https://doi.org/10.31891/2219-9365-2024-80-21
УДК 004.023

ТІТОВА Віра
Хмельницький національний університет
https://orcid.org/0000-0001-8668-4834
e-mail: titovav@khmnu.edu.ua
КЛЬОЦ Юрій
Хмельницький національний університет
https://orcid.org/0000-0002-3914-0989
e-mail: klots@khmnu.edu.ua
ЛАКОЦЕНІН Захар
Хмельницький національний університет
e-mail: iqmaloyua@gmail.com
ШЛАПАК Олександра
Хмельницький національний університет
e-mail: sasaslapak839@gmail.com
ТРОЦ Віталій
Хмельницький національний університет
trotsvitalik@gmail.com

ПОРІВНЯЛЬНИЙ АНАЛІЗ МОДЕЛЕЙ АТАК НА ІНФОРМАЦІЙНУ БЕЗПЕКУ

В даній статті проведено аналіз існуючих на сьогоднішній день способів моделювання загроз інформаційної безпеки, зокрема атак.

На основі проведеного аналізу можна зробити висновки, що усі існуючі моделі атак мають низку загальних недоліків, а тому існує необхідність удосконалення та розробки нових методик визначення актуальних загроз безпеці інформації, що виключають існуючі недоліки.

Підвищити якість моделювання актуальних моделей загроз інформаційної безпеки можливо за рахунок визначення необхідних та достатніх показників та автоматизації процесу для виключення гіпотетичних помилок експертів.

Ключові слова: моделі безпеки, моделі атак, інформаційні системи, загрози інформаційної безпеки.

TITOVA Vira, KLOTS Yurii, LAKOTSENIN Zakhar, SHLAPAK Oleksandra
Khmelnitskyi National University

COMPARATIVE ANALYSIS OF MODELS OF ATTACKS ON INFORMATION SECURITYS

To ensure information security, it is necessary to: determine the goals and objectives of the information system; to investigate business processes in the information system (functional subsystems, modules and their functions); identify all users of the information system; roles and powers of users in the information system (access rights), a list of information technologies that ensure the execution of business processes (IT infrastructure, software, including information protection tools, models and methods of user access to the information system, etc.). Directly in the area of information security, it is necessary to determine the current violator in the information system, determine the list of current information security threats (information security threat modeling), design and implement an information security system (information protection system), as well as carry out on a regular basis a qualitative assessment of the effectiveness of the information protection system.

One of the most important tasks from the above is the choice of a method of modeling threats to information security and attacks on information systems, which is what this article is dedicated to.

Based on the analysis of information security threat modeling methods, it can be concluded that all existing attack models have a number of common shortcomings. It is possible to improve the quality of the definition (simulation) of current information security threat models by determining the necessary and sufficient indicators and automating the process to eliminate hypothetical errors of experts.

Keywords: security models, attack models, information systems, information security threats.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Інформаційна безпека в останні роки стає все більш значущою та важливою сферою національної безпеки багатьох розвинених країн світу та України зокрема. Розширення областей та сфер застосування інформаційних технологій значно розширює перспективи розвитку нових інформаційних загроз. Зарубіжні спеціальні служби розширюють свій вплив інформаційно-психологічного впливу, спрямованого на дестабілізацію внутрішньополітичної та соціальної ситуації в різних регіонах світу, що призводить до підриву суверенітету та порушення територіальної цілісності інших держав. Зростають масштаби комп'ютерної злочинності, насамперед у кредитно-фінансовій сфері. У сфері оборони країни, в галузі державної та громадської безпеки, в економічній сфері, в галузі науки, технологій та освіти, у галузі

стратегічної стабільності та рівноправного стратегічного партнерства спостерігаються визначені на рівні держави стратегічні цілі для забезпечення ефективного стану інформаційної безпеки.

Одночасно зі зростанням та розвитком інформаційних технологій розвиваються тактики, техніки та способи реалізації проведення атак, розширюється інструментарій для порушення стану інформаційної безпеки. Змінити ситуацію можна шляхом розробки нових підходів до забезпечення інформаційної безпеки, які можуть надати надійний захист від сучасних загроз безпеці інформації [1,2].

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Для забезпечення інформаційної безпеки необхідно: визначити цілі та завдання інформаційної системи (ІС); дослідити бізнес-процеси в ІС (функціональні підсистеми, модулі та їх функції); визначити всіх користувачів ІС; ролі та повноваження користувачів в ІС (права доступу), перелік інформаційних технологій, що забезпечують виконання бізнес-процесів (ІТ-інфраструктура, програмне забезпечення, у тому числі засоби захисту інформації, моделі та методи доступу користувачів до ІС тощо). Безпосередньо у частині інформаційної безпеки необхідно визначити актуального порушника в ІС, визначити перелік актуальних загроз безпеці інформації (моделювання загроз безпеці інформації), спроектувати та впровадити систему інформаційної безпеки (систему захисту інформації), а також проводити на регулярній основі якісну оцінку ефективності системи захисту інформації.

Однією з найважливіших завдань із перелічених є вибір способу моделювання загроз інформаційної безпеки (ЗІБ) та атак на ІС, чому і присвячена дана стаття.

ОГЛЯД ІСНУЮЧИХ РІШЕНЬ

Статичні моделі ЗІБ включають опис виявлених, аналіз вихідної захищеності ІС, опис можливих порушників, оцінку реалізованості та небезпеки загроз, перелік актуальних ЗІБ в ІС. Розробляються експертами власників ІС з урахуванням призначення, умов та особливостей функціонування ІС.

Статичні моделі ЗІБ мають такі недоліки [3,4]:

- недоліки експертних методів (експертних оцінок);
- розробляються на поточний стан ІС, у зв'язку з цим виникають складності у постійній актуалізації таких моделей у конкретні певний момент часу – проблема підтримки в актуальному стані моделі ЗІБ;
- не враховують усі необхідні показники при визначенні переліку актуальних ЗІБ, а саме: зміни до моделі ризиків (негативних наслідків від реалізації ЗІБ); зміна умов експлуатації об'єктів впливу (елементи архітектури ІС, що обробляють інформацію, що захищається); версійність ПЗ; способи реалізації тактик і технік атак, які динамічно розвиваються;
- не раціональне використання безлічі відомих баз даних ЗІБ, уразливостей, тактик та технік атак (MITRE ATT&CK, CVE, CWE, OSVDB, NVD, Secunia тощо);
- як наслідок, неякісна оцінка ефективності захищеності інформації (рівня захищеності ІС).

Згідно ДСТУ [5], комп'ютерна атака – цілеспрямований несанкціонований вплив на інформацію, ресурс автоматизованої інформаційної системи або отримання несанкціонованого доступу до них із застосуванням програмних або програмно-апаратних засобів.

Під об'єктом атаки (мета атаки) розуміється елемент ІС.

Порушник – будь-яка особа, яка навмисно використовує вразливості технічних та нетехнічних заходів та засобів контролю та управління безпекою з метою захоплення або компрометації інформаційних систем та мереж, або зниження доступності ресурсів інформаційної системи та мережевих ресурсів для законних користувачів.

В даний час існує безліч моделей атак, методів та засобів моделювання атак. Основні моделі атак на ІС представлені на рисунку 1.

ISSN 2219-9365

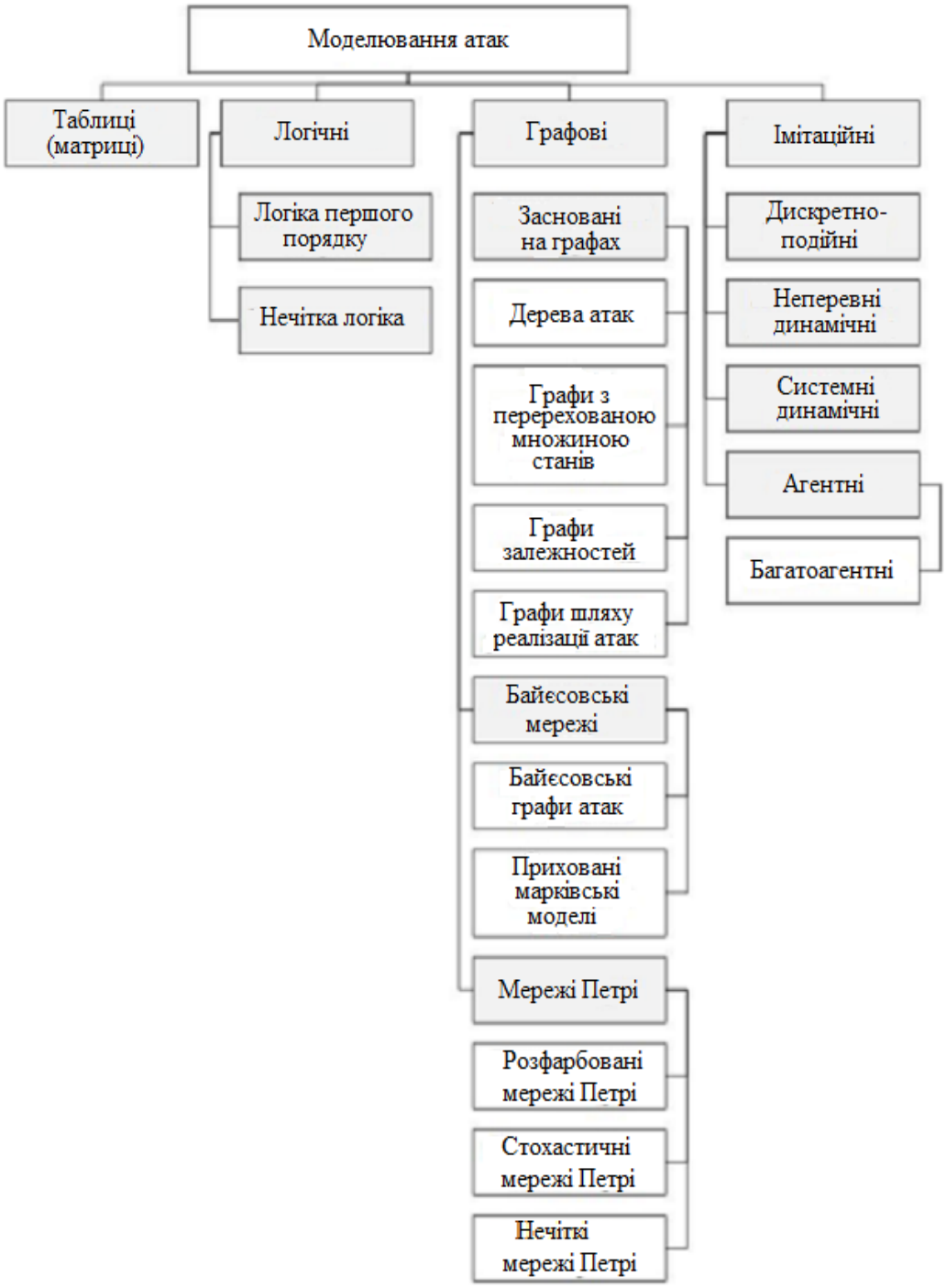

Рис. 1. Моделі атак на інформаційні системи

Переваги та недоліки основних моделей атак представлені у таблиці 1.

Отже, можна зробити висновок, що усі існуючі моделі атак мають низку загальних недоліків, а саме:

- складність моделювання;
- вимагають обчислювальних ресурсів;
- вимагають залучення висококваліфікованих фахівців у галузі інформаційної безпеки;
- помилки експертних методів (експертних оцінок).

На підставі проведеного аналізу можна зробити висновок про необхідність удосконалення та розробки нових методик визначення актуальних ЗІБ (моделювання ЗІБ), що виключають існуючі недоліки.

Таблиця 1

Переваги та недоліки моделей атак

№ п/п	Модель	Переваги	Недоліки
1.	**Табличні (Матричні)**	Найбільш прості	Складна при моделюванні циклічних атак, великої кількості зв'язків між інцидентами чи діями порушника.
2.	**Логічні**	Обробка інцидентів та використання мов уявлення знань про предметної галузі. Враховує випадки невизначеності вхідних даних про моделювані атаках	Використання спеціалізованого ПЗ, забезпечує механізми логічного висновку; Вимагає значних обчислювальних ресурсів
3.	**Графові**	Призначені для вирішення більшої кількості завдань, таких як «аналіз інцидентів, виявлення атак, оцінка ефективності захищеності інформації, визначення заходів щодо інформаційної безпеки, мінімізація ризиків та ресурсів для забезпечення інформаційної безпеки.	Масштабованість, пов'язана з формуванням графа для ІС з великою кількістю елементів
4.	**Графові на деревах атак**	Наочність, масштабованість, адаптованість, універсальність	Складні при моделюванні циклічних атак; Відсутність динамічного моделювання
5.	**Байєсовські графи**	Наочність, масштабованість, адаптованість, універсальність, враховує випадки невизначеності вхідних даних про атаки	Складні при моделюванні циклічних атак; Відсутність динамічного моделювання
6.	**Мережі Петрі**	Зручність моделювання динамічних та паралельних процесів, здатні відбивати ймовірнісні процеси, використання тимчасових параметрів, простота вивчення та використання, наявність великого кількості інструментальних засобів, можливість використання для аналізу різних аспектів інформаційної безпеки досліджуваної ІС	Нездатність описувати поведінку порушника та цілі атаки
7.	**Імітаційні**	Дозволяють моделювати поведінкові характеристики порушника та цілі атаки. Зручні для моделювання розподілених атак, мають широкий спектр інструментальних засобів	Вимагають великих обчислювальних ресурсів

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

В даній статті проведено аналіз існуючих на сьогоднішній день способів моделювання ЗІБ.

На основі проведеного аналізу можна зробити висновки, що усі існуючі моделі атак мають низку загальних недоліків. Основними з них є:

1. При моделюванні ЗІБ не завжди існує можливість виявлення нових якісних характеристик.
2. Будь-яка модель ЗІБ мінімізує пояснення можливих явищ.
3. Як правило, необхідних даних для налаштування моделей не вистачає.
4. Недоліки експертних методів (експертних оцінок).
5. Моделі ЗІБ розробляються на поточний стан ІС, у зв'язку з цим виникають складнощі у постійній актуалізації таких моделей ЗІБ.
6. Не враховують усі необхідні показники щодо переліку актуальних ЗІБ.
7. Не раціональне використання безлічі відомих баз даних ЗІБ, уразливостей, тактик та технік атак (MITRE ATT&CK, CVE, CWE, OSVDB, NVD, Secunia і т.д.).
8. Як наслідок, неякісна оцінка рівня захищеності ІС

Підвищити якість визначення (моделювання) актуальних моделей ЗІБ можливо за рахунок визначення необхідних та достатніх показників та автоматизувати процес для виключення гіпотетичних помилок експертів.

Література

1. Laptiev, S. (2022). Удосконалений метод захисту персональних даних від атак за допомогою алгоритмів соціальної інженерії. «Кібербезпека: освіта, наука, техніка», 4(16), 45–62. https://doi.org/10.28925/2663-4023.2022.16.4562.

2. Лєнков, С., Джулій, В., & Муляр, І. (2024). Метод оцінки ефективності безпеки конфіденційних даних розподіленої інформаційної системи. Pidvodni Tehnologii, 1(14), 18–34. https://doi.org/10.32347/uwt.2024.14.1201.

3. Mead, N., Shull, F., Vemuru, K., & Villadsen, O. A. Hybrid Threat Modeling Method. CMU/SEI-2018-TN-002. Software Engineering Institute, Carnegie Mellon University. 2018.

4. Khan, R.; McLaughlin, K.; Laverty, D.; & Sezer, Sakir. STRIDE-based Threat Modeling for Cyber-Physical Systems. In Proceedings of the 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe. 2017. DOI 10.1109/ISGTEurope.2017.8260283.

5. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. – Введ. 01.01.98. К.: Держстандарт України, 1998. 12 с.

References

1. Laptiev, S. (2022). Udoskonalenyi metod zakhystu personalnykh danykh vid atak za dopomohoiu alhorytmiv sotsialnoi inzhenerii. «Kiberbezpeka: osvita, nauka, tekhnika», 4(16), 45–62. https://doi.org/10.28925/2663-4023.2022.16.4562.

2. Lienkov, S., Dzhulii, V., & Muliar, I. (2024). Metod otsinky efektyvnosti bezpeky konfidentsiinykh danykh rozpodilenoi informatsiinoi systemy. Pidvodni Tehnologii, 1(14), 18–34. https://doi.org/10.32347/uwt.2024.14.1201.

3. Mead, N., Shull, F., Vemuru, K., & Villadsen, O. A. Hybrid Threat Modeling Method. CMU/SEI-2018-TN-002. Software Engineering Institute, Carnegie Mellon University. 2018.

4. Khan, R.; McLaughlin, K.; Laverty, D.; & Sezer, Sakir. STRIDE-based Threat Modeling for Cyber-Physical Systems. In Proceedings of the 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe. 2017. DOI 10.1109/ISGTEurope.2017.8260283.

5. DSTU 3396.2-97. Zakhyst informatsii. Tekhnichnyi zakhyst informatsii. Terminy ta vyznachennia. – Vved. 01.01.98. K.: Derzhstandart Ukrainy, 1998. 12