УДК 004.738.5:339]:004.056

ДОСЛІДЖЕННЯ ЗАСОБІВ БЕЗПЕКИ В СИСТЕМАХ ЕЛЕКТРОННОЇ КОМЕРЦІЇ

Карабанов Д.С., Чеботарьова Д.В.
Науковий керівник – проф. Безрук В.М.
Харківський національний університет радіоелектроніки, каф. ІМІ,
м. Харків, Україна
e-mail: denys.karabanov@nure.ua
e-mail: dariia.chebotarova@nure.ua

The work is devoted to the research of current problems of information security and the analysis of modern security tools in electronic commerce systems. Recently, the number of cyber-attacks and fraud in e-commerce systems has increased significantly. A comprehensive approach to solving information security problems, including the use of modern software and technical tools, improvement of regulatory and legal support, implementation of certain organizational measures, will allow to achieve effective results in the field of protection of electronic commerce systems.

В усьому світі швидкими темпами зростають масштаби впровадження та використання систем електронної комерції. Сьогодні ринок електронної комерції величезний і постійно змінюється. Великим поштовхом для повсюдного використання електронної комерції стала пандемія covid-19, що призвела до суттєвого збільшення онлайн покупок та цифрових фінансових послуг під час карантинних обмежень. За цей час компанії і користувачі відчули всі переваги електронної комерції, тому тепер її використання тільки зростає. Навіть в Україні, незважаючи на війну, ринок електронної комерції продовжує зростати.

Електронна комерція та цифрові фінансові послуги демонструють значні переваги: зручність, суттєва економія часу, новий рівень ефективності та прозорості, автоматизація процесів, зменшення кількості помилок, покращення обслуговування клієнтів, зниження витрат на організацію та підтримку бізнесу, спрощення розширення бізнесу та виходу на міжнародні ринки та багато інших. Серед недоліків найважливіше місце посідає проблема безпеки конфіденційних даних та фінансових операцій. Зі зростанням обсягів електронної комерції збільшується кількість кібератак, шахрайства, фінансових втрат та витоків даних.

Основними кіберзагрозами для електронної комерції є фішинг, malware- та ransomware-атаки, SQL-ін’єкції, DDoS та брутфорс-атаки, спрямовані на злам доступу до облікових записів [1]. Крім того, зловмисники постійно використовують нові технології та вдосконалюють свої методи. Саме тому питання безпеки є надзвичайно актуальними та потребує досліджень та розробки нових засобів безпеки. Забезпечення

безпеки електронної комерції є важливим для підтримки довіри клієнтів, мінімізації фінансових втрат та дотримання відповідних норм і галузевих стандартів [2].

Метою доповіді є дослідження актуальних проблем інформаційної безпеки та аналіз сучасних засобів безпеки в системах електронної комерції. В роботі детально проаналізовано проблеми безпеки (вразливості, загрози, атаки) та різні засоби (методи, інструменти, програми) захисту систем електронної комерції.

В системах електронної комерції важливо захищати дані всіх користувачів та гарантувати безпеку всіх транзакцій, особливо фінансових. Тому надійний захист систем електронної комерції вимагає побудови концепції безпеки на основі багатогранного та комплексного підходу. Значно підвищити безпеку мережі та знизити ризики кібератак допоможе впровадження та використання таких засобів: управляння доступом та багатофакторна автентифікація; шифрування SSL; брандмауери веб-додатків; рішення для захисту від DDoS-атак; вдосконалена аналітика та алгоритми машинного навчання для виявлення підозрілих моделей і поведінки, які можуть свідчити про шахрайство; аналітика ризиків даних; оцінка вразливостей та тестування на проникнення; постійні оновлення безпеки та регулярні виправлення; неперервне навчання співробітників; моніторинг мережі та виявлення вторгнень, використання протоколів захищеного обміну інформацією та безпечних електронних транзакцій тощо.

Комплексний підхід до вирішення проблем безпеки інформації, зокрема використання сучасних засобів програмно-технічного характеру, удосконалення нормативно-правового забезпечення, вжиття актуальних організаційних заходів, дозволить досягнути ефективних результатів у сфері захисту інформації та фінансових транзакцій в системах електронної комерції.

Забезпечення надійної безпеки мережі для електронної комерції є першорядним. Кіберзагрози постійно розвиваються, кількість атак збільшується, тому фінансовим установам і окремим користувачам вкрай важливо застосовувати найкращі методи захисту конфіденційних та фінансових даних.

Список використаних джерел:

1. Липська В. 10 головних челенджів для електронної комерції у 2024 році [Електронний ресурс] / В. Липська // Wezom. – 2024. – Режим доступу до ресурсу: https://wezom.com.ua/ua/blog/10-golovnih-chelendzhiv-dlya-elektronnoyi-komertsiyi-u-2024-rotsi.

2. Payment security: An in-depth, actionable guide for businesses [Електронний ресурс] // Stripe. – 2023. – Режим доступу до ресурсу: https://stripe.com/resources/more/payment-security.