Інформаційні технології, кібербезпека та комп'ютерна інженерія

МОДЕЛЬ ПОТЕНЦІЙНОГО ПОРУШНИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ЦИФРОВОМУ СВІТІ

Шаповалова Олена Олександрівна
к.т.н., доцент, доцент кафедри кібербезпеки
та інформаційних технологій
olena.shapovalova@hneu.net
Луговий Богдан Владиславович
здобувач першого (бакалаврського)
рівня вищої освіти
bodya051105@gmail.com
кафедра кібербезпеки
та інформаційних технологій
Харківський національний економічний
університет імені Семена Кузнеця, Україна

У сучасному цифровому світі, який характеризується стрімким зростанням обсягу даних, розширенням кіберпростору та глобальною інтеграцією інформаційних систем, рівень кіберзагроз зростає геометрично. Швидкий розвиток цифрових технологій створює не лише нові можливості для суспільства й бізнесу, але й відкриває широкий спектр шляхів для потенційних порушників інформаційної безпеки. Сучасні кіберзлочинці стають більш ресурсними, організованими, мотивованими та технологічно підготовленими, використовуючи широкий інструментарій – від соціальної інженерії до складних багаторівневих APT-атак, здатних обходити традиційні системи захисту. У цих умовах ефективний кіберзахист уже не може обмежуватися лише аналізом технічних вразливостей. Він потребує системного й прогностичного підходу, заснованого на глибокому розумінні моделі потенційного порушника – його цілей, ресурсів, поведінкових стратегій, рівня компетентності та очікуваної вигоди.

Провідні світові дослідження, у яких прямо або опосередковано розглядається модель порушника інформаційної безпеки (attacker modelling, attacker profiling, APT/insider modelling, threat actor attribution), показують, що математичні моделі порушника відіграють ключову роль у побудові комплексних систем захисту та прогнозуванні кіберінцидентів. Науковці аналізують як технічні, так і поведінкові параметри кіберзлочинців, створюючи багатовимірні моделі потенційного порушника у цифровому середовищі. У роботі E. Irshad та A. B. Siddiqui особливий акцент робиться на побудові моделей порушника на основі неструктурованих джерел розвідки загроз. Автори демонструють, що автоматичне вилучення поведінкових та технічних ознак із CTI-звітів дозволяє створювати точні профілі threat actors, підвищуючи рівень атрибуції кібератак та покращуючи прогнозування їхніх наступних дій [1]. Комплексний огляд досліджень APT-груп подають N. Rani

та співавтори, які аналізують сучасні підходи до атрибуції та поведінкового аналізу високоресурсних зловмисників. У роботі узагальнено моделі, що поєднують тактичні патерни ATT&CK, часові характеристики атак, інструментарій груп та їхні стратегічні цілі [2]. Подібну увагу до структурного моделювання атак демонструє B. Stojanović, який акцентує на ролі спеціалізованих датасетів у побудові реалістичних сценаріїв поведінки APT та підготовці алгоритмічних моделей прогнозування [3].

Досить вагомий напрям становлять дослідження інсайдерських загроз. Так, Y. Wei пропонує модель на основі каскадних автокодерів, яка відтворює нормальні поведінкові патерни співробітників і виявляє потенційних внутрішніх порушників шляхом ідентифікації аномалій. Модель порушника в цьому випадку формується як відхилення від статистичної норми, що робить її універсальною для корпоративних середовищ [4].

Важливою складовою сучасного розуміння моделей порушника є психологічний аспект. Дослідження U. Hani та ін. демонструє, що профілювання хакерів може базуватися не лише на технічних ознаках, а й на психологічних характеристиках. На основі моделі Big Five автори формують прогностичні ML-моделі, які дозволяють передбачати типи кіберповедінки залежно від особистісних параметрів [5].

Додаткові можливості для формування моделі порушника розглянуті у статтях D. T. Salim та співавторів, де узагальнено методи аналізу APT, зокрема техніки послідовного відстеження тактик, інструментів та процедур (TTPs). Автори наголошують на важливості інтеграції поведінкових ознак у багатокомпонентну модель порушника [6].

Сучасні тенденції розвитку штучного інтелекту переглядають традиційні підходи до моделювання загроз. У роботі S. A. Alansary підкреслюється, що AI-дрівен порушники діють набагато динамічніше й складніше, використовуючи генеративні моделі для автоматизації атак. Це вимагає нової парадигми моделювання зловмисника, що включає адаптивність, навчання та здатність до самостійного пошуку вразливостей [7].

Таким чином, сучасний науковий дискурс у сфері інформаційної безпеки засвідчує, що модель порушника перестала бути суто технічною конструкцією. Вона еволюціонувала у багаторівневу систему, що інтегрує поведінкові, психологічні, організаційні, технічні та інтелектуальні характеристики зловмисника. Це дозволяє формувати більш точні механізми прогнозування та підвищувати ефективність кіберзахисту в умовах швидкозмінного цифрового середовища.

У цьому контексті виникає необхідність створення формалізованої та водночас гнучкої математичної моделі потенційного порушника інформаційної безпеки, яка здатна інтегрувати як числові, так і нечіткі параметри, відображати реальні умови цифрового середовища та забезпечувати кількісну оцінку рівня загрози.

Метою статті є розробка такої моделі, що дозволить більш повно описати ймовірну поведінку порушника, враховуючи його ресурси, рівень

компетентності, мотивацію, очікувану вигоду, можливі ризики, характер цілей атаки та стратегічні особливості взаємодії з системою захисту. Запропонований підхід спрямований на поглиблення теоретичних основ вивчення кіберзагроз та створення практичного інструменту для прогнозування атак і підвищення ефективності систем кіберзахисту у цифровому світі.

У сучасному цифровому середовищі порушник інформаційної безпеки розглядається не лише як технічний агент, здатний виконувати шкідливі дії над інформаційними активами, а як складний раціональний суб'єкт, що оптимізує власні дії з урахуванням очікуваного виграшу, витрат, доступних ресурсів та ймовірної протидії системи захисту.

М. В. Капустян, С. В. Орленко та В. О. Хорошко визначають модель порушника як абстрактне формалізоване або неформалізоване описання його можливих дій, що враховує практичні й теоретичні спроможності, наявні знання, часові й просторові умови реалізації атаки. У межах автоматизованих систем порушник може бути як внутрішнім, так і зовнішнім, що визначає різний рівень доступу, кваліфікації та потенційної небезпеки.

Відповідно до підходу авторів, модель порушника повинна включати чотири ключові компоненти: мету порушника та її градацію за рівнем небезпеки для інформаційної системи; категорії осіб, серед яких може бути зловмисник (користувачі, адміністратори, сторонні суб'єкти тощо); оцінку кваліфікації, що охоплює рівень знань у галузі обчислювальної техніки, програмування, проектування та експлуатації АС; прогнозування характеру дій, які зловмисник здатний реалізувати залежно від своїх технічних можливостей та доступу до компонентів системи [8].

Згідно з підходом М. Будька, модель порушника повинна комплексно описувати потенційного зловмисника, охоплюючи низку ключових характеристик, необхідних для аналізу загроз та побудови ефективної системи захисту. Передусім вона має визначати категорії осіб, серед яких може виникнути порушник, а також рівень його можливостей, що включає наявні ресурси та доступ до елементів автоматизованої системи. Важливими є припущення щодо кваліфікації та рівня знань зловмисника, що впливають на його здатність використовувати вразливості та недоліки системи. Модель повинна враховувати методи й способи, які можуть застосовуватися під час здійснення порушень, а також можливу мету порушника, ранжовану за ступенем небезпечності для інформаційної системи. Крім того, важливими є оцінка потенційних місць реалізації атак, можливих способів здійснення загроз та характеру дій, які зловмисник потенційно здатний виконати. Такий підхід забезпечує всебічне уявлення про поведінку порушника та створює основу для побудови адекватних моделей ризику й систем протидії [9].

Проведений аналіз дозволив сформувати такі ключові аспекти, що характеризують потенційного порушника інформаційної безпеки: компетентність порушника (рівень технічних навичок); набір доступних ресурсів (обчислювальні, часові, фінансові); мотивацію та цілі (матеріальні,

політичні, особисті); ризики, які зловмисник готовий прийняти; стратегію протидії захисним механізмам; а також динамічність поведінки в умовах невизначеності. Формалізація цих характеристик забезпечує можливість аналітичного прогнозування ймовірності атаки, оцінки її інтенсивності та раннього виявлення підготовчих дій порушника, що є критично важливим для побудови проактивних систем кіберзахисту.

Модель потенційного порушника ґрунтується на формалізації його ресурсних можливостей, мотиваційних чинників та поведінкових стратегій у цифровому середовищі. Нехай порушник описується впорядкованою множиною параметрів:

$$A=\{C, R, M_r, U, R_{isk}, S, P\},$$

де C – рівень компетентності;
R – доступні технічні, часові та фінансові ресурси;
M_r – мотивація (економічна, політична, ідеологічна);
U – очікувана вигода від атаки;
R_{isk} – прийнятний рівень ризику;
S – стратегія обходу захисту;
P – поведінкові патерни (динаміка дій, стиль атаки, стохастичні особливості).

Компетентність та ресурси визначають простір можливих дій порушника:

$$A_s=f(C,R),$$

де A_s – множина допустимих атакувальних дій.

Очікувана корисність зловмисника для конкретної атаки визначається:

$$U_A=M_r \cdot U - R_{isk} \cdot L,$$

де L – оцінка можливих втрат порушника (ймовірність викриття, юридичні наслідки, витрати).

Порушник ініціює атаку, якщо:

$$U_A>\theta,$$

де θ – порогове значення раціональності зловмисника.

Стратегія порушника моделюється як оптимізаційна задача:

$$S^* = arg \max_{S \in \Omega} E[U_A(S)],$$

де Ω – множина можливих стратегій, включно з соціальною інженерією, експлуатацією вразливостей, APT-тактиками тощо.

Для динамічних атак використовується марковський підхід, де стан системи безпеки X_t та стан порушника A_t еволюціонують як:

$$P(X_{t+1},A_{t+1}|Xt,At)=T,$$

де T – матриця ймовірностей переходів, побудована на основі поведінкових патернів порушника.

Додатково нечіткі множини застосовуються для моделювання невизначеності мотивації та ризикової поведінки:

$$M_r=m(\mu),\ R_{isk}=r(\lambda),$$

де μ та λ– функції належності, що описують нечіткі стани.

Таким чином, модель дозволяє оцінювати здатність порушника здійснювати атаку, прогнозувати його дії та будувати проактивні стратегії кіберзахисту на основі формалізованих характеристик та ймовірнісних переходів між станами.

У ході дослідження сформовано комплексний підхід до моделювання потенційного порушника інформаційної безпеки в умовах сучасного цифрового середовища, яке характеризується високою динамічністю, невизначеністю та зростанням рівня кіберзагроз. Проведений аналіз сучасних наукових джерел засвідчує, що традиційні уявлення про зловмисника як про суто технічного агента вже не відповідають реаліям кіберпростору. Натомість порушник сьогодні є раціональним, адаптивним, ресурсним суб’єктом, здатним оптимізувати власну поведінку відповідно до очікуваної вигоди, доступних ресурсів, можливих ризиків та умов протидії систем захисту.

Розроблена модель інтегрує технічні, поведінкові, психологічні та стратегічні характеристики зловмисника, що дозволяє набагато повніше оцінювати його можливості й мотиви. Формалізація ключових параметрів, а саме компетентності, ресурсів, мотивації, прийнятного ризику, поведінкових патернів і стратегій, забезпечує побудову математично обґрунтованої структури, придатної для кількісного аналізу кіберзагроз. Поєднання апарату функцій корисності, оптимізаційних моделей та марковських процесів дає змогу описати динамічну взаємодію між порушником і системою захисту в умовах невизначеності.

Важливим результатом дослідження є обґрунтування того, що ефективний кіберзахист у сучасних умовах має спиратися не лише на технічний аналіз уразливостей, але й на глибоке розуміння поведінкових та стратегічних характеристик кіберзлочинців. Модель порушника, що інтегрує багатовимірні параметри, стає ключовим елементом проактивних систем безпеки, здатних адаптуватися до змін у ландшафті загроз.

У подальших дослідженнях доцільно зосередитися на практичній валідації моделі на реальних інцидентах, синтетичних APT-datasetax та поведінкових логах, а також розробити алгоритмічні засоби автоматичного наповнення моделі на основі даних розвідки загроз (CTI). Додатковим напрямом є інтеграція елементів штучного інтелекту для формування

адаптивних моделей порушника, що здатні до самооновлення та оперативного врахування нових тенденцій у кіберзлочинності.

References

1. Irshad, E., & Siddiqui, A. B. (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
2. Rani, N., Saha, B., & Shukla, S. K. (2025). A comprehensive survey of automated Advanced Persistent Threat attribution: Taxonomy, methods, challenges and open research problems. *Journal of Information Security and Applications, 92*, 104076. https://doi.org/10.1016/j.jisa.2025.104076
3. Stojanović, B., Hofer-Schmitz, K., & Kleb, U. (2020). APT datasets and attack modeling for automated detection methods: A review. *Computers & Security, 92*, 101734. https://doi.org/10.1016/j.cose.2020.101734
4. Wei, Y., Chow, K.-P., & Yiu, S.-M. (2021). Insider threat prediction based on unsupervised anomaly detection scheme for proactive forensic investigation. *Forensic Science International: Digital Investigation, 38*, 301126. https://doi.org/10.1016/j.fsidi.2021.301126
5. Hani, U., Sohaib, O., Khan, K., & Aleidi, A. (2024). Psychological profiling of hackers via machine learning toward sustainable cybersecurity. *Frontiers in Computer Science, 6*, Article 1381351. https://doi.org/10.3389/fcomp.2024.1381351
6. Salim, D. T., Singh, M. M., & Keikhosrokiani, P. (2023). A systematic literature review for APT detection and Effective Cyber Situational Awareness (ECSA) conceptual model. *Heliyon, 9*(7), e17156. https://doi.org/10.1016/j.heliyon.2023.e17156
7. Alansary, S. A., Ayyad, S. M., Talaat, F. M., & Saafan, M. M. (2025). Emerging AI threats in cybercrime: A review of zero-day attacks via machine, deep, and federated learning. *Knowledge and Information Systems, 67*, 10951–10987. https://doi.org/10.1007/s10115-025-02556-6
8. Капустян, М. В., Орленко, С. В., & Хорошко, В. О. (2006). Створення моделі загроз інформації та механізму її ефективного захисту. *Вісник Національного університету "Львівська політехніка"*, № 551: Автоматика, вимірювання та керування. С. 58–63.
9. Будько, М. (2005). Методика оцінки загроз для інформації автоматизованих систем. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: науково-технічний збірник*. Вип. 10. С. 35–46.

Відомості про авторів, які взяли участь у 5-й Міжнародній науково-практичній конференції «Scientific Exploration: Bridging Theory and Practice», 20-22 жовтня 2025, Берлін, Німеччина

Прізвище ім'я по-батькові	Автор 1	Шаповалова Олена Олександрівна
	Автор 2	Луговий Богдан Владиславович
Для сертифікату Ім'я та Прізвище латинськими літерами	Автор 1	Shapovalova Olena
	Автор 2	Luhovyi Bohdan
	Автор 3	
Заклад вищої освіти або організація	Автор 1	Харківський національний економічний університет імені Семена Кузнеця, Україна
	Автор 2	Харківський національний економічний університет імені Семена Кузнеця, Україна
Науковий ступінь та вчене звання Для здобувачів вищої освіти рівень (бакалавр / магістр)	Автор 1	К.т.н., доцент
	Автор 2	бакалавр
Назва кафедри	Автор 1	Кафедра кібербезпеки та інформаційних технологій
	Автор 2	Кафедра кібербезпеки та інформаційних технологій
E-mail	Автор 1	olena.shapovalova@hneu.net
	Автор 2	bodya051105@gmail.com
Назва секції (обов'язково)		Інформаційні технології, кібербезпека та комп'ютерна інженерія
Паперова версія сертифікату з мокрою печаткою та підписом (оплачується окремо)	Автор 1	Ні
	Автор 2	Ні
Дані для відправлення паперової версії сертифікату Новою поштою ПІБ Номер телефону Назва міста відділення №		Заповнюється тільки у разі замовлення друкованого сертифікату