УДК 004.4+336 https://doi.org/10.35546/kntu2078-4481.2023.3.13

В. В. КОВАЛЕВСЬКИЙ
аспірант кафедри інженерії програмного забезпечення
Державний університет «Житомирська політехніка»
ORCID: 0000-0001-7144-1899

Т. А. ВАКАЛЮК
доктор педагогічних наук, професор,
завідувач кафедри інженерії програмного забезпечення
Державний університет «Житомирська політехніка»
ORCID: 0000-0001-6825-4697

ОГЛЯД НАЯВНИХ МЕТОДІВ ОЦІНКИ ЕФЕКТИВНОСТІ РОБОТИ СИСТЕМ ЗАХИСТУ СЕРВІСІВ ЕЛЕКТРОННОЇ КОМЕРЦІЇ

Оцінка ефективності роботи систем захисту інформаційних систем та, зокрема, сервісі електронної комерції є актуальної задачею, що потребує постійного вдосконалення та розвитку. В даній роботі проведено огляд існуючих методів оцінки ефективності роботи систем захисту, а також розглянуто наявні підходи для побудови моделей безпекових ризиків інформаційних систем. Однією з основних вимог до оцінки ефективності роботи систем захисту є послідовність та безперервність проведення заходів направлених на виявлення потенційних загроз та вразливих елементів системи. Такий підхід забезпечує своєчасну реакцію на безпекові інциденти та мінімізацію їх наслідків. Важливу роль у цьому процесі відіграє автоматизація, що дозволяє пришвидшити прийняття рішень щодо безпекових інцидентів та виключити або мінімізувати вплив людського фактору. Для забезпечення ширшого охоплення автоматизації процесів оцінки ефективності роботи систем захисту, постає нагальною потреба у формалізації процесів, що відбуваються в середині інформаційної системи та побудови відповідних моделей цих процесів, які в свою чергу дозволяють відпрацьовувати різноманітні сценарії прийняття рішень при виникненні безпекових інцидентів. Окрім цього це надає можливість визначити ключові показники ефективності роботи систем захисту значення яких репрезентують загальний стан системи та допомагають провести якісну оцінку ефективності її роботи. Одним із підходів до оцінки ефективності роботи системи безпеки, що пропонують дослідники, є використання системи економетрики кібербезпеки (Cyberspace Security Econometrics System (CSES). Особливістю даної системи оцінки ефективності роботи системи безпеки є урахування економічних ризиків при виникненні безпекових інцидентів, що в свою чергу дозволяє оцінити фінансовий вплив на роботу інформаційної системи у разі відмови систем захисту. Невід'ємною частиною оцінки ефективності роботи систем захисту є моделювання атак на систему у контрольованих умовах. Це дозволяє отримувати інформацію щодо відповідності системи захисту сучасним загрозам та визначати її елементи, що потребують вдосконалення чи модернізації. Слід зазначити, що існують різні стандарти та фреймворки для моделювання атак на інформаційні системи. Таке різноманіття зумовлене відмінностями безпекових стандартів у різних галузях та цілях, що переслідуються при моделювання атак.

Ключові слова: *електронна комерція, інформаційна безпека, система, показники ефективності, моделювання.*

V. V. KOVALEVSKYI
Postgraduate Student at the Department of Software Engineering
Zhytomyr Polytechnic State University
ORCID: 0000-0001-7144-1899

T. A. VAKALIUK
Doctor of Pedagogical Science, Professor,
Head of the Software Engineering Department
Zhytomyr Polytechnic State University
ORCID: 0000-0001-6825-4697

REVIEW OF EXISTING METHODS FOR ASSESSING THE EFFECTIVENESS OF THE OPERATION OF E-COMMERCE SERVICE PROTECTION SYSTEMS

The evaluation of the effectiveness of information system protection systems, and in particular, e-commerce services, is a crucial task that necessitates continual advancement and development. This paper provides an overview of existing methods for evaluating the effectiveness of information systems protection systems and considers existing approaches for building models of information system security risks. One of the primary requirements for evaluating the effectiveness of information system protection systems is the consistency and continuity of measures aimed at identifying potential

threats and vulnerable system elements. This approach ensures timely response to security incidents and minimizes their consequences. Automation plays a significant role in this process, as it allows for faster decision-making on security incidents and excludes or minimizes the influence of the human factor. To ensure wider coverage of automation of the processes of evaluating the effectiveness of information system protection systems, there is an urgent need for the formalization of the processes that take place within the information system and the construction of appropriate models of these processes, which in turn allow to work on various scenarios for decision-making in the event of security incidents. Additionally, this provides an opportunity to identify key performance indicators of information system protection systems, the values of which represent the overall state of the system and help to conduct a qualitative assessment of the effectiveness of its work. One of the approaches to evaluate the effectiveness of the security system, which is proposed by researchers, is the use of the cyberspace security econometrics system (Cyberspace Security Econometrics System (CSES)). A key feature of this system for evaluating the effectiveness of the security is the consideration of economic risks in the event of security incidents, which in turn allows to assess the financial impact on the operation of the information system in the event of a failure of the protection systems. An important part of the evaluation of the effectiveness of information system protection systems is the modeling of attacks on the system within controlled environment. This allows to obtain information on the compliance of the protection system with modern threats and identify its elements that need to be improved or modernized. It should be noted that there are different standards and frameworks for modeling attacks on information systems. This diversity is due to the differences in security standards for different industries and the goals pursued in modeling attacks.

Key words: *e-commerce, information security, system, performance indicators, modeling.*

Постановка проблеми

Забезпечення захисту сервісів електронної комерції є задачею яка ніколи не втрачає своєї актуальності. Зважаючи на стрімке зростання розповсюдження сервісів електронної комерції у різних галузях та кількість чутливої інформації якою вони оперують, якісне забезпечення інформаційної безпеки являється фундаментальною частиною їх функціонування.

В свою чергу оцінка ефективності роботи систем захисту сервісів електронної комерції є однією з важливих задач, що потребує постійної уваги як на етапі проектування сервісу електронної комерції, так і під час його роботи з кінцевими користувачами. Оцінка ефективності роботи систем захисту дозволяє своєчасно виявляти, запобігати, а також мінімізувати наслідки кібератак та дій шахраїв.

Аналіз останніх досліджень і публікацій

Проблемі оцінки ефективності роботи систем захисту інформаційних систем загалом, та сервісів електронної комерції зокрема, приділяло увагу багато дослідників, у тому числі Фредерік Шелдон (Frederick T. Sheldon), що пропонує використовувати систему економетрики кібербезпеки (CSES) [2]. Ігор Бернік (Igor Bernik) та Кайя Пріслан (Kaja Prislan) у своїй роботі використовували модель ISP 10x10M для проведення оцінки ефективності роботи систем захисту [1]. Ларрі Конклін (Larry Conklin), Вікторія Дрейк (Victoria Drake) та Свен Стрітматтер (Sven Strittmatter) у своїй статті описали підхід до моделювання загроз інформаційної безпеки, що в свою чергу дозволяє провести оцінку безпекових ризиків [3]. В. Плескач, В. Краснощок, М. Мельник, С. Клименко, Романас Тумасоніс (Romanas Tumasonis) провели аналіз стану та тенденцій в сфері розробки систем захисту для сервісів електронної комерції [12]. Енгла Лінг (Engla Rencelj Ling), Матіас Екстед (Mathias Ekstedt) у своїй статті приводять опис розробленої ними мови для моделювання загроз інформаційної безпеки (sasLang) та наводять приклади її використання [3]. Кожен із дослідників висвітлює зазначену проблему з урахуванням власного досвіду та в контексті галузі своєї основної діяльності.

Формулювання мети дослідження

Саме тому метою статті є огляд наявних методів оцінки ефективності роботи систем захисту сервісів електронної комерції та інформаційних систем загалом.

Виклад основного матеріалу дослідження

Оцінка ефективності роботи систем захисту сервісів електронної комерції це неперервний процес, який включає в себе аналіз поточного стану системи, виявлення потенційно вразливих елементів системи, постійне вдосконалення і розвиток системи захисту з урахуванням нових технологій та загроз.

Можна виділити наступні загальноприйняті підходи до організації оцінки ефективності роботи систем захисту сервісів електронної комерції:

1. Визначення та впровадження ключових показників ефективності роботи системи захисту.
2. Створення моделі безпекових ризиків сервісу електронної комерції. Таке моделювання дозволяє оцінити ефективність роботи системи захисту шляхом порівняння потенційних ризиків та наявних заходів безпеки.
3. Моделювання атак на систему в контрольованих умовах. Це допомагає оцінити ефективність роботи системи захисту та виявити можливі слабкі місця.

Визначення та впровадження ключових показників ефективності роботи систем захисту дозволяє вимірювати різні аспекти роботи системи захисту, кількість виявлених та виправлених вразливостей, швидкість виявлення

вразливостей тощо. Це дає можливість візуалізувати та формалізувати актуальні дані, що в свою чергу полегшує подальший аналіз та автоматизацію прийняття рішень. Важливу роль відіграє визначення якісних метрик, що відображатимуть реальний стан роботи системи захисту, нестимуть максимальну користь та інформативність. Від цього напряму залежить на скільки оперативними та відповідними до ситуації буду дії у разі виникнення безпекових інцидентів.

Дослідники Ігор Бернік (Igor Bernik) та Кайя Пріслан (Kaja Prislan) пропонують вимірювати ефективність роботи системи захисту використовуючи модель ISP 10x10M [1]. Даний підхід полягає у поєднанні десяти критичних факторів успіху (CSF), ста ключових показників ефективності (KPI), десять для кожного з факторів успіху, та шести визначених рівнів ефективності роботи системи захисту. В свою чергу, для критичних факторів успіху та ключових показників ефективності визначаються вагові коефіцієнти. Крім визначення вагових коефіцієнтів, дослідники використовують статистичний для встановлення кореляцій між критичними факторами успіху та індивідуальними ключовими показниками ефективності. Процедура проводилась шляхом обчислення коефіцієнтів кореляції Пірсона між CSF та між KPI, включеними в індивідуальні CSF [1].

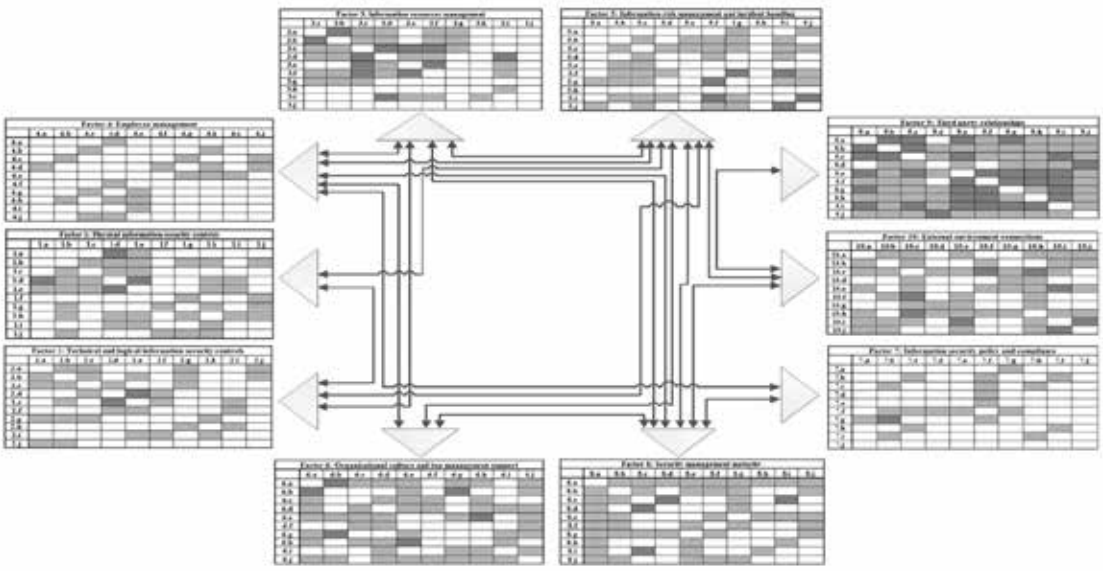

Рис. 1. Модель кореляції між CSF та KPI [1].

Аналіз результатів та визначення важливості окремих елементів моделі ISP 10x10M також дає можливість графічно представити на скільки ефективною є система безпеки в тих чи інших областях (рис. 2) [1]. Модель ISP 10×10M передбачає, що цілісна система інформаційної безпеки може бути досягнута лише шляхом забезпечення високого рівня результативності в десяти різних галузях. Однак абсолютна або 100% безпека не існує і не може бути досягнута на практиці, тому безпекові заходи лише частково успішні. Біла область позначає абсолютну ефективність інформаційної безпеки, що складається з десяти факторів, яка є лише теоретично можливою. Темна область показує оптимальний рівень ефективності інформаційної безпеки, досягнутий при ефективному управлінні всіма областями. Сіра область представляє ситуацію в якій жоден з показників не досягає очікуваних значень [1].

Результати отримані при використанні моделі ISP 10x10M надають можливість категоризувати ефективність роботи системи безпеки, що в свою чергу дозволяє визначити проблемні області та кроки необхідні для забезпечення бажаного рівня захисту [1].

Науковець Фредерік Шелдон (Frederick T. Sheldon) пропонує використовувати систему економетрики кібербезпеки (Cyberspace Security Econometrics System (CSES). Цей підхід використовує кількісну оцінку надійності, продуктивності та ефективності системи безпеки враховуючи критичність кожного елемента який потребує захисту з точки зору економічних ризиків [2].

Для визначення середньої вартості відмови системи (Mean Failure Cost (MFC) автор пропонує зібрати наступну інформацію: перелік зацікавлених сторін (Stakeholders), перелік специфікацій та вимог до системи безпеки. Для кожної з зацікавлених сторін та кожної з вимог до системи безпеки визначити коефіцієнт втрат, ставку (Stake), які понесе зацікавлена сторона у разі відмови системи яку ми захищаємо. Для кожного компонента вимог до системи безпеки визначити ймовірність їх виконання [2]. Отримані дані дозволяють створити наступну матрицю (рис. 3).

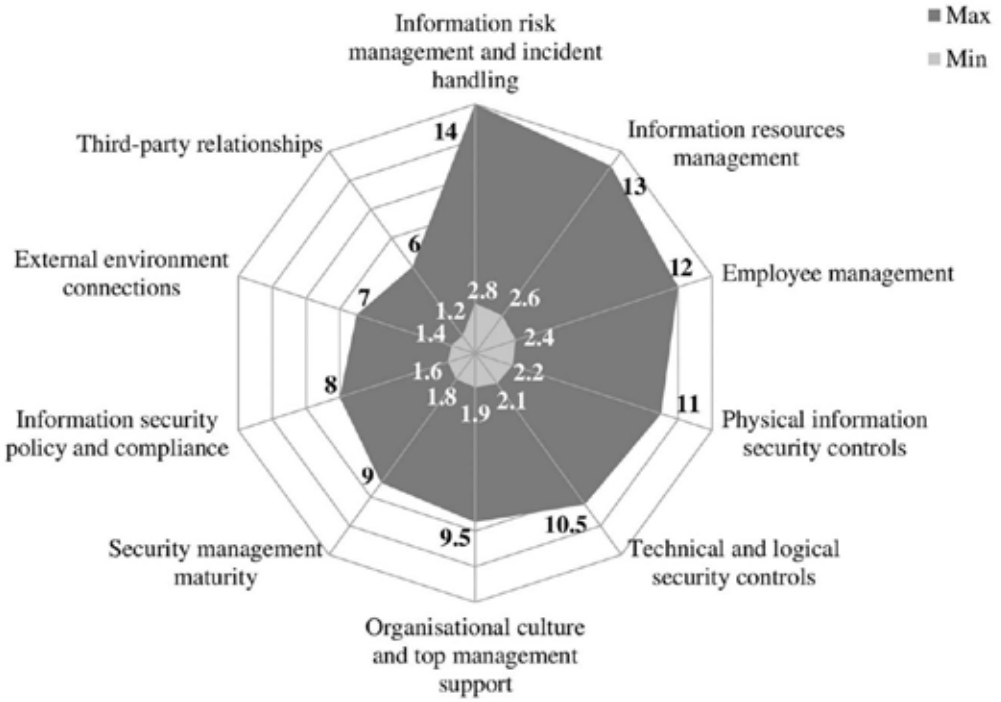

Рис. 2. Графічне представлення аналізу ефективності системи безпеки [1]

		Security Requirements				
		R1	R2	R3	...	Rn
Stakeholders	S1					
	S2					
	S3					
	...				FC_i^j	
	Sm					
		Probabilities of Security Requirements Delivery				
					P^j	

Рис. 3. Матриця вартості відмови системи безпеки [2]

Комірка матриці FC відображає втрати які несе зацікавлена сторона S у випадку, якщо не виконуються вимоги виставлені до системи безпеки R. Значення P відповідає визначеній ймовірності успішного виконання заданих вимог до системи безпеки. Враховуючи зазначене середня вартість відмови системи (MFC) визначається наступним чином (формула 1) [2].

$$MFC_i = \sum_{i=1}^{n} FC_i^j \times (1 - P^j). \quad (1)$$

Описаний спосіб оцінки ефективності системи безпеки є гнучким та дозволяє використовувати широкий спектр показників, які можуть не завжди бути безпосередньо пов'язані з безпекою системи, для отримання кінцевої оцінки в контексті кожної із зацікавлених сторін.

Моделювання безпекових ризиків – це процес, що має на меті ідентифікацію, оцінку та пом'якшення загроз для системи яку ми захищаємо (рис. 4). Цей процес дозволяє краще зрозуміти потенційні загрози та вжити заходів для їх запобігання. Базовий підхід до побудови моделі безпекових ризиків складається з чотирьох кроків [3] [4]:

1. Ідентифікація безпекових ризиків. На цьому етапі ідентифікують потенційні загрози системі. Це можна зробити провівши аналіз архітектури системи, бізнес-процесів, використання зовнішніх сервісів, тощо.
2. Оцінка безпекових ризиків. На цьому етапі проводиться оцінка ймовірності та впливу на систему кожної з визначених загроз. Це допомагає визначити, які загрози є найбільш серйозними.
3. Пом'якшення безпекових ризиків. На цьому етапі вживаються заходи для зменшення ризику виникнення загрози. Цього можна досягти впроваджуючи нові елементи системи захисту чи адаптуючи або оновлюючі вже наявні.
4. Валідація. Цей етап має на меті перевірку чи були вжиті всі необхідні заходи для пом'якшення кожної з визначених загроз.

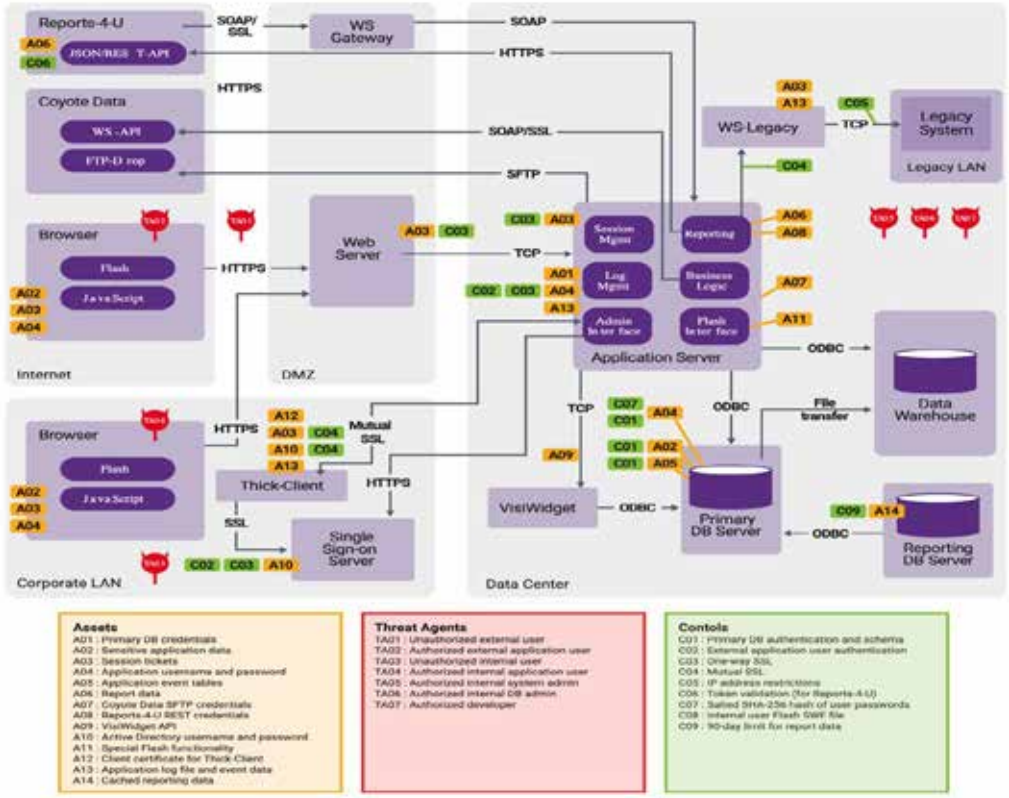

Рис. 4. Приклад моделювання безпекових ризиків [4]

Регулярне моделювання безпекових ризиків дозволяє отримати задокументовані визначені та задокументовані кроки, необхідні для покращення роботи системи безпеки. Окрім цього, такий підхід дозволяє виявляти потенційні проблеми в системі безпеки заздалегідь; проводити оцінку нових видів загроз, які не були враховані при початковому проектуванні системи безпеки; переглядати вимоги, що визначені до системи безпеки, приділяти увагу безпековим ризикам, що є унікальними для сервісів, які захищає система безпеки; вчасно проводити розподілення ресурсів необхідних для підтримання роботи системи безпеки на належному рівні [4].

Також можна виділити наступні розповсюджені підходи до моделювання безпекових ризиків: STRIDE, PASTA, Bow-tie та CORAS. Метод STRIDE фокусується на шести найпоширеніших загрозах: підробленні ідентифікації, втручанні в обробку даних, неможливості притягнення до відповідальності, розкритті інформації, відмові в обслуговуванні та підвищенні привілеїв. Метод PASTA фокусується на оцінці безпекових ризиків, що можуть вплинути на функціонування системи, і передбачає сім етапів моделювання безпекових ризиків. Метод Bow-tie дозволяє проілюструвати ризики системи у формі метелика (рис. 5), де загрози знаходяться зліва, наслідки – справа, а події – посередині.

Метод CORAS включає в себе 8 кроків (рис. 6), що дозволяють проаналізувати потенційні загрози та розробити заходи протидії [5].

Моделювання атак на систему захисту в контрольованих умовах є дієвим засобом оцінки ефективності її роботи, дозволяє в наближених до реальних умовах перевірити реакцію системи захисту на ті чи інші сценарії та сформувати звіти щодо виявлених проблем та вразливостей. Регулярне проведення таких тестувань допомагає підтримувати систему захисту на актуальному рівні в контексті потенційних загроз, що постійно змінюються.

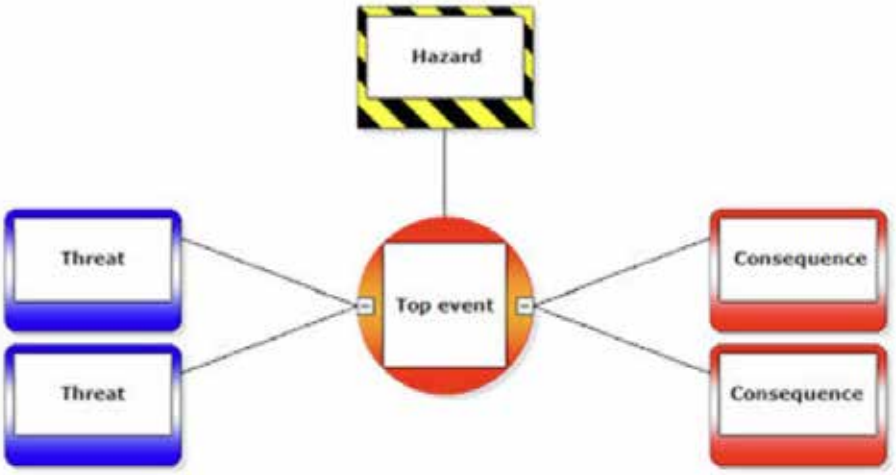

Рис. 5. Bow-tie метод моделювання безпекових ризиків [6]

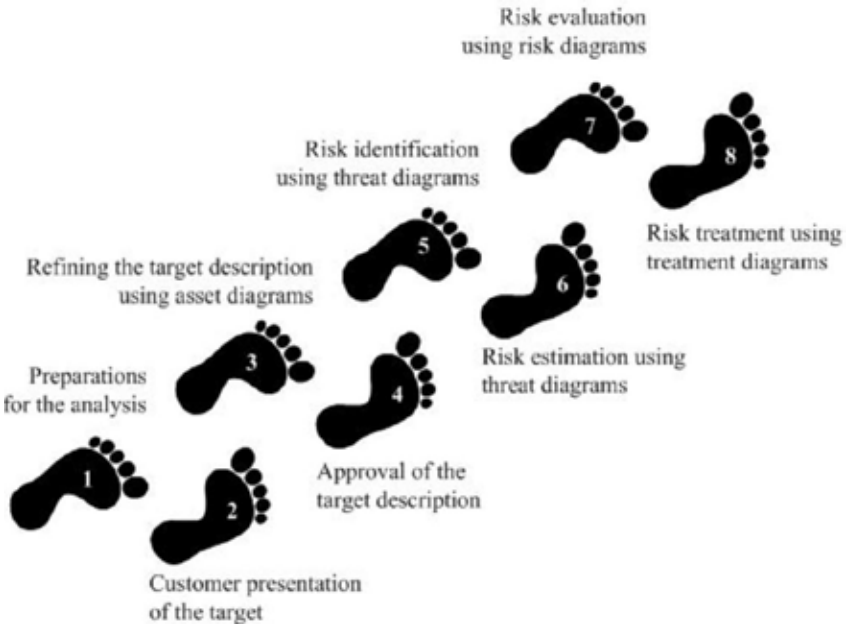

Рис. 6. Метод CORAS, етапи аналізу безпекових ризиків [7]

Одним з поширених методів проведення моделювання атак на систему захисту є тестування на проникнення (Penetration Testing). Його суть полягає в тому, що спеціалісти з безпеки намагаються обійти систему захисту використовуючи різноманітні техніки та засоби. Загалом, у тестуванні на проникнення можна виділити шість етапів (рис. 7) [8]:

1. Підготовка до тесту. На цьому етапі проводиться збір інформації про систему, де буде проводитись тестування, узгоджуються деталі тесту, включаючи затвердження методів і засобів, що будуть використані.
2. Створення плану тестування. Цей етап включає в себе визначення потенційно вразливих елементів системи безпеки та яким саме перевірки безпеки мають бути застосовані щодо них.
3. Підготовка команди, що займатиметься тестуванням, узгодження деталей та сценаріїв, що мають бути відпрацьовані.
4. Визначення цілей, на які будуть направлені спроби проникнення. Окрім заздалегідь означених потенційно проблемних елементів системи безпеки, спеціалісти визначають додаткові вектори атаки, які на їх думку будуть доцільними.
5. Проведення тесту на проникнення. На цьому етапі спеціалісти з безпеки безпосередньо намагаються обійти наявну систему захисту та задокументувати отримані результати.
6. Агрегація та аналіз отриманих даних. Цей етап має на меті обробку отриманих результатів та створення звітів щодо знайдених вразливостей та рекомендацій для їх подальшого усунення.

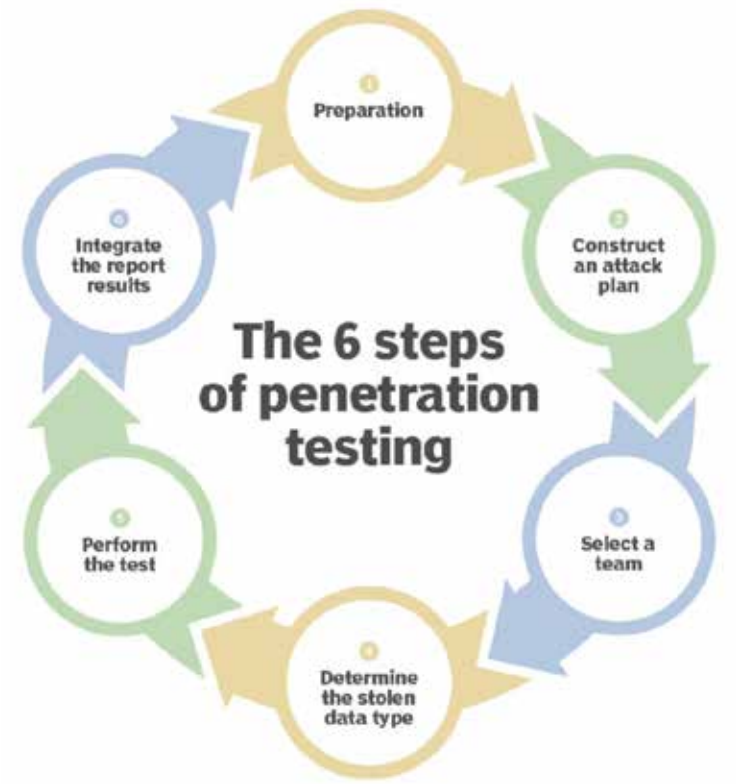

Рис. 7. Етапи тестування на проникнення [8]

Виділяють три загальні рівні проведення тестування на проникнення [8]:

1. Black box тестування – під час проведення цього тесту, спеціалісти з безпеки не мають жодної інформації про систему, яку вони тестують, задача полягає в знаходженні вразливостей, що можуть бути використані.
2. Gray box тестування – у цьому випадку спеціалісти, що проводять тестування, отримують деяку інформацію про систему безпеки, яку вони тестують. Ця інформація використовується для пошуку вразливостей, які не були виявлені при Black box тестуванні.
3. White box тестування – спеціалісти з безпеки, що проводять тестування, отримують повну інформацію про систему безпеки. Задача полягає у виявленні вразливостей, які не були знайдені під час Black box та Grey box тестування.

Також необхідно зазначити, що існують різні стандарти та фреймворки для проведення тестування на проникнення. Це обумовлено варіативністю цілей тестування та відмінностями безпекових стандартів у різних галузях. До поширених у використанні стандартів і фреймворків можна віднести OSSTMM, OWASP, PTES, ISSAF, NIST, PCI DSS [9] [10]. Кожен з них надає можливість провести тестування необхідної складності та з урахуванням специфіки роботи системи, що перевіряється.

Висновки

Провівши огляд наявних методів оцінки ефективності роботи систем захисту електронної комерції можна стверджувати, що у цьому напрямку проводиться багато досліджень та оновлень. Робота з науковими джерелами демонструє сталий інтерес до цієї теми, дослідники шукають методи покращення вже наявних підходів оцінки ефективності роботи систем захисту, а також розробляють і пропонують нові, чого вимагає неспинний розвиток технологій. Перспективами подальших досліджень вбачаються створення більш гнучких та масштабуємих методів оцінки ефективності роботи систем захисту, що забезпечить ширше їх використання для інформаційних систем різних розмірів та направленності.

Список використаної літератури

1. Bernik I, Prislan K. Measuring information security performance with 10 by 10 model for holistic state evaluation. *PLoS ONE*. 2016. Vol. 11, no. 9. URL: https://doi.org/10.1371/journal.pone.0163050.
2. Sheldon F. Evaluating security controls based on key performance indicators and stakeholder mission. proceedings of the 4th annual workshop on cyber security and informaiton intelligence research developing strategies to meet the cyber security and information intelligence challenges ahead. *Cyber security and information intelligence research workshop*. 2008.

3. Conklin L., Drake V., Strittmatter S. Threat modeling process | OWASP foundation. *OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation*. URL: https://owasp.org/www-community/Threat_Modeling_Process.

4. What is threat modeling and how does it work? | synopsys. *Synopsys | EDA Tools, Semiconductor IP and Application Security Solutions*. URL: https://www.synopsys.com/glossary/what-is-threat-modeling.html.

5. Rencelj Ling E., Ekstedt M. A threat modeling language for generating attack graphs of substation automation systems. *International journal of critical infrastructure protection*. 2023. Vol. 41. P. 100601. URL: https://doi.org/10.1016/j.ijcip.2023.100601.

6. Introduction to bowtie | civil aviation authority. *Civil Aviation Authority*. URL: https://www.caa.co.uk/safety-initiatives-and-resources/working-with-industry/bowtie/about-bowtie/introduction-to-bowtie/.

7. The CORAS Method. *The CORAS Method*. URL: https://coras.sourceforge.net/.

8. Kirvan P. Pen testing guide: Types, steps, methodologies and frameworks | TechTarget. *Security*. URL: https://www.techtarget.com/searchsecurity/tip/Pen-testing-guide-Types-steps-methodologies-and-frameworks.

9. Nicholls M. Penetration testing methodologies – the top 5 | redscan. *Redscan*. URL: https://www.redscan.com/news/top-five-penetration-testing-methodologies.

10. WSTG – latest | OWASP foundation. *OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation*. URL: https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies.

11. A systematic method for measuring the performance of a cyber security operations centre analyst / E. Agyepong et al. *Computers & security*. 2022. P. 102959. URL: https://doi.org/10.1016/j.cose.2022.102959.

12. Current state and trends in the development of e-commerce software protection systems / V. Pleskach et al. *CEUR workshop proceedings*. 2021. No. 3179. P. 79–88.

13. Cyber security risk modeling in distributed information systems / D. Palko et al. *Applied sciences*. 2023. Vol. 13, no. 4. P. 2393. URL: https://doi.org/10.3390/app13042393.

14. An integrated conceptual model for information system security risk management supported by enterprise architecture management / N. Mayer et al. *Software & systems modeling*. 2018. Vol. 18, no. 3. P. 2285–2312. URL: https://doi.org/10.1007/s10270-018-0661-x.

15. Security risk assessments: modeling and risk level propagation / D. Angermeier et al. *ACM transactions on cyber-physical systems*. 2022. URL: https://doi.org/10.1145/3569458 (date of access: 24.09.2023).

References

1. Bernik I & Prislan K. (2016). Measuring information security performance `with 10 by 10 model for holistic state evaluation. *PLoS ONE*, *11*(9). https://doi.org/10.1371/journal.pone.0163050

2. Sheldon, F. (2008). Evaluating security controls based on key performance indicators and stakeholder mission. proceedings of the 4th annual workshop on cyber security and informaiton intelligence research developing strategies to meet the cyber security and information intelligence challenges ahead. *Cyber Security and Information Intelligence Research Workshop*.

3. Conklin, L., Drake, V., & Strittmatter, S. (2022). *Threat modeling process | OWASP foundation*. OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. https://owasp.org/www-community/Threat_Modeling_Process

4. *What is threat modeling and how does it work? | synopsys*. (2023). Synopsys | EDA Tools, Semiconductor IP and Application Security Solutions. https://www.synopsys.com/glossary/what-is-threat-modeling.html

5. Rencelj Ling, E., & Ekstedt, M. (2023). A threat modeling language for generating attack graphs of substation automation systems. *International Journal of Critical Infrastructure Protection*, *41*, 100601. https://doi.org/10.1016/j.ijcip.2023.100601

6. *Introduction to bowtie | civil aviation authority*. (2023). Civil Aviation Authority. https://www.caa.co.uk/safety-initiatives-and-resources/working-with-industry/bowtie/about-bowtie/introduction-to-bowtie/

7. *The CORAS Method*. (б. д.). The CORAS Method. https://coras.sourceforge.net/

8. Kirvan, P. (2022, 7 квітня). *Pen testing guide: Types, steps, methodologies and frameworks | TechTarget*. Security. https://www.techtarget.com/searchsecurity/tip/Pen-testing-guide-Types-steps-methodologies-and-frameworks

9. Nicholls, M. (2023). *Penetration testing methodologies – the top 5 | redscan*. Redscan. https://www.redscan.com/news/top-five-penetration-testing-methodologies

10 .WSTG – latest | OWASP foundation. (2023). OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies

11. Agyepong, E., Cherdantseva, Y., Reinecke, P., & Burnap, P. (2022). A systematic method for measuring the performance of a cyber security operations centre analyst. *Computers & Security*, 102959. https://doi.org/10.1016/j.cose.2022.102959

12. Pleskach, V., Krasnoshchok, V., Melnyk, M., Klymenko, S., & Tumasonis, R. (2021). Current state and trends in the development of e-commerce software protection systems. *CEUR Workshop Proceedings*, (3179), 79–88.

13. Palko, D., Babenko, T., Bigdan, A., Kiktev, N., Hutsol, T., Kuboń, M., Hnatiienko, H., Tabor, S., Gorbovy, O., & Borusiewicz, A. (2023). Cyber security risk modeling in distributed information systems. *Applied Sciences*, *13*(4), 2393. https://doi.org/10.3390/app13042393

14. Mayer, N., Aubert, J., Grandry, E., Feltus, C., Goettelmann, E., & Wieringa, R. (2018). An integrated conceptual model for information system security risk management supported by enterprise architecture management. *Software & Systems Modeling*, *18*(3), 2285–2312. https://doi.org/10.1007/s10270-018-0661-x

15. Angermeier, D., Wester, H., Beilke, K., Hansch, G., & Eichler, J. (2022). Security risk assessments: Modeling and risk level propagation. *ACM Transactions on Cyber-Physical Systems*. https://doi.org/10.1145/3569458