DOI: https://doi.org/10.25140/2411-5363-2026-1(43)-141-148
УДК 004.056:004.94

Інна Анатоліївна Ярова
кандидат технічних наук, доцент кафедри кібербезпеки та програмного забезпечення
Національний університет «Одеська політехніка» (Одеса, Україна)
E-mail: yarova@op.edu.ua. **ORCID:** https://orcid.org/0000-0001-7154-6674. **SCOPUS Autor ID:** 57209250106

ФОРМАЛІЗОВАНА МОДЕЛЬ ПОРУШНИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Дослідження присвячене проблемі формалізації моделі порушника інформаційної безпеки. Моделі порушника інформаційної безпеки призначені для використання в процесах управління захистом інформації в кіберпросторі. В роботі запропоновано концептуальну модель порушника у вигляді ER-моделі, яка є структурованою системою ознак із високим ступенем абстрагування. На її основі розроблено формалізовану модель порушника у вигляді деталізованої структурованої системи ознак порушника із множинами значень для кожної ознаки та з можливістю оцінки рівня загрози інформаційній безпеці, яка охоплює категорії як зовнішніх, так і внутрішніх порушників.

Ключові слова: *інформаційна безпека; концептуальна модель порушника; формалізована модель порушника; класифікаційна ознака; профіль порушника; рівень загрози*
Рис.: 2. Табл.: 3. Бібл.: 14.

Актуальність теми дослідження. Складність та масштаб загроз інформації демонструють стрімке зростання, тому традиційні методи інформаційної безпеки втрачають свою ефективність. Потрібні нові інструменти для розширення можливостей реагування на загрози в режимі реального часу. Актуальним завданням є створення методологій захисту інформації, які використовують існуючі джерела експертизи для стратегічного прогнозування загроз, спираючись на характеристики суб'єктів загроз. Перспективним напрямом є ризик-орієнтовані моделі захисту інформації з можливістю адаптації засобів захисту до специфіки інформаційно-комунікаційних систем (ІКС) з урахуванням мінливості ландшафту загроз кіберпростору. Нагальним завданням є втілення принципу «безпека з етапу проєктування», який полягає в інтегруванні концепцій інформаційної безпеки та кібербезпеки в процес створення і експлуатації інфраструктурних об'єктів, забезпечуючи проактивність систем кіберзахисту протягом всього життєвого циклу технічних систем.

Постановка проблеми. Ключовим аспектом стійкості комплексних систем захисту інформації (КСЗІ) є їх здатність передбачати потенційні атаки, виявляти зміни операційних обставин, а також формулювати нові вимоги у сфері захисту інформації. Саме це визначає актуальність задачі моделювання порушника інформаційної безпеки як суб'єкта загроз. Модель порушника інформаційної безпеки є обов'язковою складовою КСЗІ, її застосування при проєктуванні та експлуатації КСЗІ є вимогою державних нормативів. Проте в базових нормативних документах технічного захисту інформації, наприклад [1], відсутні методики, що чітко регламентують процес створення моделі порушника. Рекомендації щодо змісту та структури моделі порушника мають описовий характер і дозволяють розробити тільки неформалізовану модель порушника, самі нормативні документи певною мірою є морально застарілими.

Аналіз останніх досліджень і публікацій. Останніми роками спостерігається зростання уваги дослідників до питань, пов'язаних із порушниками інформаційної безпеки. Поширеним методом створення моделей порушника є математичне моделювання, а саме – логіко-імовірнісний підхід [2; 3]. Значна частина авторів обирає предметом дослідження одну з двох категорій порушників: або зовнішніх порушників, або внутрішніх. Причому спектр ознак та характеристик порушників зазвичай є доволі обмеженим та обирається виходячи з мети авторів дослідження [4; 5]. Моделюючи зовнішнього порушника, зазвичай вводять припущення про його високу кваліфікацію та обирають як кваліфікаційні ознаки можливості, тактики та методи, техніки та процедури, ресурси та інструменти. У тому випадку, коли у ролі зовнішнього порушника розглядається група осіб

із чітким розподілом обов'язків, для моделювання доцільно використовувати теорію графів [6]. Автори [3] вважають за необхідне розроблення для зовнішнього і внутрішнього порушника окремих моделей.

Значної уваги приділяється мотивації порушників: дослідження цього типу мають емпіричний характер, проводяться із використанням баз даних кіберінцидентів та пропонують аналітичні моделі [7; 8]. Слід пам'ятати, що зовнішні порушники завжди вчинюють свої дії свідомо, але внутрішні порушники не завжди мають за мету завдання шкоди. Для порушників з-поміж представників персоналу причиною кіберінцидентів розглядаються недбалість, втома, тиск часу, корпоративні взаємовідносини [9; 10].

Модерним напрямком досліджень є атрибуція та профілювання порушників безпеки із використанням штучного інтелекту [11]. Побудовані на цьому принципі предикативні моделі потребують навчання штучного інтелекту за певними алгоритмами, у тому числі за алгоритмами поведінки порушників [12].

Виділення недосліджених частин загальної проблеми. Модель порушника являє собою його абстрактний формалізований або неформалізований опис. Абстрактність опису передбачає зосередженість на загальних характеристиках, властивих різним категоріям порушників. Неформалізована модель є викладенням інформації у вільній формі, на основі характеристик ІКС, що досліджується. Така модель може доволі деталізовано відображати об'єкт дослідження, але не може бути узагальненою саме через унікальність даних, на яких її побудовано. Проведений аналіз публікацій демонструє, що питанню створення формалізованих описів порушника приділяється недостатньо уваги. Варто зазначити, що формалізовані моделі порушника, які пропонуються науковою спільнотою, враховують малу кількість класифікаційних ознак [13; 14]. З огляду на це, дослідження у сфері створення формалізованої моделі порушника з високим ступенем деталізації та різнобічною оцінкою рівнів загрози є перспективним напрямком.

Метою дослідження є розроблення формалізованої моделі порушника інформаційної безпеки як структурованої системи профілів порушника, сформованих за ознаками, що розглядаються за чітко визначеною послідовністю, з оцінкою рівня загрози інформаційній безпеці кожного профілю та ранжуванням профілів.

Виклад основного матеріалу. Модель порушника інформаційної безпеки для КСЗІ є окремим документом, що згідно із нормативами розробляється після обстеження середовища функціонування ІКС на основі переліку загроз інформації та переліку об'єктів захисту. Методологія розроблення формалізованої моделі порушника засновується на розумінні проблемної області й повинна забезпечувати універсальність підходів і придатність використання для ІКС довільного розміру та напрямку діяльності.

Основою для формалізованої моделі порушника є концептуальна модель, що являє собою структурований опис ознак порушника із високим ступенем абстрагування. Концептуальна модель висвітлює причинно-наслідкові зв'язки в предметній галузі і є проміжним етапом між вербальною та формалізованою моделями порушника.

Концептуальну модель порушника представлено у вигляді ER-моделі, що дозволяє наочно зобразити її структуру у вигляді діаграми «сутності» – «їх атрибути» – «зв'язки між сутностями». Суттєвою перевагою ER-моделі є наочна візуалізація, яка дозволяє швидко оптимізувати структуру моделі з виявленням зайвих або відсутніх ознак порушника, а також можливість конвертації в табличну форму, що надалі спрощує формалізацію самої моделі й алгоритмізацію процесу її створення.

Для концептуальної моделі порушника (рис. 1) обрано три сутності: «Порушник», «Прогнозовані дії», «Імовірний результат». Між сутностями розміщено два зв'язки: «Ви-

конує» та «Отримує». Таким чином, сутності разом зі зв'язками створюють логічний ланцюжок, який описує процес порушення інформаційної безпеки: «Порушник» – «Виконує» – «Прогнозовані дії» – «Отримує» – «Імовірний результат».

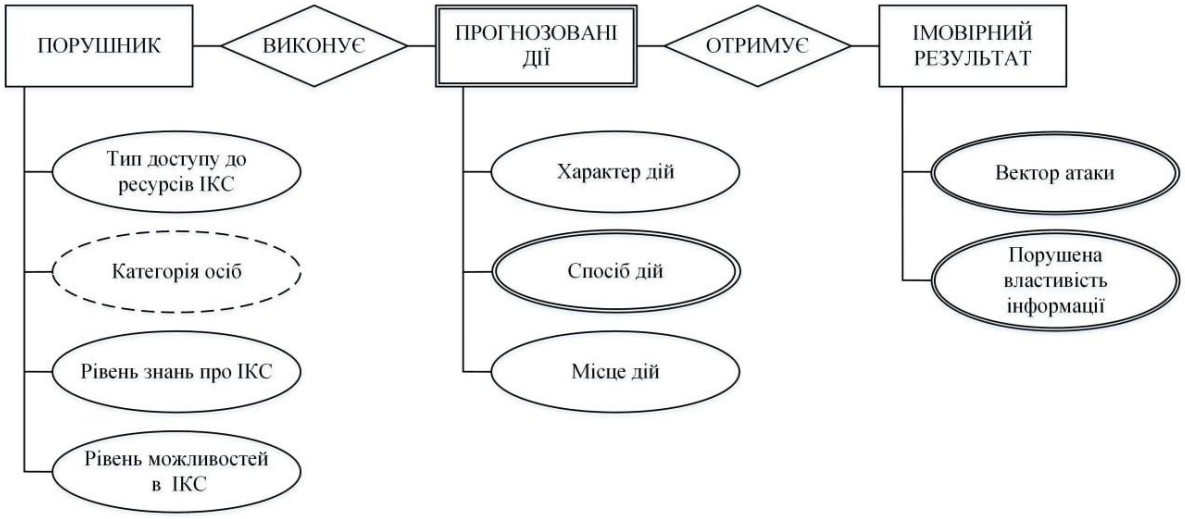

Рис. 1. Концептуальна модель порушника інформаційної безпеки
Джерело: розроблено автором.

Вихідною інформацією, яка використовується для опису порушника при створенні його концептуальної, а далі й формалізованої моделі, є ознаки порушника, що мають певні значення. Необхідно визначити атрибути сутностей, та призначити для кожного з них набори значень.

Ключовою в концептуальній моделі є сутність «Порушник», адже саме для опису порушника створюється формалізована модель. Обмеження на визначення для цієї сутності полягає в тому, що порушник – це особа або група осіб, які свідомо або несвідомо створює загрозу для ІКС. У такий спосіб виключено розгляд у ролі порушника будь-які випадкові події, які може нести загрозу для інформаційної системи. Вказана сутність є сильною: за значеннями її атрибутів можливим є однозначний опис порушника. Для сутності «Порушник» обрано такі атрибути: «Тип доступу до ресурсів ІКС», «Категорія осіб», «Рівень знать про ІКС», «Рівень можливостей в ІКС».

Атрибут «Тип доступу до ресурсів ІКС» є однозначним та може приймати одне з двох значень: «Зовнішній порушник» або «Внутрішній порушник». Це дозволяє в єдиній моделі охопити всі можливі категорії осіб-порушників, спрогнозувати їх дії та можливі наслідки порушень інформаційної безпеки. Атрибут «Категорія осіб» є похідним від атрибута «Тип доступу до ресурсів ІКС», його значення залежить від того, чи є порушник інформаційної безпеки зовнішнім або внутрішнім.

Сутність «Прогнозовані дії» призначена для опису імовірних дій порушника в інформаційній системі. Ця сутність є слабкою, оскільки значення її атрибутів залежать від значення атрибута «Тип доступу до ресурсів ІКС», ключової сутності моделі порушника. Для сутності «Прогнозовані дії» обрано однозначні атрибути «Характер дій», «Місце дій», та багатозначний атрибут «Спосіб дій».

Сутність «Імовірний результат» характеризує результат, який імовірно отримає порушник, реалізуючи загрозу. Ця сутність є сильною, оскільки незалежно від того, чи є порушник зовнішнім або внутрішнім, вона дає можливість чітко описати наслідки порушення інформаційної безпеки. Для сутності «Імовірний результат» призначено два багатозначні атрибути: «Вектор атаки» та «Порушена властивість інформації».

Розроблена концептуальна модель описує порушника інформаційної безпеки через взаємно пов'язані сутності, кожна з яких має власні атрибути. Вона є основою для розроблення формалізованої моделі порушника. Для перетворення концептуальної моделі у формалізовану модель необхідно виконати процес формалізації – представлення моделі у вигляді структурованої системи ознак порушника із множинами значень, які вводяться за чітко визначеною послідовністю.

Формалізована модель порушника інформаційної безпеки являє собою систему, складену з трьох блоків інформації – сутностей із атрибутами, що їм належать. Кожен атрибут має окремий набір значень, кожне значення в цьому наборі повинно мати власну оцінку рівня загрози за прийнятою шкалою (табл. 1). У розробленій концептуальній моделі обрано дев'ять атрибутів, кожен з яких має власний набір значень (табл. 2-4).

Таблиця 1 – Шкала оцінювання рівнів загрози інформаційної безпеки

Характеристика рівню загрози	Числове значення рівня загрози
Надзвичайно високий рівень загрози	5
Високий рівень загрози	4
Середній рівень загрози	3
Низький рівень загрози	2
Незначний рівень загрози	1

Джерело: розроблено автором

Таблиця 2 – Значення атрибута «Тип доступу до ресурсів ІКС»

Код значення	Значення атрибуту	Рівень загрози
ТД01	Зовнішній порушник	5
ТД02	Внутрішній порушник	4

Джерело: розроблено автором

Таблиця 3 – Значення атрибута «Порушена властивість інформації»

Код значення	Значення атрибуту	Рівень загрози
ПВ01	Порушення цілісності інформації	5
ПВ02	Порушення конфіденційності інформації	5
ПВ03	Порушення доступності інформації	4
ПВ04	Порушення спостереженості та керованості інформації	3
ПВ05	Несанкціоноване користування інформаційними ресурсами	2

Джерело: розроблено автором

Таблиця 4 – Значення атрибута «Характер дій»

Код значення	Значення атрибуту	Рівень загрози
ХД01	Використання засобів та заходів активного впливу на ІКС для зміни конфігурації системи	5
ХД02	Використання штатних засобів ІКС або недоліків проєктування КСЗІ для несанкціонованого доступу в систему	4
ХД03	Використання пасивних технічних засобів перехоплення інформаційних сигналів	3
ХД04	Використання виключно агентурних методів отримання інформації	2

Джерело: розроблено автором.

Для практичного використання важливим елементом формалізованої моделі порушника є кількісна оцінка сформованих профілів порушника. Результуюче значення рівня загрози для кожного профілю порушника визначається як добуток числових значень рівнів загрози всіх значень атрибутів моделі порушника. Воно є оцінкою рівня загрози для профілів порушників в розробленій формалізованій моделі. Один прохід по моделі із по-

слідовним вибором значень для кожного з атрибутів формує окремий профіль порушника. Сукупність сформованих профілів порушників являє собою результат використання формалізованої моделі порушника інформаційної безпеки.

Практичною реалізацією розробленої формалізованої моделі порушника інформаційної безпеки є програмний продукт, побудований як послідовність виконання скінченної кількості операцій вибору значень для заданих атрибутів – класифікаційних ознак порушника. Оптимальним способом представлення моделі порушника для практичного використання є подання в табличній формі, у вигляді зведеного переліку профілів порушників, з описом характеристик кожного профілю та з ранжуванням профілів за зменшенням рівня загрози інформаційній безпеці (рис. 2). Таке подання є зручним для практичного використання при проєктуванні та експлуатації КСЗІ або у процесах управління ризиками інформаційної безпеки.

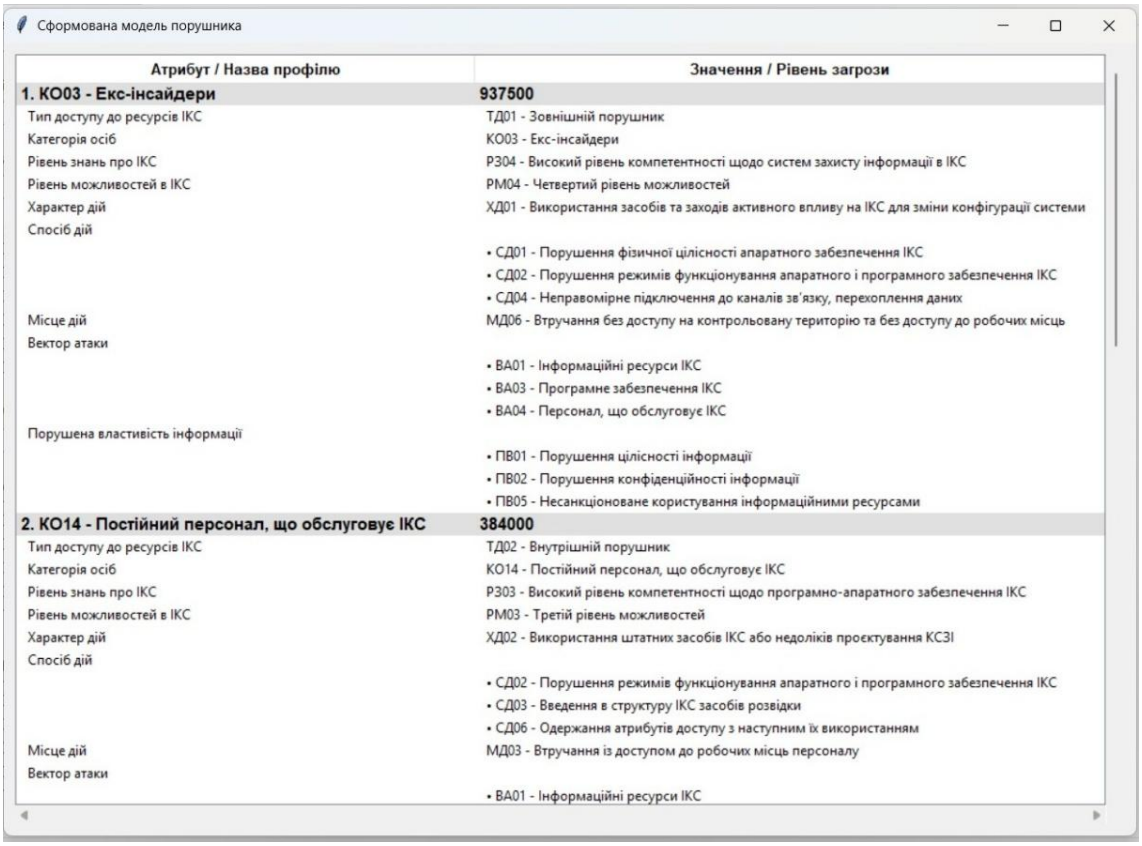

Рис. 2. Візуалізація формалізованої моделі порушника інформаційної безпеки: скріншот вікна програмного продукту

Джерело: розроблено автором.

Висновки. Спроможність вчасно розпізнати кібератаку та точно ідентифікувати порушника має ключове значення для визначення рівня загрози та вибору необхідних заходів захисту. Існуючи практики захисту інформації приділяють недостатньо уваги питанню моделювання порушників інформаційної безпеки як джерела загроз. Сучасна нормативна документація не пропонує уніфікованих підходів щодо розроблення моделі порушника. Визначення подібних підходів і формалізація методів побудови моделі порушника створюють передумови для підвищення адекватності систем технічного захисту інформації у процесі проєктування і подальшої комплексної оцінки їхньої ефективності під час функціонування. Актуальним завданням захисту інформації є реалізація принципу проактивної ідентифікації загроз, вчасного реагування та ефективного пом'якшення ризиків.

Розроблена модель порушника інформаційної безпеки – виконаний з високим ступенем формалізації деталізований опис осіб, що з певною імовірністю можуть здійснювати несанкціонований доступ до ІКС. У розробленій моделі задаються, враховуються та оцінюються ознаки цих осіб, в тому числі вперше – ознаки «Вектор атаки» та «Порушена властивість інформації». Опис порушника виконується за структурованою системою з дев'яти класифікаційних ознак, значення яких визначаються в заданій послідовності. Кожна ознака має власний набір значень з оцінкою рівня загрози для кожного значення. Результатом одноразового проходження по формалізованої моделі є формування профілю порушника із підсумковою оцінкою рівня загрози. Сукупність сформованих профілів можливих порушників, розташованих за зменшенням рівня загрози, є моделлю порушника в прикладному розумінні – саме вона використовується для систем захисту інформації згідно з вимогами НД ТЗІ.

Запропонована формалізована модель порушника інформаційної безпеки надає можливість урахувати тип доступу порушника до ІКС, та об'єднує в єдиному документі профілі як зовнішніх, так і внутрішніх порушників. Використання розробленої формалізованої моделі порушника підвищує ефективність захисту інформації за рахунок управління ризиками шляхом оцінки потенційних загроз на основі та контекстного аналізу. Отже, реалізуються результативний розподіл ресурсів захисту між критично важливими компонентами ІКС та оптимізація загальної стратегії безпеки.

Заява про використання генеративного ШІ та технологій на основі ШІ в процесі написання тексту статті

Під час проведення дослідження автор застосовувала Google Translator для огляду наукових публікацій в іноземних виданнях та перевірки граматики при перекладі анотації англійською мовою. Після використання Google Translator автор переглянула та відредагувала текст та бере на себе повну відповідальність за зміст публікації.

Список використаних джерел

1. Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. (2000). *Типове положення про службу захисту інформації в автоматизованій системі (НД ТЗІ 1.4-001-2000)*.

2. Dymova, H. O. (2025). Investigation of methods for improving intruderdetection efficiency in physical protection systems. *Таврійський науковий вісник, Серія: Технічні науки*, *3*, 75-84. https://doi.org/10.32782/tnv-tech.2025.3.9.

3. Пількевич, І. А., Бойченко, О. С., & Гуменюк, І. В. (2020). Удосконалення методу розробки логіко-імовірнісної моделі внутрішнього порушника. *Електронне моделювання, 42*(4), 71-85. 10.15407/emodel.42.04.071.

4. Tatam, M., Shanmugam, B., Azam, S., & Kannoorpatti, K. (2021). A review of threat modelling approaches for APT-style attacks. *Heliyon,* 7, 1. https://doi.org/10.1016/j.heliyon.2021.e05969.

5. Liu, Y., Li, S., Wang, X., & Xu, L. (2024). A Review of Hybrid Cyber Threats Modelling and Detection Using Artificial Intelligence in IIoT. *Computer Modeling in Engineering & Sciences*, 140(2), 1233-1261. https://doi.org/10.32604/cmes.2024.046473.

6. Браіловський, М. М., Зибін, С. В., Кобозєва, А. А., Хорошко, В. О., & Хохлачова Ю. Є. (2021). *Аналіз кіберзахищенності інформаційних систем*. ФОП Ямчинський О. В.

7. Pseftelis, T., & Chondrokoukis, G. (2025). Cyber Attack Motivations: Connecting Actors with Event Types. Preprints. https://doi.org/10.20944/preprints202505.1003.v1.

8. Kaiser, F., Wiens, M., & Schultmann, F. (2021). Motivation-based Attacker Modelling for Cyber Risk Management: A Quantitative Content Analysis and a Natural Experiment, *Journal of Information Security & Cybercrimes Research*, 4(2), 132-147. https://doi.org/10.26735/NMMD9869.

9. Colabianchi, S., Costantino, F., Nonino, F., & Palombi, G. (2025). Transforming threats into opportunities: The role of human factors in enhancing cybersecurity. *Journal of Innovation & Knowledge,* 10 (3). https://doi.org/10.1016/j.jik.2025.100695.

10. Haag, S., Siegfried, N., & Winkler, N. (2025). Informal control responses to information security policy violations: A factorial survey on insurance employees' moral licensing of insider threats. *Computers & Security,* 157. https://doi.org/10.1016/j.cose.2025.104575.

11. Irshad, E., & Basit Siddiqui, A. (2023). Cyber threat attribution using unstructured reports in cyber threat intelligence. *Egyptian Informatics Journal,* 24(1), 43-59. https://doi.org/10.1016/j.eij.2022.11.001.

12. Beauden, J. (2025). Integrating Machine Learning with Threat Hunting: A Predictive Model for Real-Time Cyber Threat Detection and Response. https://www.researchgate.net/publication/394098833_Integrating_Machine_Learning_with_Threat_Hunting_A_Predictive_Model_for_Real-Time_Cyber_Threat_Detection_and_Response.

13. Снєосіков, О. А., & Нарєжній, О. П. (2025). Моделі загроз та порушника автономної системи диференціальної корекції глобальних навігаційних супутникових систем. *Вісник ХНТУ,* 3(94), 2, 423-434. https://doi.org/10.35546/kntu2078-4481.2025.3.2.54.

14. Комаров, М. Ю., Ониськова, А. В., & Гончар, С. Ф. (2018). Аналіз і дослідження моделі порушника безпеки інформації для захищеного вузла Інтернет доступу. *Вчені записки ТНУ ім. В. І. Вернадського: Технічні науки,* 29(68), 1, 5, 138-142. https://tech.vernadskyjournals.in.ua/journals/2018/5_2018/part_1/26.pdf.

References

1. Departament spetsialnykh telekomunikatsiinykh system ta zakhystu informatsii Sluzhby bezpeky Ukrainy. (2000). [Department of Special Telecommunications Systems and Information Protection of the Security Service of Ukraine. (2000).] *Typove polozhennia pro sluzhbu zakhystu informatsii v avtomatyzovanii systemi (ND TZI 1.4-001-2000)- Standard provisions on information protection services in automated systems (ND TZI 1.4-001-2000).*

2. Dymova, H. O. (2025). Investigation of methods for improving intruderdetection efficiency in physical protection systems. *Tavriiskyi naukovyi visnyk, Seriia: Tekhnichni nauky – Tavria Scientific Bulletin, Series: Technical Sciences, 3,* 75-84. https://doi.org/10.32782/tnv-tech.2025.3.9.

3. Pilkevych, I. A., Boichenko, O. S., & Humeniuk, I. V. (2020). Udoskonalennia metodu rozrobky lohiko-imovirnisnoi modeli vnutrishnoho porushnyka [Improving the method of developing a logical-probabilistic model of an internal violator]. *Elektronne modeliuvannia – Electronic modeling, 42*(4), 71-85. 10.15407/emodel.42.04.071.

4. Tatam, M., Shanmugam, B., Azam, S., & Kannoorpatti, K. (2021). A review of threat modelling approaches for APT-style attacks. *Heliyon, 7,* 1. https://doi.org/10.1016/j.heliyon.2021.e05969.

5. Liu, Y., Li, S., Wang, X., & Xu, L. (2024). A Review of Hybrid Cyber Threats Modelling and Detection Using Artificial Intelligence in IIoT. *Computer Modeling in Engineering & Sciences,* 140(2), 1233-1261. https://doi.org/10.32604/cmes.2024.046473.

6. Brailovskyi, M. M., Zybin, S. V., Kobozieva, A. A., Khoroshko, V. O., & Khokhlachova, Yu. Ye. (2021). *Analiz kiberzakhyshchennosti informatsiinykh system* [*Analysis of cybersecurity of information systems*]. FOP Yamchynskyi O. V.

7. Pseftelis, T., & Chondrokoukis, G. (2025). Cyber Attack Motivations: Connecting Actors with Event Types. Preprints. https://doi.org/10.20944/preprints202505.1003.v1.

8. Kaiser, F., Wiens, M., & Schultmann, F. (2021). Motivation-based Attacker Modelling for Cyber Risk Management: A Quantitative Content Analysis and a Natural Experiment, *Journal of Information Security & Cybercrimes Research*, 4(2), 132-147. https://doi.org/10.26735/NMMD9869.

9. Colabianchi, S., Costantino, F., Nonino, F., & Palombi, G. (2025). Transforming threats into opportunities: The role of human factors in enhancing cybersecurity. *Journal of Innovation & Knowledge,* 10 (3). https://doi.org/10.1016/j.jik.2025.100695.

10. Haag, S., Siegfried, N., & Winkler, N. (2025). Informal control responses to information security policy violations: A factorial survey on insurance employees' moral licensing of insider threats. *Computers & Security,* 157. https://doi.org/10.1016/j.cose.2025.104575.

11. Irshad, E., & Basit Siddiqui, A. (2023). Cyber threat attribution using unstructured reports in cyber threat intelligence. *Egyptian Informatics Journal,* 24(1), 43-59. https://doi.org/10.1016/j.eij.2022.11.001.

12. Beauden, J. (2025). Integrating Machine Learning with Threat Hunting: A Predictive Model for Real-Time Cyber Threat Detection and Response. https://www.researchgate.net/publication/394098833_Integrating_Machine_Learning_with_Threat_Hunting_A_Predictive_Model_for_Real-Time_Cyber_Threat_Detection_and_Response.

13. Snieosikov, O. A., & Nariezhnii, O. P. (2025). Modeli zahroz ta porushnyka avtonomnoi systemy dyferentsialnoi korektsii hlobalnykh navihatsiinykh suputnykovykh system [Threat and intruder models of the autonomous differential correction system of global navigation satellite systems]. *Visnyk KhNTU – Bulletin of KhNTU,* 3(94), 2, 423-434. https://doi.org/10.35546/kntu2078-4481.2025.3.2.54

14. Komarov, M. Yu., Onyskova, A. V., & Honchar, S. F. (2018). Analiz i doslidzhennia modeli porushnyka bezpeky informatsii dlia zakhyshchenoho vuzla Internet dostupu [Analysis and research of information security violator model for a protected Internet access node]. *Vcheni zapysky TNU im. V. I. Vernadskoho: Tekhnichni nauky – Scientific notes of V. I. Vernadsky TNU. Series: Technical Sciences,* 29(68), 1, 5, 138-142. https://tech.vernadskyjournals.in.ua/journals/2018/5_2018/part_1/26.pdf.

Дата першого надходження статті до видання: 24.12.2025
Дата прийняття статті до друку після рецензування: 12.01.2026

УДК 004.056:004.94

Inna Yarova

PhD, Associate Professor, Department of Cybersecurity and Software
Odesa Polytechnic National University (Odesa, Ukraine)
E-mail: yarova@op.edu.ua. **ORCID:** https://orcid.org/0000-0001-7154-6674. **SCOPUS Autor ID:** 57209250106

FORMALIZED MODEL OF INFORMATION SECURITY VIOLATOR FOR INFORMATION PROTECTION SYSTEMS

The study is devoted to the problem of formalizing the model of information security violator. The model of information security violator is a mandatory component of comprehensive information protection systems in the digital space as an element of information security risk management. According to the risk-oriented approach, the violator model should be proactive, and should be used throughout the life cycle of information-communication systems, from the design stage to the decommissioning stage.

Based on the analysis of regulatory documentation in the field of technical information protection, it was established that there is no single standardized methodology for developing the violator model. Existing methodologies are of a recommendatory nature and make it possible to develop only an informal description of information security violator, with a small number of features and without a numeric assessment of threat level. The analysis of scientific papers demonstrates the unilateral approach in this field and confirms the relevance of chosen research topic.

The conceptual model of information security violator in the form of the ER-model is proposed, which is a structured system of violator characteristics with a high degree of abstraction. Based on it, a formalized model of information security violator is developed in the form of a detailed structured system of violator characteristics with the sets of value for each characteristic and with assessment of the level of information security threat for each characteristic.

The outcome from the developed model of information security violator is generation of a set of profiles of potential violators with an assessment of the overall threat level for each violator profile and with ranking of profiles by decreasing of their overall threat level. The developed model of information security violator enables to generate profiles both for external and internal user violators. In generation a violator profile, nine classification features are taken into account, including the first proposed features "The Attack Vector" and "Violated Information Property". The proposed formalized model of information security violator provides the prerequisites for effective visualization of modeling results. On its basis, a software product for practical use can be designed.

Keywords: *information security; conceptual model of information security violator; formalized model of information security violator; profile of violator; classification feature; threat level.*

Fig.: 2. Table: 3. References: 14.

Ярова І. А. Формалізована модель порушника інформаційної безпеки для систем захисту інформації. *Технічні науки та технології.* 2026. № 1(43). С. 141-148. DOI: https://doi.org/10.25140/2411-5363-2026-1(43)-141-148.