним аспектом формування довіри, лояльності та позитивної репутації бренду.

Ще одним визначальним кроком, який підсилює захист конфіденційних даних є обрання надійної платіжної системи. В рамках цього компаніям пропонується співпрацювати лише з тими платіжними системами, які відповідають стандартам безпеки даних. Цей процес забезпечує надійну обробку платіжної інформації і тим самим захищає клієнтів від кіберзагроз, спрямованих на заволодіння фінансовими даними. Важливо наголосити, що платіжні системи є цифровими охоронцями електронних транзакцій, здатними захистити фінансові та особисті конфіденційні дані від впливу третіх осіб і їх несанкціонованих дій.

Однією із головних особливостей захисту є також розробка плану кібербезпеки. Створення плану кібербезпеки є важливою умовою для оперативного вирішення проблем у разі виявлення кіберзагрози. Такий план необхідний для запобігання пошкодженням серверів та втраті важливих даних. Основною метою цього документу є розробка покрокової інструкції, яка дозволить команді швидко реагувати на інциденти, зменшуючи ризики та наслідки від певних небезпек.

З огляду на безперервний розвиток електронної комерції, захист конфіденційних даних є ключовим завданням у сфері е-комерції. Дотримання високих стандартів безпеки є необхідною умовою для забезпечення захисту інформації споживачів. Прозорість у роботі компаній та їхня підзвітність у питаннях кібербезпеки сприяють зміцненню довіри та лояльності клієнтів. Це, в свою чергу, є вирішальним фактором для забезпечення довгострокової стабільності та успіху в умовах розвитку цифрової економіки [6].

Останні роки світ уже був занепокоєний зростанням кібератак. Однак із початком пандемії більшість організацій у сфері онлайн торгівлі та електронних фінансів, перейшли в онлайн-середовище, і частка електронної комерції на ринку роздрібної торгівлі досягла 17% у 2020 році, відповідно до звіту UNCTAD та eTrade. Варто відзначити, що за 2019 та 2020 роки, обсяг продажів в електронній комерції виріс на майже трильйон доларів.

За даними аналітиків Cybervore з прогнозом eMarketer, до грудня 2021 року американські ритейлери продадуть товар онлайн на суму, що перевищує $843,15 млрд. Варто відзначити, що успіх онлайн маазинів залежит не від якості і асортименту продукції, що реалізується, а від безпечного простору, на що насамперед звертають увагу споживачі. За даними дослідження Cybervore, 83% організацій в США технічно уразливі хакерами. Власникам онлайн-бізнесу важливо забезпечити дотримання норм кібербезпеки. З цією метою рекомендується впровадити

стандарт PCI, які б забезпечили захист інформації, пов'язаної з кредитними картками клієнтів. Також варто використовувати систему верифікації адреси, яка порівнює реальну адресу власника картки з даними, збереженими у банку-емітенті. Не слід забувати про встановлення SSL-сертифікату, який забезпечує безпечне передавання даних на сайті через їх шифрування. Крім того, необхідно застосовувати безпечні протоколи https для захисту інформації користувачів.

На сьогодні активно впроваджуються алгоритми штучного інтелекту та машинного навчання, які можуть швидко виявляти проблеми та надсилати сповіщення у разі збоїв. Такі системи здатні розпізнавати шахрайські дії та навіть скасовувати підозрілі транзакції.

Іноді хакери інтегрують шкідливий код на платіжну сторінку інтернет-магазинів. Неправильне або навмисне перепрограмування веб-застосунків дозволяє шахраям маніпулювати фінансами онлайн-платформи на свій розсуд. У сфері електронної комерції поширеними є кіберзлочини, що використовують вірусний код.

В боротьбі за неправомірною наживою шахраї вигадують все нові й нові методи, які сприяють заволодінню коштів клієнтів чи конфіденційними даними в е-комерції. Одним із таких методів є міжсайтовий скриптинг (XSS) – вбудовування вірусного коду на сервер з метою викрадення файлів cookies. Основною метою шахраїв є саме персональні дані та облікові записи клієнтів е-комерції. В такому випадку для заволодіння даними використовується SQL-ін'єкція – впровадження фальшивого коду на сторінки онлайн-магазину, що дозволяє викрадати бази даних. Інколи використовується такий метод як «інфікування» файлів cookie – процес змінюючи файли cookie, хакери отримують доступ до несанкціонованої інформації про користувачів. Керування віддаленим кодом (Remote Command Execution) – це атака, під час якої хакер дистанційно надсилає команди на чужий пристрій [7].

Таким чином, в процесі дослідження з'ясовано, що розвиток ІТ-технологій це непростий процес, який з кожним кроком у своєму розвитку збільшує силу та обсяг, рухаючись з великою швидкістю. Наразі життя людини все глибше й глибше занурюється у цифровий формат. Саме тому компанії повинні докладати чималих зусиль для того, щоб споживач відчував себе захищеним і міг безперешкодно здійснювати купівлю товару через мережу інтернет, не звертаючи увагу на зовнішні загрози. Міжнародне законодавство також підсилено працює у цьому напрямку, зобов'язуючи ритейлерів впроваджувати в свою діяльність новітні розробки, в тому числі й на базі штучного інтелекту. Законодавчий і технічний аспект цього питання вже дає плідні результати, сприяючи повноцінному захисту прав споживачів і самих власників електронної комерції.

Вимоги до впровадження інноваційних рішень, таких як автоматизовані системи моніторингу та аналізу транзакцій, можуть ефективно виявити та запобігти шахрайству в електронній комерції. Крім того, регуляторні органи наполягають на впровадження комплексних механізмів шифрування даних і багатофакторної автентифікації, що гарантує додатковий рівень захисту.

Дотримання таких вимог лише покращує загальну безпеку онлайн-платформи, але й сприяє зміцненню довіри клієнтів до ритейлерів. Компанії, які відповідають стандартам безпеки, мають конкурентну перевагу, оскільки споживачі стають більш важливими для захисту своїх персональних даних. Також міжнародна співпраця у сфері кібербезпеки дозволяє більш ефективно координувати заходи між країнами для боротьби із серйозними кіберзагрозами.

Отже, підтримка кібербезпеки є критично важливою умовою для забезпечення надійного функціонування електронної комерції. Ефективні заходи, зокрема навчання співробітників, контроль доступу до конфіденційної інформації та шифрування даних, значно знижують ризики кібератаки на конфіденційні дані клієнтів. Дотримання міжнародних стандартів безпеки та використання сучасних технологій та штучного інтелекту, сприяють захисту як бізнесу, так і прав споживачів. Впровадження системи моніторингу та резервного копіювання інформації гарантують стійкість до інцидентів і забезпечують безперервність діяльності. Таким чином, інвестування в кібербезпеку є ключовим елементом збереження довіри клієнтів і сталого розвитку е-комерції.

Висновки. Питання захисту конфіденційних даних буде актуальним і надалі, оскільки сектор електронної комерції розвивається й надалі. Важливо забезпечити баланс між нормативною базою та технічними можливостями захисту конфіденційних даних в електронній комерції. Поміж з тим головним залишається питання дослідження засобів захисту конфіденційних даних, зважаючи на розвиток нових секторів цифрової економіки. Невід'ємною складовою таких заходів є впровадження інноваційних стандартів кібербезпеки та штучного інтелекту для моніторингу й запобігання можливим загрозам. Ефективність захисту даних залежатиме від тісної співпраці між державними органами, цифровим бізнесом і споживачами. Лише таким чином можна досягти стійкого розвитку сектора електронної комерції та забезпечити високий рівень довіри до цифрових платформ.

Список використаних джерел:

1. Шкригун Ю. О. «Електронний бізнес», «електронна комерція» та «електронна торгівля»: відмінності й особливості. *Управління економікою: теорія та практика* : Зб. наук. пр. ІЕП НАНУ. 2020. С. 312–325. (дата звернення 07.10.2024)

2. Мервінський О. Європейські вимоги щодо захисту персональних даних у сфері електронної комерції. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, вип. 2 (30), 2015. С. 34–40. URL: https://ela.kpi.ua/server/api/core/bitstreams/5b9bcf0b-4000-4fa9-851e-347a28175910/content (дата звернення 11.10.2024)

3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: https://eur-lex.europa.eu/eli/ reg/2016/679/o (дата звернення 03.10.2024)

4. GDPR для інтернет-магазина 2019. URL: https://bsoprivacygroup.com/ru/gdpr-dlia-internet-mahazynu/ (дата звернення 04.10.2024)

5. Булах О. В. Вплив мобільних технологій на розвиток світового ринку електронної комерції. *Академічні візії*, 21. 2023. URL: https://academy-vision.org/index.php/av/article/view/466/418 (дата звернення 01.10.2024)

6. Як забезпечити конфіденційність даних в електронній комерції. URL: https://7-price.com/blog/how-to-ensure-data-privacy-in-ecommerce (дата звернення 05.10.2024)

7. Гурчунова Є. Як захистити бізнес в інтернеті від шахраїв та хакерів: керівництво до дії. *Інтернет маркетинг*, 2021. URL: https://aboutmarketing.info/internet-marketynh/yak-zakhystyty-biznes-v-interneti-vid-shakhrayiv-ta-khakeriv-kerivnytstvo-do-diyi/ (дата звернення 06.10.2024)