MPLD3 is used to display matplotlib generated figures to templates.

The web application is currently going to provide quick access to HRV data and computation methods but with the emergence of machine learning, the app platform will surely include use case of machine learning techniques for a deep analysis of the HRV correlation to stress.

1. Bulletin de l'Académie Nationale de Médecine Volume 197, Issue 1, January 2013, Pages 175-186

2. Afonsocraposo. BioSPPy - Biosignal Processing in Python [Електронний ресурс] / Afonsocraposo. – 2021. – Режим доступу до ресурсу: https://github.com/PIA-Group/BioSPPy.

3. https://www.scipy.org/ [Електронний ресурс] // 2021 – Режим доступу до ресурсу: https://www.scipy.org/.

4. NOnLinear measures for Dynamical Systems (nolds) [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://github.com/CSchoel/nolds.

УДК 004.418

Тригубець Б. - аспірант
Тернопільський національний технічний університет імені Івана Пулюя

ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ В ЕЛЕКТРОННІЙ КОМЕРЦІЇ

Науковий керівник: к.т.н., доцент Загородна Н. В.

Tryhubets B.
Ternopil Ivan Puluj National Technical University

INFORMATION SECURITY TECHNOLOGIES IN E-COMMERCE

Supervisor: Zahorodna N. V.

Ключові слова: електронна комерція, захист інформації, інтернет-магазини
Keywords: e-commerce, data protection online shopping

З кожним роком інформаційні технології все глибше інтегровуються в життя кожного користувача інтернету. Цей вплив замітний всюди: в онлайн-ЗМІ, онлайн-навчанні, онлайн-покупках. Останній напрямок розвивається найстрімкіше. Причина його розвитку проста — через веб-сайти та мобільні додатки бізнес отримує найкоротший шлях до кінцевого споживача. На нього не впливають карантинні обмеження, актуальні у 2021 році, не впливає віддаленість кінцевого споживача до фізичного місця перебування власника бізнесу та його товарів [1]. Тому з кожним роком на ринку з'являється все більше компаній, які надають свої послуги лише в онлайн-форматі [2]. Саме цю сферу і називають електронною комерцією.

Проте одночасно з розвитком та спрощенням взаємодії користувача з процесом купівлі товарів виникає інша проблема — безпека користувача та інтернет-магазину під час цих покупок. Злоумисники розвивають свої інструменти паралельно з розвитком індустрії, а тому перед компаніями стоїть задача надавати не лише зручні, але й безпечні послуги.

Адже на відміну від звичайних інформаційних сайтів, інтернет-магазини та мобільні додатки, пов’язані з онлайн-продажами, володіють набагато детальнішою

інформацією про користувача, мають його платіжні дані, а будь-яке несанкціоноване вторгнення може призвести до втрати цієї фінансової інформації, її секретності, і як наслідок – використання цієї інформації зловмисником в корисливих цілях [3].

Тому онлайн-підприємства повинні ретельно захищати свої активи від випадкового чи злочинного внутрішнього та зовнішнього їх неправильного використання. Інформація клієнта також повинна бути захищена, а підприємству необхідно бути готовим до того, що використання пластикових карт клієнтами в якості основного платіжного інструменту провокує спроби різного роду комп'ютерних злочинів.

Основними видами шахрайських дій зловмисників на ресурсах такого типу це придбання товарів і послуг за реквізитами скомпрометованих кредитних карток (у деяких випадках за допомогою спеціальних ботів, розпізнавання яких також є одним з методів захисту) та злам баз даних, що містять інформацію з пластикових карт, якими оплачували у даному інтернет-магазині (в окремих випадках причиною цього є людський фактор).

Відповідно до цих вразливостей можна виділити два складові елементи захисту електронного бізнесу:

- програмний захист інформації, призначений для захисту цінної інформації, що обробляється і зберігається на комп'ютерах та серверах інтернет-магазину, методи, які дозволяють ресурсу безперебійно функціонувати та надавати послуги клієнтам, незважаючи на зовнішні атаки (для прикладу DDoS-атаки, які у електронній комерції мають свої особливості), а також захист транзакцій в системах електронної комерції [4].
- організаційний захист інформації, який містить заходи, що спонукають працівників беззаперечно дотримуватися правил захисту інформації підприємства. Ці заходи займають важливе місце, адже недобросовісні працівники можуть використати службову інформацію в злочинних цілях [5].

Оскільки методи шахрайського здобуття інформації під час інтернет-еквайрингу стрімко розвиваються, виникає необхідність регулярного виявлення вразливостей протоколів та методів захисту та їх подальшого дослідження, що дасть змогу уникнути таких проблем у майбутньому.

Список використаної літератури

1. Кулик В. А. Розвиток електронного бізнесу в Україні. *Економіка та управління підприємствами.* 2017. С. 174.
2. Поліванов В.Є., Дмитрієва Н.О. Економічна сутність та генезис світового електронного бізнесу. *Актуальні проблеми міжнародних відносин.* 2018. № 134. С. 114.
3. Арістова І. В. *Інформаційна безпека людини як споживача телекомунікаційних послуг: монографія*/ І. В. Арістова, Д.В. Сулацький. – К.: Ред. журн. «Право України»; Х.: Право, 2013. – 184 с.
4. Йона О. О. *Дослідження стану сучасних технологій захисту електронних транзакцій* / О. О. Йона // Технологический аудит и резервы производства. − 2015. − № 2/6(22). − С. 42–44.
5. Bidgoli H. *Electronic Commerce*, Academic Press, 2002, 487p.