УДК 330.865

А. Свердлова

ДО ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ АСИМЕТРІЇ В АНАЛІТИЦІ РИНКУ РІШЕНЬ ТА ПОСЛУГ З КІБЕРБЕЗПЕКИ

Державний університет інтелектуальних технологій і зв'язку

Анотація.

У роботі звернено увагу на те, що на сьогодні існує не тільки проблема інформаційної асиметрії на ринку послуг та рішень з кібербезпеки, а й у сфері аналітики, присвяченій цьому ринку. На основі вивчення різних існуючих підходів до класифікації ринку послуг та рішень з кібербезпеки, які часто є суперечливими або неповними, було запропоновано авторське бачення поділу цього ринку на категорії/сегменти відповідно до сучасних реалій.

Ключові слова: інформаційна асиметрія, аналітика, ринок рішень та послуг з кібербезпеки, класифікація.

Abstract.

The study draws attention to the fact that, today, there is not only a problem of information asymmetry in the market for cybersecurity services and solutions but also in the field of analytics dedicated to this market. Based on the analysis of various existing approaches to the classification of the cybersecurity services and solutions market – which are often contradictory or incomplete – the author proposes a new perspective on categorizing this market into segments that reflect current realities.

Keywords: information asymmetry, analytics, market for cybersecurity solutions and services, classification.

Вступ

У сучасному цифровому світі кіберзагрози стають дедалі складнішими та масовішими. Щодня мільйони даних піддаються ризику через хакерські атаки, витоки інформації та шкідливе програмне забезпечення. За даними Cybersecurity Ventures, у 2024 році світові збитки від кіберзлочинів очікуються на рівні 9,5 трлн доларів США [1]. У дослідженні [2] було виявлено, що комп'ютери, які підключені до Інтернету зазнають, в середньому 2244 атаки на день, що еквівалентно одній атаці кожні 39 секунд. Згідно звіту IBM Security Report 2024 [3], більш ніж 68% компаній по всьому світу за останній рік зазнали хоча б одного інциденту безпеки або витоку даних.

Отже, сьогодні кібербезпека вже перестала бути лише IT-проблемою – вона стала критичним елементом національної, корпоративної та персональної безпеки.

Наразі, в умовах стрімкого розвитку цифрових технологій, кібербезпека набуває критичного значення як для окремих підприємств, так і для цілих держав. Зростаюча залежність економіки від інформаційних та комунікаційних технологій супроводжується збільшенням кількості кіберзагроз, а це, своєю чергою, стимулює активний розвиток ринку послуг та рішень з кібербезпеки.

Водночас, глибоке і якісне дослідження цього ринку наштовхується на низку проблем. Однією з головних проблем дослідження ринку кібербезпеки є інформаційна асиметрія, що призводить до спотворення аналітики, економічних прогнозів і стратегічних рішень. Метою цієї роботи є звернення уваги на проблему інформаційної асиметрії під час вивчення ринку послуг та рішень з кібербезпеки.

Результати дослідження

Зазвичай інформаційна асиметрія розглядається як ситуація на ринку, коли одні учасники мають більше або якіснішу інформацію, ніж інші, що призводить до неефективності, викривлення конкуренції та ін. Це «класична» асиметрія – у реальній економічній дійсності, між, наприклад, продавцями та покупцями, роботодавцями та працівниками, компаніями та споживачами тощо. Однак існує другий рівень цієї проблеми – інформаційна асиметрія в самій аналітиці та дослідженнях.

Інформаційна асиметрія в галузі кібербезпеки має кілька серйозних наслідків. Вона призводить до спотворення аналітики, оскільки неповна або некоректна інформація ускладнює точне оцінювання ризиків і вразливостей, що може призвести до неточних висновків. Це, своєю чергою, створює невизначеність в економічних прогнозах, адже підприємства, інвестори та регулюючі органи не можуть точно передбачити тенденції розвитку кіберзагроз. Неефективне стратегічне планування, яке виникає через недостовірну інформацію, може призвести до неправильного розподілу ресурсів та низької ефективності заходів із захисту. Як приклад, можна навести масштабну кібератаку на

американське кредитне бюро Equifax. У 2017 році американське кредитне бюро Equifax стало жертвою масштабної кібератаки, під час якої було викрадено особисті дані понад 147 млн людей. Причиною стала вразливість у відкритому ПЗ Apache Struts, про яку компанія знала, але не виправила її вчасно [4]. Крім того, асиметрія інформації знижує довіру на ринку між постачальниками, споживачами та інвесторами, що погіршує взаємодію та співпрацю. Все це також призводить до затримок у реагуванні на нові кіберзагрози, коли одна зі сторін ринку володіє більшою чи кращою інформацією.

Таким чином, інформаційна асиметрія створює умови для невизначеності та високих ризиків, що ускладнює ефективне функціонування ринку кібербезпеки та збільшує ймовірність економічних збитків.

Явище інформаційної асиметрії виникає тоді, коли одна сторона володіє значно більшим обсягом достовірної інформації, ніж інша. У сфері кібербезпеки така асиметрія проявляється в обмеженому доступі до реальних даних про вразливості, масштаби атак, рівень захищеності компаній тощо. Часто постачальники послуг або постраждалі організації навмисно приховують або спотворюють інформацію, що створює викривлену картину ринку. У поєднанні з великою кількістю фейкових чи неперевірених джерел в інтернеті це значно ускладнює об'єктивний аналіз, формування економічних прогнозів та прийняття обґрунтованих рішень у сфері інвестицій у кіберзахист.

На наш погляд, однією з проблем аналізу ринку послуг та рішень з кібербезпеки є відсутність єдиного бачення на його структуру. Під час інформаційного пошуку класифікації категорій ринків у сфері кібербезпеки, ми зіткнулись з проблемою інформаційної асиметрії і в цьому питанні. Проаналізувавши різні аналітичні матеріали консалтингових агенцій (зокрема, Gartner, Fortune Business Insights, Allied Market Research, Grand View Research та ін.), опис статистики у міжнародних баз даних (зокрема, Statista), що свідчать про ті чи інші аспекти діяльності компаній у сфері кібербезпеки, ми дійшли висновку, що ринок рішень та послуг з кібербезпеки, який охоплює всі засоби, що спрямовані на захист комп'ютерних систем, мереж, даних і користувачів від кіберзагроз, аналітики бачать по-різному. Це пов'язано передусім з тим, що ми маємо справу з розробкою класифікації нового об'єкту дослідження, який тільки формується, знаходиться постійно у русі й змінює свій зміст і структуру під впливом нових технологічних трендів, законодавчих змін та різної реакції всіх зацікавлених сторін.

На наш погляд, станом на 2025 рік ринок послуг та рішень з кібербезпеки можна поділити на різні категорії/сегменти за такими ознаками: масштаб діяльності, тип клієнтів, галузева спеціалізація і технології (табл.1).

Таблиця 1

Поділ ринку послуг та рішень з кібербезпеки на категорії/сегменти*

Ознака	Категорії / Сегменти	Опис / Приклади
Масштаб діяльності	Глобальний	Palo Alto Networks, CrowdStrike – працюють по всьому світу
	Регіональний	Bitdefender (Європа), ESET – сильна присутність у певних регіонах
	Локальний	Місцеві MSSP, національні антивіруси – обслуговують локальні компанії
Тип клієнтів	Корпорації	Повний спектр послуг: SIEM, SOC, IAM
	Державні установи	Потребують спеціалізованого захисту критичної інфраструктури
	Малий і середній бізнес	Хмарні рішення, керовані послуги
	Фізичні особи (B2C)	VPN, антивіруси, захист особистих даних
Галузева спеціалізація	Фінанси	Захист банківських транзакцій, відповідність PCI DSS
	Охорона здоров'я	HIPAA, GDPR – конфіденційність медичних записів
	Освіта	Захист даних студентів, кібергігієна
	Промисловість (OT)	ICS, SCADA – фізичні інфраструктури
	E-commerce	Захист онлайн-платежів, фішинг, DDoS
Технології	Мережева безпека	Брандмауери, VPN, IDS/IPS
	Хмарна безпека	Захист хмарних середовищ AWS, Azure
	Endpoint Security	Захист кінцевих пристроїв, антивірусні системи
	Кіберрозвідка	Виявлення загроз, розвіддані про APT-групи
	IAM / Zero Trust	Управління доступом, багатофакторна автентифікація
	ШІ в кібербезпеці	Автоматичне виявлення аномалій, поведінковий аналіз

*Джерело: складено на основі даних Gartner, Statista, Fortune Business Insights.

Звичайно, ринок послуг та рішень з кібербезпеки є дуже динамічним, у ньому з кожним роком з'являються нові сегменти, тому наш поділ не є вичерпним, але у той же час ця класифікація може допомогти зорієнтуватись тим, хто починає свій шлях в аналітиці у сфері кібербезпеки.

Висновки

В роботі звернено увагу на проблему інформаційної асиметрії не тільки на ринку послуг та рішень з кібербезпеки, а й у сфері аналітики, присвяченій цьому ринку. Інформаційна асиметрія є ключовою проблемою ринку послуг та рішень з кібербезпеки. Різний рівень обізнаності між учасниками ринку (постачальниками, клієнтами, регуляторами та ін.) призводить до порушення прозорості, що ускладнює ухвалення обґрунтованих рішень, створює високі ризики та знижує ефективність інвестицій у кіберзахист. Також, наявність асиметрії знижує точність аналітики та прогнозування, бо обмежений доступ до повної та достовірної інформації унеможливлює точне оцінювання кіберризиків. Багато компаній не розголошують факти атак або втрат, що ще більше ускладнює збір повної аналітичної картини та формує викривлені уявлення про рівень безпеки.

Для подолання асиметрії необхідно впроваджувати прозорі звітні стандарти щодо інцидентів безпеки, стимулювати відкритий обмін даними про кіберзагрози та сприяти цифровій грамотності. Також є перспективними є наукові дослідження, які узагальнюють, систематизують, уточнюють теоретичні положення у цій галузі знань.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Cybersecurity Ventures. URL: https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165.
2. Study: Hackers Attack Every 39 Seconds. URL: https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds.
3. IBM Security Report 2024.URL: https://www.ibm.com/reports/data-breach.
4. Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes. URL: https://investor.equifax.com/news-events/press-releases/detail/237/equifax-releases-details-on-cybersecurity-incident?utm_source=chatgpt.com.

Свердлова Анастасія – здобувачка групи КБ-3.02, факультет інформаційних технологій і кібербезпеки, Державний університет інтелектуальних технологій і зв'язку, м. Одеса, e-mail: sanastasiya2005@gmail.com

Науковий керівник: ***Кораблінова Ірина Анатоліївна*** – канд. економ. наук, доцент, доцент кафедри публічного управління та цифрової економіки, Державний університет інтелектуальних технологій і зв'язку, м. Одеса.

Sverdlova Anastasiya – student, Faculty of Information Technologies and Cyber Security, State University of Intelligent Technologies and Telecommunications, Odesa, e-mail: sanastasiya2005@gmail.com

Supervisor: ***Korablinova Iryna***, PhD in Economics, Associate Professor, Associate Professor of the Department of Public Administration and Digital Economy, State University of Intelligent Technologies and Telecommunications, Odesa.