УДК 004.4+336
DOI https://doi.org/10.32782/2663-5941/2022.6/16

Ковалевський В.В.
Державний університет «Житомирська політехніка»

Вакалюк Т.А.
Державний університет «Житомирська політехніка»

СТАН ДОСЛІДЖЕНЬ У ГАЛУЗІ РОЗРОБКИ ТА ФУНКЦІОНУВАННІ СИСТЕМ ЗАХИСТУ СЕРВІСІВ ЕЛЕКТРОННОЇ КОМЕРЦІЇ

Проблема захисту веб додатків та, зокрема, сервісів електронної комерції є актуальною задачею, що потребує постійної уваги та роботи над вдосконаленням наявних методів. В даній роботі проаналізовано стан досліджень у цій галузі, а також наведено приклади наявних розробок, що направлені на підвищення безпекових показників. Згідно проведеного аналізу, науковці розглядають безпекову складову функціонування сервісів електронної комерції як сукупність організаційних та технічних заходів. Технічні заходи націлені на аналіз роботи систем і своєчасне виявлення потенційних загроз. Для цього використовуються методи нечіткої логіки, машинне навчання, математичне моделювання. У свою чергу, організаційні заходи мають на меті інформування користувачів щодо наявних загроз, роботу з законодавчими аспектами захисту інформації, впровадження наявних міжнародних безпекових стандартів. Також до організаційних заходів можна віднести законотворчі ініціативи, направлені на впорядкування процесів зберігання та обробки персональних даних користувачів сервісів електронної комерції. Одним із підходів щодо забезпечення комплексного захисту сервісів електронної комерції, що запропонували дослідники, є представлення сервісу електронної комерції у вигляді неорієнтованого графу, де кожен компонент сервісу є вершиною графу, а його ребра – зв'язки між цими компонентами. Це дозволяє спростити задачу автоматизації подальшого масштабування системи моніторингу, що аналізує комунікацію між ключовими компонентами сервісу електронної комерції та надсилає інформацію щодо виявлених аномалій у роботі сервісу. Науковці також розглядають методики адаптації і спрощення наявних фреймворків управління інформаційною безпекою, що має на меті спрощення їх впровадження для невеликих організацій. Це надасть змогу розширити застосування загальноприйнятих безпекових стандартів та покращити захищеність кінцевих користувачів сервісів електронної комерції. Окремі науковці пропонують використання методів математичного моделювання для побудови формальної моделі прийняття рішень у системі інформаційної безпеки, що дозволяє знизити вплив суб'єктивних факторів на кінцеві результати її роботи.

Ключові слова: *електронна комерція, інформаційна безпека, система, модель оцінювання, аналіз.*

Постановка проблеми. Питання забезпечення захисту сервісів електронної комерції не втрачає своєї актуальності та набуває все більшого розповсюдження з розвитком комерційної діяльності у глобальній мережі Інтернет. Пандемія COVID-19 значно вплинула на швидкість розповсюдження сервісів електронної комерції, що, в свою чергу, підвищило попит на постачання якісних безпекових рішень, що забезпечать надійний захист користувацьких даних.

Аналіз останніх досліджень і публікацій. Проблемі аналізу ефективності роботи систем забезпечення захисту веб сервісів загалом, та сервісів електронної комерції зокрема, приділяло увагу багато вчених, у тому числі: Бенц М. (Benz M.) та Чаттерджі Д. (Chatterjee D.), Ідіано д'Адамо (Idiano D'Adamo), Росіо Гонсалес-Санчес (Rocío González-Sánchez), Марія Соня Медіна-Сальгадо (Maria Sonia Medina-Salgado), Давід Сеттембре-Блундо(Davide Settembre-Blundo), Б. Тригубець, О. Мервінський, О. Мілов, А. Войтко, І. Гусарова, О. Домаскін, Є. Іванченко, І. Іванченко, О. Король, Г. Коц, І. Опірський, О. Фразе-Фразенко, Цю Ліронг (Qiu Lirong), Лі Цзе (Li Jie) та інші. Проте кожен з науковців розглядав зазначену проблему з різних аспектів.

Формулювання цілей статті. Саме тому метою статті є аналіз стану досліджень у галузі розробки та функціонуванні систем захисту сервісів електронної комерції.

Виклад основного матеріалу. Проблема захисту як веб додатків загалом, так і сервісів електронної комерції зокрема, є актуальним питанням, увага до якого не згасає, так як з розвитком систем захисту покращуються та адаптуються методи їх подолання. Постійно

проводиться робота над дотриманням балансу доцільного зменшення потенційних безпекових ризиків та збереженням комфортного середовища для кінцевих користувачів.

Забезпечення захисту сервісів електронної комерції поділяється на дві основні категорії – технічне та організаційне. До технічних заходів забезпечення захисту можна віднести різноманітні автоматизовані системи аналізу користувацького трафіку, організацію безпечних умов обробки і зберігання інформації якою оперує сервіс електронної комерції, своєчасне оновлення програмного забезпечення для запобігання використанню зловмисниками наявних вразливостей, проведення планових тестувань систем захисту сервісів електронної комерції незалежними експертами. У свою чергу, організаційні заходи включають в себе проведення планових аудитів систем захисту на відповідність встановленим вимогам, інформування користувачів щодо потенційних загроз, сертифікація в межах наявних міжнародних безпекових стандартів.

Клер Лейбатс (Claire Laybats) та Люк Тредіннік (Luke Tredinnick) у своїй роботі розглядають сучасні виклики інформаційній безпеці [1]. Згідно їх аналізу, незважаючи на стрімкий розвиток інформаційних технологій та збільшенню цінної інформації якою оперують різні системи, світ не спостерігає бурхливого зростання кількості кіберзлочинів. Автори вважають, що це пояснюється тим, що по мірі розповсюдження різноманітних інформаційних систем за останні десятиліття, паралельно зростала і зазнала змін та розвитку сфера інформаційної безпеки. Також вони роблять висновки, що основним напрямком забезпечення інформаційної безпеки в першу чергу має бути розуміння та управління ризиками, а не усунення загроз та їх наслідків. Незважаючи на розвиток технологій, головним безпековим ризиком будь-якої інформаційної системи являється людський фактор і зменшення його впливу на вразливість системи має бути частиною безпекових заходів [1].

У контексті організаційних заходів велика увага приділяється захисту, обробці та зберіганню персональних даних користувачів сервісів електронної комерції, що відображено у нормативно-правових актах, прийнятих у різних країнах. О. Мервінський проводить аналіз основних законодавчих вимог щодо захисту персональних даних у сфері електронної комерції, наголошуючи на важливості їх врахування при використанні технічних засобів забезпечення захисту сервісів електронної комерції [2].

Б. Тригубець у своєму дослідженні акцентує увагу на важливості захищеності обробки фінансової та персональної інформації користувачів, якою оперують системи електронної комерції [3]. Розглядаючи основні види шахрайських дій направлених на неправомірне використання користувацьких даних, науковець виділяє дві складові захисту сервісів електронної комерції: програмну та організаційну, вказуючи на необхідність постійного вдосконалення методів захисту для своєчасного запобігання наявним загрозам [3].

Бенц М. (Benz M.) та Чаттерджі Д. (Chatterjee D.) розглянули інформаційні безпекові ризики, що стосуються малого і середнього бізнесу та запропонували методологію аналізу стану захищеності інформаційної системи [4]. Автори зазначають, що не зважаючи на вже наявні фреймворки управління інформаційною безпекою – такі як ISO, CIS, PCI DSS, COBIT – для невеликих компаній вони можуть бути занадто складними та дорогими для впровадження. Запропонована методологія базується на фреймворку NIST CSF (National Institute of Standards and Technology's cybersecurity framework), що дозволяє використовувати його систему оцінки та рекомендацій (рис.1) [4]. Розробники методології проаналізували роботу фреймворку, використовуючи власний досвід та, враховуючи потреби цільової аудиторії, адаптували необхідні параметри фреймворку для створення набору вхідних даних для подальшого аналізу [4].

Результатом обробки даних є рекомендації щодо можливих змін та покращень для підвищення рівня інформаційної безпеки системи, що аналізується. Також надається приблизна оцінка вартості необхідних заходів з фінансової точки зору та необхідних людських ресурсів для її впровадження. Розроблена методологія дозволяє ідентифікувати найбільш вразливі місця інформаційної системи, оцінити її зрілість відносно наявних стандартів та визначити найбільш ефективні заходи для покращення інформаційної безпеки [4].

Колективом авторів (Ідіано д'Адамо (Idiano D'Adamo), Росіо Гонсалес-Санчес (Rocío González-Sánchez), Марія Соня Медіна-Сальгадо(Maria Sonia Medina-Salgado), Давід Сеттембре-Блундо(Davide Settembre-Blundo)) було проаналізовано тенденції розвитку сервісів електронної комерції в останні роки, зважаючи на їх бурхливий розвиток через пандемію COVID-19 [7]. Автори використовували дані з відкритих джерел, серед яких можна виділити Euro-

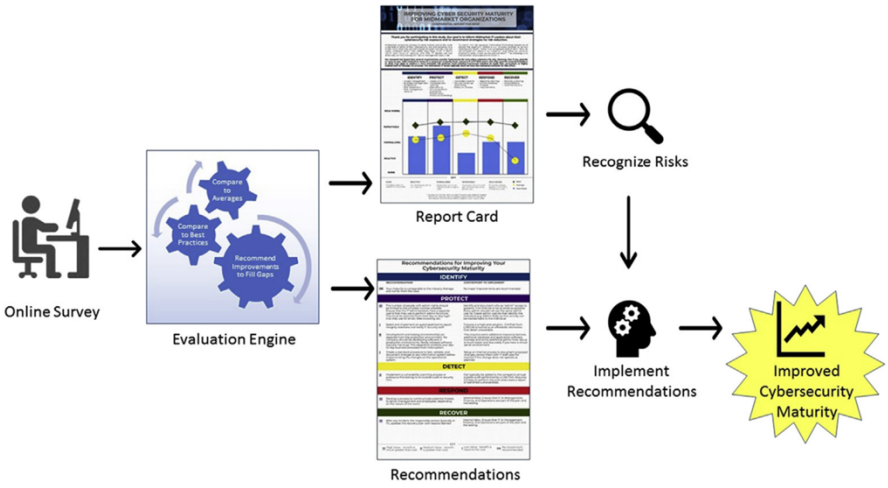

Рис. 1. Робота фреймворку NIST CSF (за Бенц М. (Benz M.) та Чаттерджі Д. (Chatterjee D.)) [4]

stat та Salesforce Shopping Index, а також залучали незалежних експертів для проведення опитувань згідно теми дослідження. Для аналізу отриманих даних використовувались MCDA метод та метод оцінювання за шкалою Лайкерта (Likert Scale Survey) [7].

Отримані результати дозволяють стверджувати, що одним із вагомих факторів, які впливають на стале зростання та розвиток сервісів електронної комерції, є забезпечення надійної та безпечної обробки і зберігання фінансової інформації користувачів та їх персональних даних. Автори зазначають про необхідність планування інвестицій у інформаційну безпеку та системний підхід до управління ризиками захисту інформації громадян та підприємств, що збирається та обробляється через цифрові канали [7].

Групою авторів (О. Мілов, А. Войтко, І. Гусарова, О. Домаскін, Є. Іванченко, І. Іванченко, О. Король, Г. Коц, І. Опірський, О. Фразе-Фразенко) запропоновано методологію моделювання взаємодії антагоністичних агентів у системах кібербезпеки [8]. У запропонованій методології традиційні методи і інструменти моделювання не протиставляються один одному, а розглядаються в сукупності, формуючи тим самим єдину методологічну базу моделювання поведінки антагоністичних агентів. Автори зазначають, що системи інформаційної безпеки функціонують в умовах невизначеності, що характеризується браком інформації для формалізації процесів з якими вони взаємодіють. Це, в свою чергу, підвищує суб'єктивний вплив особи, що приймає рішення на роботу системи інформаційної безпеки. Таким чином, побудова формальної моделі прийняття рішень дозволяє знизити вплив суб'єктивних факторів на функціонування системи інформаційної безпеки і, як результат, підвищити ефективність її роботи. Враховуючи складність і різноманітність процесів та об'єктів, з якими взаємодіє система інформаційної безпеки, досить складно використовувати уніфікований метод моделювання, який дозволить отримати необхідний рівень абстракції, тому автори пропонують використовувати інтеграцію різноманітних методів моделювання для побудови загальної моделі взаємодії антагоністичних агентів (рис.2). Така методика дозволяє сукупне використання всієї множини моделей та координацію їх застосування, що дозволяє підвищити якість моделювання за рахунок компенсації недоліків одних моделей перевагами інших. Саме ця особливість запропонованої методології виділяє її на тлі інших [8].

Необхідно зазначити, що автори вказують на наявні обмеження розробленої моделі, що, в свою чергу, залишає простір для майбутніх досліджень

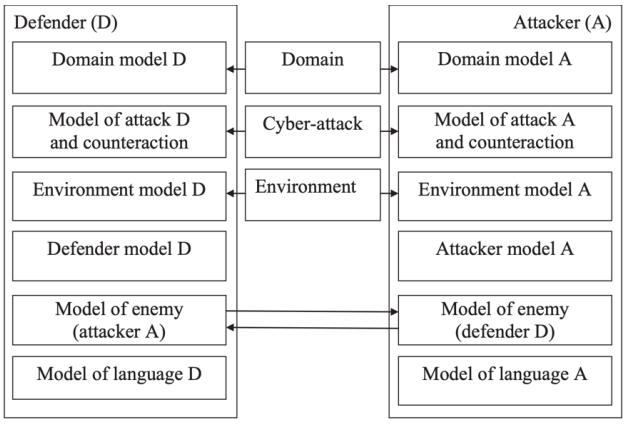

Рис. 2. Схема взаємозв'язку моделей компонентів антагоністичної взаємодії (за колективом авторів [8]).

та розширенню інструментів моделювання, таких як використання нейронних мереж, глибинного аналізу даних, застосування генетичних алгоритмів [8].

Х. Матбулі (H. Matbouli) та К. Гао (Q. Gao) провели дослідження безпекових ризиків, що мають вплив на розвиток та розповсюдження сервісів електронної комерції [9]. Автори зазначають, що недостатня захищеність сервісів електронної комерції призводить до значних фінансових втрат як через дії зловмисників, так і через побоювання користувачів щодо захищеності їх фінансових даних при проведенні електронних платежів. Як приклад, автори наводять статистику компанії McAfee, однієї з найбільших компаній, що спеціалізується на розробці систем інформаційної безпеки. У відповідності до цих даних, 63% споживачів переривали процес оформлення онлайн купівлі, не отримуючи підтверджень тому, що сервіс електронної комерції, яким вони вирішили скористуватись, відповідає необхідним безпековим стандартам [9].

Згідно проведеного аналізу, основними безпековими загрозами для сервісів електронної комерції являються викрадення конфіденційної та фінансової інформації користувачів. Запобігання цьому потребує комплексного підходу, що охоплює весь процес електронної комерції, починаючи з підвищення безпекової обізнаності користувача і закінчуючи підтримкою інфраструктури сервісу електронної комерції (сервери, канали передачі інформації, платіжні системи тощо) на належному рівні, що відповідає сучасним безпековим стандартам [9].

Науковці пропонують перелік організаційних стратегій та технологічних рішень, направлених на покращення інформаційної безпеки сервісів електронної комерції.

Яцзюань Чжан (Yajuan Zhang), Сіньян Денг (Xinyang Deng), Дайцзюнь Вей (Daijun Wei) та Йонг Денг (Yong Deng) пропонують модель оцінювання захищеності сервісу електронної комерції, що має на меті покращити та спростити цей процес [10]. Автори зазначають, що запропонована модель оцінювання охоплює більшість основних безпекових параметрів функціонування сервісу електронної комерції. В основу розробленої моделі покладено метод аналізу ієрархій у поєднанні з теорією Демпстера-Шафера [10].

Запропонована модель складається з п’яти основних етапів:

– розбиття поставленої задачі на основні компоненти;

– присвоєння оціночної ваги кожному з компонентів;

– дисконтування кожного компоненту;

– об’єднання отриманих коефіцієнтів ;

– визначення оцінки компоненту [10].

До перших двох етапів застосовується метод аналізу ієрархій, останні три використовують теорію Демпстера-Шафера (рис. 3).

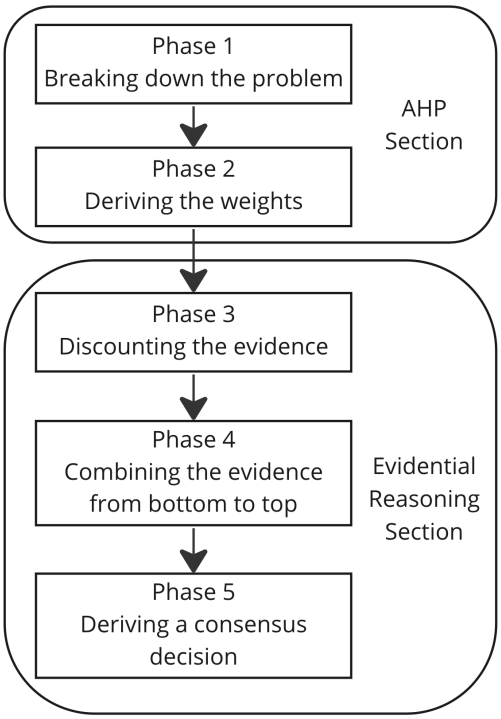

Рис. 3. Етапи роботи моделі [10]

Автори провели порівняння роботи розробленого алгоритму з аналогічними дослідженнями. Проаналізувавши отримані дані, вони дійшли висновку, що запропонований ними підхід дає більш точні результати оцінювання і є простішим у реалізації [10].

Колектив дослідників (Лука Деметріо (Luca Demetrio), Габріеле Коста (Gabriele Costa), Андреа Валенса (Andrea Valenza), Джованні Лагоріо (Giovanni Lagorio)) провели аналіз функціонування Web Application Firewall (WAF) та розробили інструмент, який дозволяє проводити симуляцію атаки на інформаційну систему захищену WAF [11].

Метою їх дослідження була спроба компрометації роботи WAF, що використовує машинне навчання для виявлення аномалій у вхідному трафіку. Слід зазначити, що WAF у комбінації з алгоритмами машинного навчання є сучасним підходом до забезпечення захисту інформацій-

них систем. Такі системи захисту здатні завчасно виявляти потенційні загрози, використовуючи попередньо накопичені дані щодо нормальної роботи інформаційної системи, і, керуючись закладеними у них політиками обробки трафіку, блокувати потенційно небезпечні активності [11].

Дослідники скористались особливостями обробки даних алгоритмами машинного навчання для створення запитів, які не будуть розцінені як потенційно небезпечні (рис. 4).

```
1  admin' OR 1=1#
2  admin' OR 0X1=1 or 0x726!=0x726 OR 0x1Dd
     not IN/*(seleCt 0X0)>c^Bj>N]*/ ((SeLeCT
      476),(SELECT (SElEct 477)),0X1de) oR
     8308 noT lIkE  8308\x0c AnD truE OR '
     FZ6/q' LiKE 'fz6/qI' anD TRUE anD '>U'
     != '>uz'#t'%'03;Nd
```

Рис. 4. Семантично еквівалентні запити [11]

Методологія, використана авторами, належить до класу підходів керованого мутаційного тестування. Її ідея полягає в тому, що тестування починається з невдалої спроби, вхідні дані якої поступово трансформуються через випадкове застосування попередньо визначених операторів мутації. Модифіковані тести виконуються, порівнюються і впорядковуються згідно заданим критеріям. Процес повторюється для тестів, які показали найкращі результати, доки не буде знайдено успішний тест (рис. 5) [11].

Таким чином, дослідникам вдалося обійти захисні алгоритми WAF та скомпрометувати систему захисту. Дослідження проводились з використанням популярних WAF систем, що доступні на ринку [11].

Цю Ліронг (Qiu Lirong) та Лі Цзе (Li Jie), вивчаючи проблему інформаційної безпеки сервісів електронної комерції, запропонували комплексну систему аналізу захищеності інформаційної системи, що включає в себе моніторинг, аналіз даних, оцінювання ризиків та інформування у разі виявлення потенційної загрози [12].

Автори пропонують представити систему електронної комерції у вигляді неорієнованого графу, де кожен компонент системи електронної комерції є його вершиною, а ребра – зв'язки між цими компонентами. Таким чином, система моніторингу отримує інформацію про всі зв'язки компоненту, який підключений до неї. Це дозволяє автоматизувати оптимізацію масштабування системи моніторингу для більш раціонального використання ресурсів. Автори пропонують наступний алгоритм для реалізації масштабування системи моніторингу (рис. 6). Де G – система

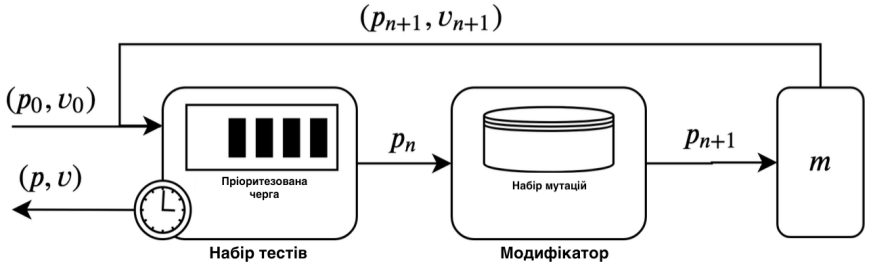

Рис. 5. Принцип роботи алгоритму [11]

(1) $\Phi = \varnothing$; $S = \varnothing$;
(2) while G has more edges do
(3) if $S = \varnothing$ then
(4) Pick an edge (u, v) such that $d(u) + d(v)$ is the largest;
(5) else
(6) Pick an edge (u, v) such that $v \in S$ and $d(u) + d(v)$ is the largest;
(7) $T_v \leftarrow$ the ME rooted at v;
(8) Add T_v into Φ;
(9) $S \leftarrow S \cup$ neighbor(v);
(10) Remove edges in T_v from G;
(11) if $d(u) > 0$ then
(12) $T_u \leftarrow$ the ME rooted at u;
(13) Add T_u into Φ;
(14) Remove edges in T_u from G;
(15) $S \leftarrow S \cup$ neighbor(u);
(16) Remove u and v and all nodes with degree 0 from G;
(17) Return Φ

Рис. 6. Запропонований алгоритм оптимізації системи моніторингу [12]

електронної комерції, $\Phi = \{T_1,\ldots,T_n\}$ – множина компонентів, S – мінімальне необхідне покриття моніторингу [12].

Система моніторингу збирає дані з підключених до неї компонентів системи електронної комерції і проводить їх аналіз, керуючись заданими правилами та інформацією про наявні вразливості. При виявленні аномалій генеруються попередження про наявну загрозу. Автори зазначають, що запропонована система не охоплює всі аспекти функціонування системи електронної комерції та має функціональні обмеження. Запропоновані авторами алгоритми також потребують подальшого вдосконалення та оптимізації [12].

Висновки. Проаналізувавши стан досліджень у галузі розробки та функціонування систем захисту сервісів електронної комерції можна стверджувати, що єдиного підходу до цього питання немає. Дослідники продовжують працювати над розробкою алгоритмів та методик, що дозволять проводити більш детальний аналіз систем захисту сервісів електронної комерції та покращити рівень їх захищеності. Дана проблема є актуальною та потребує подальших досліджень.

Список літератури:

1. Laybats Claire, Tredinnick Luke. Information security. *Business Information Review.* Vol. 33 (2). 2016. Pp. 76-80. 10.1177/0266382116653061.

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. https://ela.kpi.ua/bitstream/123456789/18033/1/30_p34.pdf

3. Тригубець Б. Технології захисту інформації в електронній комерції. *Матеріали IV Міжнародної студентської науково – технічної конференції.* Тернопіль: Тернопільський національний технічний університет ім. І.Пулюя (м. Тернопіль, 28-29 квітня 2021 р.), 2021. С. 11-12. https://tntu.edu.ua/storage/pages/00000852/Zbirnyk-studconf2021.pdf

4. Benz M., Chatterjee D. Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons.* Vol. 63 (4). 2020. Pp. 531-540. doi: 10.1016/j.bushor.2020.03.010

5. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. URL: https://doi.org/10.6028/NIST.CSWP.04162018 (дата звернення 25.11.2022).

6. Bill Sweeney. Cybersecurity Is Every Executive's Job. Harvard Business Review. 2016. https://hbr.org/2016/09/cybersecurity-is-every-executives-job

7. D'Adamo I., González-Sánchez R., Medina-Salgado M.S., Settembre-Blundo D. E-Commerce Calls for Cyber-Security and Sustainability: How European Citizens Look for a Trusted Online Environment. *Sustainability.* Vol. 13 (12), 2021. 6752. https://doi.org/10.3390/su13126752

8. Milov O., Voitko A., Husarova I., Domaskin O., Ivanchenko Ye., Ivanchenko I., Korol O., Kots H., Opirskyy I., Fraze-Frazenko O. Development of methodology for modeling the interaction of antagonistic agents in cybersecurity systems. *Eastern-European Journal of Enterprise Technologies.Vol.* 2. 2019. Pp. 56-66. 10.15587/1729-4061.2019.164730

9. Matbouli H., Gao Q. An overview on web security threats and impact to e-commerce success. *International Conference on Information Technology and e-Services*, 2012. pp. 1-6, doi: 10.1109/ICITeS.2012.6216645

10. Zhang, Y., Deng, X., Wei, D., Deng, Y. Assessment of E-Commerce security using AHP and evidential reasoning. *Expert Systems with Applications,* Vol. 39(3), 2012. 3611–3623. doi:10.1016/j.eswa.2011.09.051

11. Demetrio L., Valenza A., Costa G., Lagorio G. WAF-A-MoLE: Evading Web Application Firewalls through Adversarial Machine Learning. *Proceedings of the 35th Annual ACM Symposium on Applied Computing (SAC '20)*. Association for Computing Machinery, New York, NY, USA, 2020. Pp. 1745–1752. https://doi.org/10.1145/3341105.3373962

12. Qiu L., Li J. Covering the Monitoring Network: A Unified Framework to Protect E-Commerce Security. *Complexity*. 2017. 6254842. 10.1155/2017/6254842

Kovalevskyi V.V., Vakaliuk T.A. THE STATE OF RESEARCH IN THE FIELD OF DEVELOPMENT AND FUNCTIONING OF PROTECTION SYSTEMS FOR E-COMMERCE SERVICES

Protection of web applications and, in particular, e-commerce services is a task which requires constant attention and work on improving existing defense and security methods. This paper analyzes the state of research in this field and provides examples of existing developments aimed at increasing safety indicators. According to the conducted analysis, scientists consider the security component of e-commerce services as a set of organizational and technical measures. Technical measures are aimed at analyzing the operation of systems and timely detection of potential threats. To achieve desired results there are used methods of

fuzzy logic, machine learning, and mathematical modeling. Organizational measures cover users informing about existing threats, working with legislative aspects of information protection and implementation of existing international security standards. Organizational measures also include legislative initiatives pointed to streamline the processes of storing and processing personal data of e-commerce service users. One of the approaches to provide comprehensive protection of e-commerce services proposed by researchers is to represent the e-commerce service in the form of an undirected graph, where each component of the service is a vertex of the graph, and its edges are connections between these components. This makes it possible to simplify the automation task for the further scaling of the monitoring system, which analyzes the communication between the key components of the e-commerce service and sends information about detected anomalies. Scientists also consider methods of adaptation and simplification of existing information security management frameworks to simplify their implementation for small organizations. This will allow to expand the integration of generally accepted security standards and improve the security for the end users of e-commerce services. Some scientists suggest the use of mathematical modeling methods to build a formal decision-making model of the information security system, which should help to reduce the influence of human factors on the final decision-making results.

Key words: *e-commerce, information security, system, assessment model, analysis.*