*Климанський В. І.  
 здобувач вищої освіти ступеня доктора філософії  
 Державний торговельно-економічний університет, Україна*

**ЗАХИЩЕНІСТЬ ПЕРСОНАЛЬНИХ ДАНИХ ФІЗИЧНИХ ОСІБ ЯК ФАКТОР НАЦІОНАЛЬНОЇ БЕЗПЕКИ**

Захист персональних даних клієнтів став викликом для бізнесу в умовах війни, адже компанії зіштовхуються з постійними кібератаками з боку держави-агресора, спрямованими на викрадення інформації про клієнтів.

Однією з найбільших кібер загроз для населення залишається "фішинг", за допомогою якого злочинці можуть отримати несанкціонований до персональних даних, таких як контактні дані, банківські рахунки та інша чутлива інформація.

Згідно даних сервісу opendatabot - кожен дев'ятий опитаний українець ставав жертвою шахраїв від початку повномасштабного вторгнення. У результаті опитування було виявлено, що 11% українців стали жертвою шахраїв від початку повномасштабного вторгнення. При чому на долю покупки/продажу товару в інтернеті припадає 52.7% всіх шахрайств, а на шахрайські посилання ще 18.6%. ще 12% припадає на злами приватних соціальних мереж. [1] Для порівняння, за вісім місяців 2023 року в Україні було відкрито майже 60 тисяч проваджень про шахрайство за ст.190 ККУ. Це більше, ніж навіть загалом за два попередні 2 роки: так, у 2021 було відкрито 23,8 тисяч проваджень, а у 2022 — 32 тисячі. [2]

Одним з прикладів ІТ-ініціативи на рівні держави є платформа "Дія", яка стала одним з основних засобів доступу до державних послуг. Використовуючи систему "Дія", громадяни можуть отримувати різноманітні сервіси, що значно скорочує потребу в фізичному контакті з урядовими установами, що особливо актуально під час війни. Це знижує ризики атак на фізичну інфраструктуру, але в той же час може сприяти підвищенню ризиків національного суверенітету в інформаційному просторі. Ще до початку повномасштабного вторгнення РФ в Україну, портал "Дія" було неодноразово атакован хакерами, і хоча офіційні особи заявляють що особисті дані не були втрачені, багато українців підозрювали саме нещодавню атаку на сервій як причина витоку персональних даних [3].

Отже система надання послуг не може бути на 100% захищена і гарантувати абсолютну захищеність персональних даних. Це доводить, до саме під час великих соціальних зрушень та загроз, таких як національна війна, зростають кібер ризики і питання кібербезпеки на даний час є як ніколи актуальним.

Але тим паче кібербезпека є актуальна для електронної комерції та інших онлайн майданчиків надання послуг

Забезпечення безпеки платіжної інформації стає пріоритетом для банків, платіжних систем та інтернет-магазинів. Для боротьби з такими загрозами компанії впроваджують сучасні системи кіберзахисту, включаючи автоматизовані системи відстеження аномалій, біометричні методи аутентифікації та блокчейн-рішення для підвищення безпеки транзакцій [4].

Найбільші онлайн постачальники цифрових продуктів для створення власних інтернет-магазинів такі як Shopify найголовнішими кібер-загрозами для діяльності електронної комерції визначають DDoS атаки, витоки персональних даних, платіжне шахрайство, шкідливе програмне забезпечення, яке може бути встановлене несанкціоновано та програми-вимагач, загрози злому доступу до адміністративних налаштувань веб-сайтів та основного коду тощо [5]. При чому це не весь список потенційних загроз, з якими можуть зіткнутися веб сайт електронної комерції.

Бізнесам, які оперують в сфері електронної торгівлі, варто серйозно сприймати загрозу кібершахрайства та більше ресурсів приділяти власній інтернет безпеці та безпеці персональних даних користувачів, які можуть бути доступними бізнесу за-для обробки замовлень товарів або послуг. З огляду на масштаб проблеми та загрози масових втрат персональних даних фізичних осіб, зниження рівня діяльності чи повна зупинка такої серед приватних бізнесів чи державних установ, підвищення рівня кібербезпеки в умовах ведення повномасштабної війни стає критично важливим для України та напряму стосуються національної безпеки країни.

Звичайно, кібербезпека державних організацій, каналів передачі інформації, зв’язку військових, фінансових та енергетичних об’єктів є критично пріоритетною в сучасних умовах. Першочергова ціль існування держави як соціального та політичного утворення полягає в забезпеченні безпечної життєдіяльності її громадян. Тож втручання у кіберсферу суверенної країни і перешкоджання діяльності приватних компаній та життя і комфорту громадян варто розглядати як чергову загрозу безпеці та втручанням в національні інтереси суверенної держави.

Список використаних джерел:

1. Кожен дев'ятий опитаний українець ставав жертвою шахраїв від початку повномасштабного вторгнення. Сервіс статистики opendatabot : веб-сайт. URL:<https://opendatabot.ua/analytics/stopfraud-nbu>
2. Кількість справ про шахрайство у 2023 році сягнула історичного антирекорду. Сервіс статистики opendatabot : веб-сайт. URL: <https://opendatabot.ua/analytics/fraud-pandemic-2>
3. З «Дії» чи ні? Звідки хакери взяли персональні дані 2 млн українців. Розслідування DOU. DOU : веб-сайт. URL: <https://dou.ua/lenta/articles/inquiry-about-diia-data-leak/>
4. Ковальчук В. П. "Захист персональних даних у бізнесі: виклики та рішення." *Журнал корпоративної безпеки*, 2023, № 3, с. 59–74.
5. How To Improve Ecommerce Security for Your Online Store. Shopify Blog. URL: <https://www.shopify.com/blog/ecommerce-security>