Юридичні аспекти захисту конфіденційності та безпеки даних в електронній комерції

Волинець В.В.[1]

Опубліковано	Секція	УДК
30.03.2024	Економіка	347.7

DOI: https://doi.org/10.5281/zenodo.11189625

Анотація. Щоденно у світі електронної комерції відбувається велика різноманітність транзакцій, багато з них вимагають надання доступу до даних споживачів. Однак багато користувачів висловлюють побоювання щодо надання особистих даних через часті випадки зловживання отриманою інформацією, використання її в рекламних цілях або передання третім особам. Щоб уникнути не лише незадоволених клієнтів, а й настання правових наслідків компанії повинні володіти юридичними аспектами захисту конфіденційності та безпеки даних під час здійснення електронної комерційної діяльності.

У дослідженні визначено сутність та значення конфіденційності даних у високо конкурентному середовищі ведення бізнесу. Розглянуто необхідність забезпечення відповідності електронної комерції. Деталізовано напрямки впливу конфіденційності даних на бізнес в електронній площині. Структуровано регіональні закони, на основі яких відбувається регулювання захисту даних споживачів товарів та послуг. Згруповано об'єднуючі принципи, які закладені в основу всіх нормативно-правових актів і яких в обов'язковому порядку повинні дотримуватись всі компанії, які працюють з персональними даними. Досліджено сутність політики конфіденційності компанії, визначено її значення та основні елементи. Запропоновано варіанти її розробки. Розкрито необхідність та шляхи забезпечення безпеки даних в електронній комерції.

Ключові слова: відповідність електронній комерції, персоналізації, коефіцієнт конверсії, політика конфіденційності, регіональні закони, персональні дані.

Legal aspects of privacy and data security protection in electronic commerce

Annotation. A wide variety of transactions take place every day in the world of e-commerce, many of which require access to consumer data. However, many users express concerns about providing personal data due to frequent cases of abuse of the received information, its use for advertising purposes or transfer to third parties. In order to avoid not only dissatisfied customers, but also the onset of legal consequences, companies must master the legal aspects of protecting privacy and data security during e-commerce activities.

The study identifies the essence and importance of data privacy in a highly competitive business environment. Considered the need to ensure the compliance of electronic commerce. The areas of impact of data privacy on business in the electronic plane are detailed. The reasons

[1] доктор юридичних наук, професор кафедри готельно-ресторанної справи, Київський університет туризму економіки і права, ORCID: https://orcid.org/0009-0003-0714-236X

for increased pressure and attention to data privacy and security in electronic commerce are determined. The need to switch to first- and zero-party data has been established, discarding data from third parties. Trends in personalization in e-commerce are explored. The value of optimization of the conversion factor is considered. The need to connect and expand customer data on different platforms has been established. Regional laws are structured, on the basis of which regulation of data protection of consumers of goods and services takes place. The unifying principles that form the basis of all legal acts and which must be followed by all companies working with personal data are grouped: legality, fairness and transparency, purpose limitations, data minimization, accuracy, accountability, integrity and confidentiality, storage restrictions. The essence of the company's privacy policy was studied, its meaning and main elements were determined. Variants of its development are proposed. The need and ways to ensure data security in e-commerce are revealed.

Keywords: e-commerce compliance, personalization, conversion rate, privacy policy, regional laws, personal data.

Вступ

Ера цифрових технологій продовжує трансформувати суспільство та економіку, ставлячи перед державою досить складне завдання, пов’язане з адаптацією існуючих правових інструментів до нового сегменту регулювання цієї діяльності. Індустрія цифрових технологій швидко просувається до провідних економічних позицій, зокрема в електронній комерції.

Управління високодохідним інтернет-магазином є привабливою бізнес-моделлю для багатьох компаній сьогодні. Однак, крім зосередження на діяльності, що приносить прибуток, надзвичайно важливо забезпечити відповідність законодавству. Конфіденційність даних є основою цієї відповідності. Без міцної правової основи компанії ризикують зіткнутися з судовим позовом і завдати шкоди своєму авторитету та іміджу. Ситуація набуває особливої актуальності в умовах, коли очікується зростання глобальних роздрібних онлайн продажів до на 39% до 2027 року [1].

Зростання електронної комерції (у такій формі, як ми її частіше знаємо), незважаючи на те, що вона стає все більш зручною як для продавців, так і для клієнтів, також відкриває нові зони ризику для них обох. Майже неможливо завершити транзакцію, не передавши свої особисті дані, і саме з цієї причини конфіденційність даних зараз стала однією з найважливіших і актуальних проблем електронної комерції. Ситуація посилюється в умовах стрімкого поширення правової охорони особистих даних по всьому світу. Так, для прикладу у 2024 році очікується, що 75 відсотків населення світу будуть захищені сучасними правилами конфіденційності даних [2]. Лише у 2023 році в Сполучених Штатах було прийнято п’ять нових законів про конфіденційність даних, а міжнародні органи захисту даних, як-от Національна комісія з інформатики та свободи Франції (CNIL), посилила контроль за дотриманням визначених вимог. Окрім того, компанії повинні боротися не лише з міжнародними законами про конфіденційність, але й з очікуваннями споживачів щодо захисту даних і розумних практик збору даних. На основі вищенаведеного можемо стверджувати про високу актуальність обраного напрямку дослідження.

Враховуючи той факт, що питання захисту конфіденційності та безпеки даних набувають все більшої актуальності з кожним роком, вони притягують фокус уваги багатьох дослідників, науковців та правознавців. Вагомий вклад у розкриття тематики дослідження був здійснений Чучковською А., Наумовим В., Кіліаном В., Подрецьким П., Костовою Н., Гуржієм Т., Петрицьким А., Ярмишем О., Миколенком О., Армашем Н., Олійником О., Барабашиним А., Волинцем В. та ін. Серед зарубіжних фахівців вважаємо

за необхідне виділити напрацювання Herath D., Mazitova L., Cooper T., Socha P., Lubowicka K., Fitria A., Tiwalade A., Ray D., Firat B.та ін.

Зокрема, у роботі Волинця В. розглядаються правові аспекти захисту інтелектуальної власності у сфері цифрових технологій електронної комерції. Herath D., Mazitova L. та Cooper T., здійснюють міркування на тему того, які найважливіші моменти конфіденційності необхідно враховувати компаніям, які працюють у сфері електронної комерції. Дане дослідження охоплює розгляд особливостей збору даних та отримання згоди на їх опрацювання від користувачів, порядок забезпечення безпеки даних і шифрування, зберігання та видалення даних, обмін та їх передача тощо [3].

Tiwalade A., Ray D., та Firat B. досліджували конфіденційність і захист даних в електронній комерції розвинутих країнах крізь призму оцінки різних підходів до захисту даних [4].

Проте, не применшуючи вклад зазначених авторів, динамічність процесів, пов'язаних із захистом конфіденційності даних, яка відстежується протягом останніх декількох років формує собою поле для подальших розвідок.

Метою даної статті є дослідити юридичні аспекти захисту конфіденційності та безпеки даних під час ведення діяльності в онлайн середовищі.

Завдання статті містять:

- визначення взаємовпливу конфіденційності даних та електронної комерції;
- виокремлення шляхів акумуляції особистих даних;
- систематизація регіональних законів щодо захисту конфіденційності даних;
- узагальнення принципів, якими повинні керуватись компанії при роботі з конфіденційними даними;
- представлення ефективних шляхів забезпечення високого ступеня безпеки даних в електронній комерції.

Матеріали та методи.

Для дослідження використано такі матеріали:

1) нормативно-правові акти, що регулюють захист конфіденційності та безпеки даних в електронній комерції;
2) науково-практичні праці вітчизняних та зарубіжних авторів, які досліджують питання захисту конфіденційності та безпеки даних в електронній комерції.

У ході дослідження використовувалися такі методи: формально-правовий та порівняльно-правовий, що дозволило визначити аналізувати національне та міжнародне законодавство у сфері захисту конфіденційності та безпеки даних; формально-логічний метод застосовано для з'ясування змісту правових норм та аналізу інструментів, передбачених для захисту даних споживачів; функціонально-інструментальний метод, передбачений для виявлення особливостей забезпечення охорони, що досліджується; діалектичний метод сприяв дослідженню правового забезпечення охорони конфіденційності даних

Результати

Конфіденційність є ключовим аспектом електронної комерції, оскільки вона впливає як на довіру, так і на відповідність нормам діючого законодавства в країні, де провадиться онлайн-бізнес. Клієнти очікують від бізнесу захисту їхніх особистих і фінансових даних, тоді як регулятори встановлюють суворі правила та штрафи за витік та поширення таких даних. Так, більшість дослідників та соціологів сходять на думці, що безпека даних перетворюється на той фактор, який може або простимулювати або стримати здійснення покупки. Позитивний аспект цього полягає в тому, щодо дотримання вимог щодо конфіденційності даних електронної комерції підвищує

довгострокову взаємодію з клієнтами та відкриває можливості до зростання доходів від електронної комерції.

У даному контексті важливого значення набуває дотримання відповідності електронної комерції. Дана відповідність охоплює різноманітні правові та нормативні вимоги, яких мають дотримуватися онлайн-бізнеси. Це стосується захисту даних споживачів, прав споживачів і фінансових операцій. Ці вимоги захищають споживачів і гарантують, що компанії електронної комерції ведуть бізнес етично, безпечно та відповідно до місцевих і міжнародних законів. Це може включати дотримання стандартів конфіденційності даних, таких як GDPR (General Data Protection Regulation)в Європейському Союзі, забезпечення безпечної обробки платежів і чітке відображення контактної інформації та політики повернення на вебсайті.

Розглянемо 5 напрямків впливу конфіденційності даних на електронну комерцію (рис. 1):

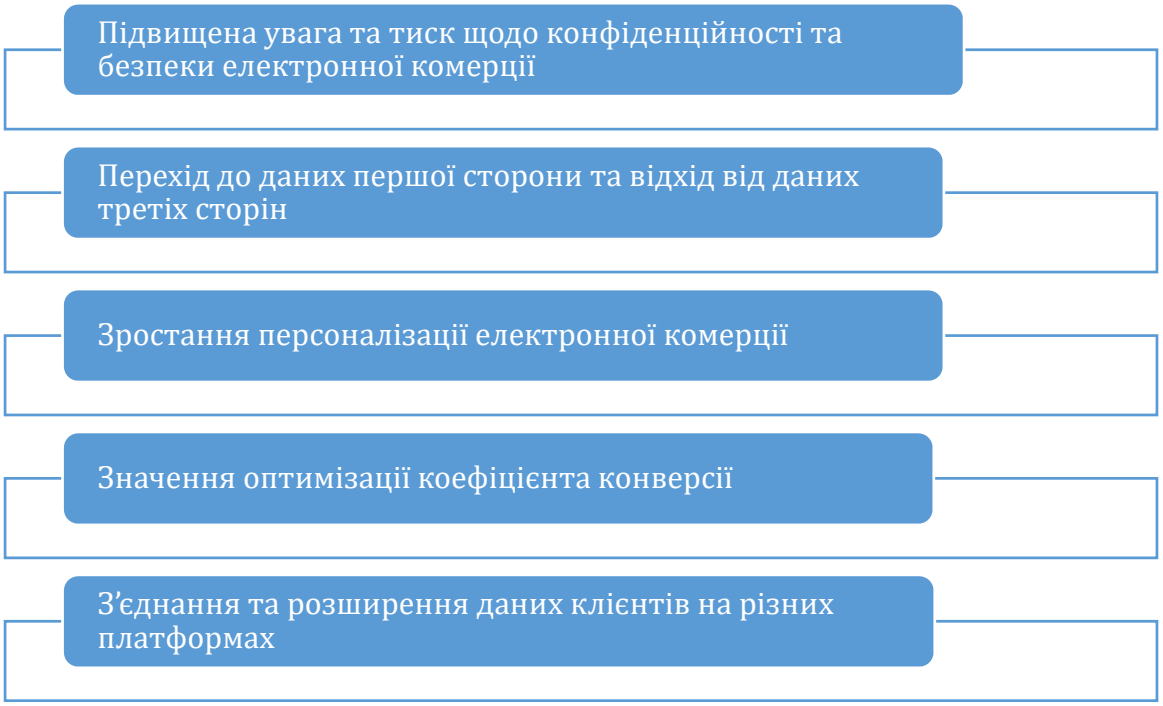

Рис.1. Напрямки впливу конфіденційності даних на електронну комерцію
Джерело: розроблено автором на основі [1]

Розглянемо дані напрямки детальніше. Розгул кіберзлочинності посилив стурбованість споживачів щодо безпеки та конфіденційності їхньої діяльності та даних в Інтернеті, особливо під час покупок. Таким чином, вони очікують, що компанії забезпечуватимуть безпеку своїх вебсайтів, програм і операцій електронної комерції.

Звіт про прозорість (Pwc) за 2022 рік представляє наступну статистику, спів ставну до вищезазначеного [5]:

- 71% споживачів не будуть купувати в компанії, якій не довіряють;
- 73% клієнтів не рекомендуватимуть сайт електронної комерції своїм друзям, якщо вони відчуватимуть, що покупка на ньому не є безпечною.
- лише 30% споживачів стверджують, що мають високий рівень довіри до онлайн-компаній, з якими вони співпрацюють.

Це підтверджує той факт, що споживачі все більш чутливі до заходів безпеки, збору даних і конфіденційності, які вживаються онлайн-бізнесом. На цю спрямованість і тиск слід відповідати реальними діями, які потім можна повідомити відвідувачам сайту, щоб завоювати їх довіру.

Галузь електронної комерції спостерігає серйозні зміни в типі та джерелі індивідуальних даних, на які покладаються компанії, від даних третіх сторін до даних першої чи нульової сторони.

Дані третіх сторін збираються опосередковано, від рекламодавців та інших джерел. Дані третіх сторін часто включають демографічну інформацію, сигнали купівлі та дані про поведінку, які одержані з інструментів відстеження.

Проте такі дані несуть в собі ряд недоліків:

- вони не стосуються взаємодії конкретно з однією компанією;
- щоб дані несли в собі аналітичну цінність вони повинні бути зіставлені з іншими даними першої та третьої сторони.

Іноді дані з різних джерел поєднуються, що дозволяє суттєво усунути зазначені недоліки. Через це галузь електронної комерції все більше зміщується в бік до нульових даних. Це пов’язано із тим, що дані нульової сторони надходять безпосередньо від клієнтів, які навмисно діляться своєю особистою інформацією. Отримана інформація стосується їхніх виражених інтересів і вподобань. Це відповідає вимогам щодо дійсної згоди відповідно до законів про конфіденційність, як-от GDPR.

Дані першої сторони, з іншого боку, збираються компаніями на основі веб дій клієнтів і відвідувачів на каналах компанії – за допомогою файлів cookie браузера та інших технологій відстеження. Ці дії включають перегляд електронної комерції, покупки та будь-які інші форми взаємодії на сайті чи додатку. Отримані дані можуть включати IP-адреси, шаблони навігації, уподобання щодо покупок, час, проведений на сторінці або на сайті, і багато іншого.

Персоналізація також є ключем до зміни стратегії даних. Повідомляється, що 70% споживачів зараз очікують персоналізованого досвіду та розчаровуються, якщо вони його не отримують. Застосовуючи найкращі методи персоналізації, необхідно централізувати свої дані на платформі керування параметрами (PMP). Це дасть змогу збирати, зберігати та активувати дані, гармонійно використовуючи інструменти та системи, та максимізувати їх цінність. У поєднанні з керуванням згодою ці дані потім використовуються відповідно до виражених уподобань клієнта щодо згоди.

Компанії сьогодні повинні докладати значних зусиль, щоб задовольнити зростаючі очікування щодо конфіденційності даних електронної комерції, побудувати та зберегти довіру, а також забезпечити чудовий персоналізований досвід. Згода на оброку персональних даних є основою, яка робить це можливим. Це гарантує дотримання індивідуальних уподобань, надаючи клієнтам контроль, свободу вибору та персоналізований досвід, який вони очікують отримати.

Ще у 2020 році компанія McKinsey виявила, що 76% споживачів змінили магазини, бренди або канали, оскільки лояльність до бренду послабилася; хоча через пандемію витрати на електронну комерцію зросли.Підприємства електронної комерції не можуть розраховувати або покладатися на лояльність до бренду. Однак персоналізація – особливо якщо вона підтримується даними – може бути потужним інструментом для посилення лояльності до бренду та зв’язку. Але на той момент лише 15% роздрібних продавців запровадили персоналізацію в усіх каналах – попри визнану її цінність, яку визначили як пріоритет майже дві третини опитаних компаній (64%).

У 2024 році вже 85% компаній використовують персоналізацію. А світова ринкова вартість програмного забезпечення для персоналізації, за прогнозами, досягне 943 мільйонів доларів до кінця цього року [6]. Ключем до цього буму персоналізації є

розширення доступу до особистої інформації, яка дає знання, необхідні для здійснення індивідуальних покупок. Водночас зазначені тенденції викликають декілька важливих запитань:

1. Як компанії підтримують конфіденційність даних електронної комерції одночасно керуючи вподобаннями клієнтів на різних платформах?
2. Чи забезпечується конфіденційність даних клієнтів і усуваються проблеми щодо конфіденційності.
3. Чи відповідально використовуються інструменти штучного інтелекту для забезпечення конфіденційності?
4. Які заходи вживаються, щоб гарантувати дотримання правил конфіденційності?
5. Чи отримується згода клієнтів, особливо у випадках коли дані обмінюються або передаються між інструментами та системами?

Оптимізація коефіцієнта конверсії (CRO) – ще одна важлива практика електронної комерції, на яку сильно впливає зміна ставлення до конфіденційності даних. Щоб надати потенційним клієнтам і клієнтам, які повертаються, найкращий досвід, компанії електронної комерції використовують дані про поведінку, щоб задовольнити їхні потреби та вподобання. Таким чином, керування перевагами – і його різноманітні наслідки для збору та використання особистої інформації – має вирішальне значення для оптимізації переходів, утримання клієнтів і збільшення витрат. Ось дії CRO, які відповідають найкращим практикам конфіденційності даних:

нотування конкретних комунікаційних вподобань, для зв'язку з відвідувачами та клієнтами лише тоді, коли вони з найбільшою ймовірністю цього потребують;

надання відвідувачам індивідуальних пропозицій щодо продуктів, які їх цікавлять;

формування спеціальних пропозицій на критичних етапах шляху покупця, щоб забезпечити отримання даних нульової сторони та запобігти відмові від покупки;

забезпечення онлайн інтерфейсу, який відображає вибір клієнта щодо згоди на використання даних;

Внаслідок виконання зазначених дій компанії мають можливість продемонструвати повагу до конфіденційності в електронній комерції, одночасно створюючи безперебійний досвід роботи з клієнтами та збільшуючи коефіцієнти конверсії.

Водночас, компанії які працюють в середовищі електронної комерції повинні орієнтуватися в складному ландшафті законів про конфіденційність даних залежно від того, звідки походять їхні клієнти. Ці регіональні закони включають (табл. 1):

Таблиця 1

Регіональні закони про захист конфіденційності даних

Назва закону	Напрямок регулювання
Закон про цифрові ринки (DMA)	націлений на великі онлайн-платформи, що працюють у ЄС, щоб забезпечити чесну конкуренцію
Загальний регламент захисту даних (GDPR)	золотий стандарт законодавства про захист даних, який встановлює суворі правила, що стосуються будь-якого бізнесу з клієнтами з ЄС.
Закон Каліфорнії про конфіденційність споживачів (CCPA):	дає жителям Каліфорнії право знати, які особисті дані збираються, і вимагати їх видалення.
Закон Вірджинії про захист даних споживачів (VCDPA)	дозволяє жителям Вірджинії відмовитися від обробки даних для цільової реклами та продажів
Lei Geral de Proteção de Dados (LGPD)	закон Бразилії, який регулює використання персональних даних.

Закон про захист особистої інформації (POPIA)	закон Південної Африки, який захищає особисту інформацію, регулюючи способи її обробки
Федеральний закон про захист даних (FADP)	закон Швейцарії про конфіденційність даних, який вимагає прозорості та законної основи для обробки персональних даних
ЄС–США Конфіденційність даних	ця міжнародна система охоплює обмін персональними даними між країнами ЄС і США, гарантуючи певні заходи
Закону про захист конфіденційності дітей в Інтернеті (COPPA)	даний закон передбачає, що для контенту, призначеного для дітей, певні функції можуть бути вимкнені чи обмежені.

Джерело: розроблено автором на основі [7]

Більшість законів про конфіденційність у всьому світі базується на GDPR ЄС, яке стало першим всеосяжним оновленням законодавства щодо конфіденційності даних з 2000 року. GDPR є нормативним актом, який базується на правах, а це означає, що він побудований навколо концепції, згідно з якою люди мають право контролювати, хто має доступ до власної особистої інформації та способів використання цієї інформації.

Завдяки такому підходу, заснованому на правах, GDPR і наступні закони в усьому світі відображають сім ключових принципів, яких повинні дотримуватися компанії (рис. 2):

Рис. 2. Принципи, яких повинні дотримуватись компанії при роботі з персональними даними

Джерело: розроблено автором на основі [8]

1. Законність, справедливість і прозорість: компанії повинні діяти чесно та відповідно до закону, а також повинні повідомляти споживачам, які саме типи

інформації збираються, навіщо вони потрібні, як вони використовуються, з ким вони передаються, як вони захищені. , і як довго вони зберігаються.

2. Обмеження за призначенням: компанії можуть використовувати зібрані дані лише для первинно заявленої мети й відповідно не можуть використовувати цю інформацію для нових напрямків без отримання на це відповідної згоди суб'єктів.
3. Мінімізація даних. Компанії повинні збирати якомога меншу кількість даних для своїх заявлених цілей і не можуть збирати додаткову інформацію на випадок, якщо вона стане в нагоді пізніше.
4. Точність: компаніями повинна підтримуватись точність і актуальність персональних даних.
5. Обмеження щодо зберігання: можна зберігати дані, що ідентифікують особу, лише до того моменту, поки вони використовуються. В іншому випадку всю непотрібну інформацію слід видалити.
6. Цілісність і конфіденційність: компанії повинні вживати відповідних заходів безпеки, цілісності та конфіденційності, щоб захистити інформацію споживача від розголошення.
7. Підзвітність: компанія повинна бути здатною підтвердити відповідність GDPR усім цим принципам. В іншому випадку на неї можуть накласти штрафи, судові заборони та інші покарання.

Попри те, що всі зазначені нормативні акти відрізняються, більшість із них також наголошує на наступних моментах: контролі споживачів, наприклад, на можливості споживачів виправляти чи видаляти особисту інформацію з бази даних або відмовлятися від продажу, поширення чи використання їхньої інформації в маркетингових цілях.

Крім того, майже всі зазначені закони надають споживачам право подавати суб'єкту персональних даних запит на доступ для перегляду всіх даних, про нього, якими він володіє. Окрім того, даними законами гарантується право споживачів на видалення таких даних на їх вимогу.

Для того, щоб забезпечити своє функціонування у рамках правового поля суб'єкти господарювання зобов'язані зазначати на сайтах, через які здійснюється продаж інформацію про їхню політику конфіденційності. Політика конфіденційності містить в собі дані про те, яка дані споживачів збираються компанією, чому вони збираються, яким чином вони зберігаються та як надається доступ до них третім особам. Для забезпечення дотримання вищезгаданих нормативно правових актів компанії, які працюють в середовищі електронної комерції можуть використовувати такі інструменти як банери файлів cookie, форми згоди та центри налаштувань.

Як показує досвід політика конфіденційності електронної комерції – це не просто формальність – це важлива частина будь-якого успішного онлайн-бізнесу. Ось кілька причин, чому це так:

- у багатьох регіонах законодавство вимагає наявність політики конфіденційності для будь-якої компанії, яка збирає особисті дані;
- чітка політика конфіденційності демонструє прозорість, створює міцну репутацію та зміцнює довіру клієнтів;
- багато платформ електронної комерції, як-от Shopify і Woocommerce, вимагають політики конфіденційності для використання їхніх послуг;
- надійна політика конфіденційності захищає від потенційних судових суперечок, пов'язаних із конфіденційністю даних клієнтів.

Хоча кожна компанія унікальна, дане твердження дуже рідко використовується коли мова іде про її політику конфіденційності. Будучи юридичними суб'єктами, вони повинні охоплювати всі аспекти акумуляції, використання та зберігання даних, щоб

користувачі могли надати інформовану згоду. Ось основні елементи, які слід включити в політику конфіденційності електронної комерції:

1. Які файли cookie та технології відстеження використовуються, їх призначення та як користувачі можуть ними керувати.
2. Як використовується аналітика та які дані збираються у файлах журналу.
3. Як збираються дані для реклами та як інформація про користувачів може використовуватися для показу цільової реклами.
4. Які сторонні служби мають доступ до даних користувачів і з яких причин.
5. Як дані користувача використовуються в маркетингових цілях і як користувачі можуть відмовитися.
6. Як обробляється та поширюється створений користувачами вміст, а також права, які користувачі мають на їхній вміст.
7. Шляхи керування конфіденційністю та згодою дітей, зокрема дотриманням відповідних законів, як-от Закону про захист конфіденційності дітей в Інтернеті (COPPA).
8. Застереження щодо будь-яких зовнішніх посилань на вебсайти та відсутності контролю над їх практикою конфіденційності.

Враховуючи необхідність врахування зазначених аспектів при розробці політики конфіденційності компанії можуть стикнутись зі значними труднощами. Для їх уникнення можна скористатись послугами адвоката. Експерт із законодавства про конфіденційність, який розуміє нюанси бізнесу конкретної компанії, часто є найкращим вибором. Юристи, які регулярно працюють із питаннями конфіденційності та повністю розуміють правові наслідки захисту даних, можуть надати хороші юридичні поради та створити ефективний правовий документ.

Окрім того, є варіант використання онлайн генератора політики конфіденційності та використання DIY шаблонів. Останні втілюються у наявності на просторах Інтернету стандартних шаблонів політики конфіденційності, які дозволяють її розробити на основі певних параметрів. Звичайно такий варіант є набагато дешевшим, проте використання шаблонів та генераторів загрожує компаніям залишити поза полем зору деякі аспекти їх діяльності, а отже не може повністю усунути загрозу настання правових наслідків за захист конфіденційності даних споживачів.

В умовах стрімкого зростання кількості кіберзлочинів зростає актуальність забезпечення безпеки даних, одержаних в ході електронної комерційної діяльності. Це передбачає використання надійних заходів безпеки для захисту комп'ютерних систем від хакерів: брандмауерів, антивірусного програмного забезпечення та систем виявлення вторгнень.

Окрім того, важливим є навчання співробітників конфіденційності даних. Вони повинні володіти знаннями про ризики витоку даних, фішингу та зловмисного програмного забезпечення. Співробітники також повинні знати як виявляти підозрілу діяльність та повідомляти про неї. Ще одним інструментом захисту даних є розглянута нами вище політика конфіденційності.

Окрім кроків, перелічених вище, компанії електронної комерції також можуть вжити таких заходів для захисту конфіденційності даних своїх клієнтів: шифрування конфіденційних даних, використання надійних паролів, обережність при наданні своїх даних в інтернеті та відстеження останніх випадків шахрайства.

Конфіденційні дані, наприклад номери кредитних карток, повинні бути зашифровані, коли вони зберігаються в комп'ютерних системах або передаються через Інтернет. Співробітники та клієнти повинні використовувати надійні паролі для своїх облікових записів електронної комерції. Надійні паролі мають містити принаймні вісім символів і містити поєднання великих і малих літер, цифр і символів. Крім того, клієнти

повинні бути обережними з інформацією, яку вони публікують в Інтернеті, особливо в соціальних мережах. Надаючи занадто багато особистої інформації, хакерам буде легше атакувати їх. Хакери завжди винаходять нові способи викрадення даних. Клієнти повинні бути в курсі останніх випадків шахрайства та бути обережними, натискаючи посилання або відкриваючи вкладення від невідомих відправників [9].

Висновки

В ході дослідження встановлено, що успішність бізнесу електронної комерції та доступ до конфіденційних даних є тісно взаємопов'язаними поняттями. Саме тому, компанії докладають все більше зусиль для отримання доступу до таких даних. При цьому критичної важливості досягає вимога забезпечення захисту конфіденційності та безпеки даних. У відповідь на загрози витоку останніх та зростаючий попит на захист даних з боку споживачів зростає щільність правового покриття даного напрямку. Відтак, при здійсненні своєї діяльності компанії повинні враховувати законодавство щодо конфіденційності даних у країні розташування покупця. Охопити весь спектр міжнародних законів, звісно, дуже важко. Тому при організації роботи з конфіденційними даними необхідно керуватись такими принципами: підзвітність, точність, цілісність і конфіденційність, обмеження щодо зберігання, законність, справедливість, прозорість, обмеження щодо призначення та мінімізація даних.

На щастя, конфіденційність даних все більше стає конкурентною перевагою. Прозорість для споживачів є виграшною маркетинговою стратегією, особливо в поєднанні з персоналізацією. Більшість споживачів готові ділитися своєю особистою інформацією, але лише якщо вони вірять, що вона безпечно зберігатиметься, використовуватиметься лише для цілей, на які вони погодилися, і надасть їм ті переваги, які вони хочуть. Відтак, продавцям необхідно переконати споживачів, що їхні дані будуть у безпеці. Вагомим інструментом на шляху до цього є розробка політики конфіденційності.

З іншого боку, для того, щоб бути успішними сьогодні – компаніям необхідно не лише ефективно акумулювати конфіденційні дані, а й забезпечувати високий рівень їх безпеки через використання таких інструментів як брандмауерів, антивірусного програмного забезпечення та систем виявлення вторгнень.

Таким чином дослідження показало, що юридичних аспектів щодо захисту конфіденційності та безпеки даних є дуже багато, але лише їх неухильне дотримання дозволить суб'єктами залишатись конкурентними в агресивному середовищі Інтернет бізнесу, а також захистить останніх від фінансових, адміністративних та кримінальних санкцій.

Список використаних джерел

1. Ecommerce privacy compliance and effects of data privacy. usercentrics. 2024. URL: https://usercentrics.com/knowledge-hub/five-ways-data-privacy-is-shaping-ecommerce/
2. Protect Your Customers and Business with an Ecommerce Privacy Policy. Big Commerce. n.d. URL: https://www.bigcommerce.com/articles/ecommerce/privacy-policy/
3. Herath D., Mazitova L. and Cooper T. What are the most important privacy considerations for E-Commerce businesses? Liked In. 2024. URL: https://www.linkedin.com/advice/0/what-most-important-privacy-considerations-e-commerce-zlgme
4. Tiwalade A., Ray D., Firat B. Privacy and Data Protection in E-commerce in Developing Nations: Evaluation of Different Data Protection Approaches. Core. 2021. URL: https://core.ac.uk/download/pdf/288375411.pdf

5. Pwc Global Annual Review 2022. Pwc. 2023. URL: https://www.pwc.com/gx/en/global-annual-review/2022/PwC_Global_Annual_Review_2022.pdf
6. Arthur. Data privacy for Online Stores: What You Need to Know. heydata. 2024. URL: https://heydata.eu/en/magazine/data-privacy-online-stores-essential-guide.
7. Global Data Privacy Laws. aosphere. n.d. URL: https://www.aosphere.com/aos/dp?gad_source=1&gclid=CjwKCAjw26KxBhBDEiwAu6KXt44IuCnsx5Kr76c5HABOMeJPXdxwFWLzrsSmVcvpyUWkmnzsqaC7XRoCQFIQAvD_BwE
8. E-commerce Data Privacy: What You Need To Know. Redclover. 2023. URL: https://redcloveradvisors.com/2023/05/30/e-commerce-data-privacy-what-you-need-to-know/
9. Mirza Hadi Baig. Data Privacy Issues in E-Commerce. LikedIn. 2023. URL: https://www.linkedin.com/pulse/data-privacy-issues-e-commerce-mirza-hadi-baig