НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

ІНСТИТУТ ПРОБЛЕМ МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ ІМ. Г.Є. ПУХОВА

НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ «КІБЕРБЕЗПЕКА ЕНЕРГЕТИКИ»

Матеріали

29 травня 2024 року

Київ – 2024

УДК [621.3+620.9]::[004[056.53+42+94] + 504.06]
ББК 31
Б-39

Рекомендовано до друку Вченою радою Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України (протокол № 06 від 30 травня 2024 р.)

Б-39 **Кібербезпека енергетики,** науково-практична конференція Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України : матеріали, 29 травня 2024 р. Київ : ІПМЕ ім. Г.Є.Пухова НАН України, 2024. 121 с.

В-39 **Cybersecurity of energy**, scientific-practical conference of the G.E. Pukhov Institute for Modeling in Energy Engineering National Academy of Sciences of Ukraine : materials, May 29, 2024. Kyiv: PIMEE NAS of Ukraine, 2024. 121 p.

ОРГАНІЗАТОРИ КОНФЕРЕНЦІЇ

Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України
(м. Київ)

ПРОГРАМНИЙ КОМІТЕТ

Мохор Володимир Володимирович
член-кореспондент НАН України, доктор технічних наук, професор,
директор Інституту, голова програмного комітету

Чемерис Олександр Анатолійович
доктор технічних наук, старший науковий співробітник
заступник директора з наукової роботи

Чьочь Вікторія Володимирівна
кандидат технічних наук,
заступник директора з науково-технічної роботи

Артемчук Володимир Олександрвич
доктор технічних наук, старший науковий співробітник
заступник директора з науково-організаційної роботи

ОРГАНІЗАЦІЙНИЙКОМІТЕТ

Артемчук Володимир Олександрвич
доктор технічних наук, старший науковий співробітник
заступник директора з науково-організаційної роботи

Клименко Тетяна Михайлівна
Завідувачка науково-організаційного відділу

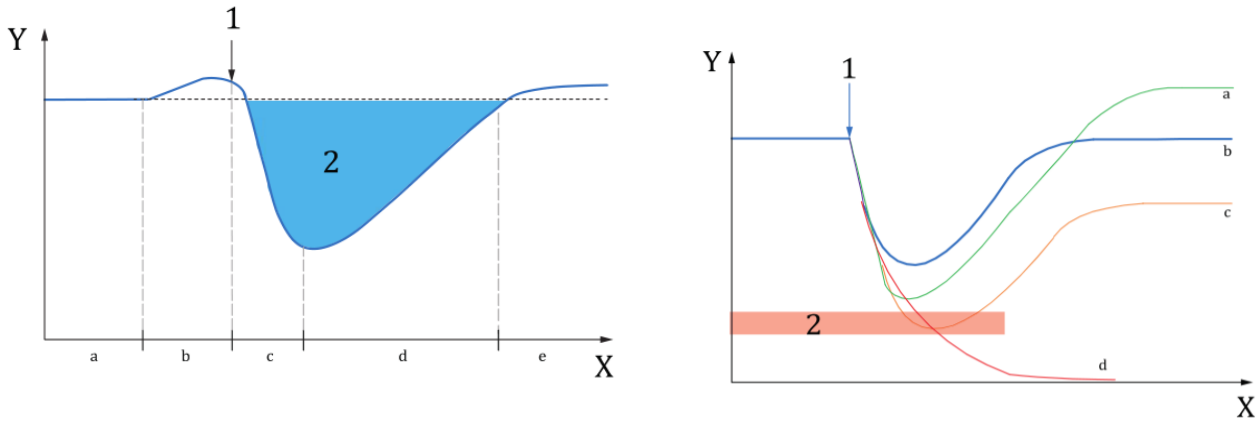
Цуркан Оксана Володимирівна
молодший науковий співробітник

В.В. Мохор, О.О. Бакалинський, Я.Ю. Дорогий, В.В. Цуркан

ПАРАДИГМА НОВИХ РИЗИКІВ КІБЕРБЕЗПЕКИ

Діяльність будь-якої організації незалежно від типу, розміру та природи направлена на досягнення поставленої мети [1]. Цьому сприяє глобальна мережа Інтернет, яка з одного боку є середовищем для обміну інформацією. Тоді як з іншого – джерелом нових ризиків кібербезпеки [2]. Тож запорукою діяльності організацій є здатність реагувати на змінювання як внутрішніх, так і зовнішніх обставин [3]. У даному випадку ключовою вимогою ефективного управління новими ризиками кібербезпеки є можливість передбачення, підготовлення і реагування організаціями на будь-які змінення обставин їх діяльності [4, 5]. Насамперед це досягається реагуванням на неочікувані або маловірогідні ризики з боку глобальної мережі Інтернет. Крім того відновленням нормального функціонування після виникнення нових ризиків кібербезпеки. І, що не менш важливе, адаптуванням до таких проявів небезпек [1–3]. Тож здатність організацій засвоювати, відновлювати та адаптовувати свою діяльність до мінливих обставин визначає організаційну резильєнтність (рис. 1, а) [3]. Цим обумовлюється актуальність аналізування парадигми нових ризиків кібербезпеки.

Під новим (емерджентним) ризиком кібербезпеки (англ. emerging cybersecurity risk) розуміється ризик зі значною невизначеністю, що призводить до настання серйозних наслідків (рис. 1, б[c, d]). З огляду на типове його тлумачення [4], це вказує, по-перше, на відсутність або незначний обсяг даних про вразливості, загрози, наслідки. По-друге, виникнення нового ризику кібербезпеки може призвести до припинення діяльності організації (рис. 1, б[d]).



а) реалізування сценарію:
1 – настання нового ризику;
2 – припинення діяльності;
[a] ідентифікування нового ризику;
[b] передбачення/підготовлення;
[c] поглинання/витримування;
[d] реагування/відновлення;
[e] адаптування/трансформування

б) наслідки реалізування сценарію:
1 – настання нового ризику;
2 – межі стрес-тестування;
[a] діяльність покращилася;
[b] діяльність не змінилася;
[c] діяльність призупинилася;
[d] діяльність припинилася

Рисунок 1 – Приклад впливання сценарію нового ризику кібербезпеки на діяльність організації: X – тривалість реалізування сценарію, Y – діяльність організації [3]

Залежно від змінення обставин діяльності організації природа нових ризиків кібербезпеки визначається [3]:

- проігнорованими або не відчутними ризиками;
- відомими ризиками в новому або незнайомому інтерпретуванні;
- ризиками зі значним розвитком;
- системними ризиками;
- новим комбінуванням ризиків.

Належність нових ризиків кібербезпеки до однієї з виокремлених груп визначається відповідними факторами, а саме [3]:

- знання (невідомі зміни обставин діяльності організації, недостатньо даних для визначення імовірності (вірогідності) та наслідків);
- волатильність (швидкі, непередбачувані зміни умов або обставин, впливання невідомого фактору, нестабільність інформації);
- невизначеність (перехід від ранніх попереджень до нових ризиків, визначення джерел нових ризиків);
- складність (системний характер або взаємодіяння нових ризиків з іншими ризиками);
- неоднозначність (можливість різноманітних інтерпретувань наявних даних, незрозумілість причин змінення обставин діяльності організації).

Характерною особливістю урахування даних факторів є мінливість з часом. Це стосується доступності інформації для ідентифікування, аналізування, зіставлення і, як наслідок, обробляння нових ризиків кібербезпеки [3, 5]. До того ж накопичення, аналізування, інтерпретування даних для прийняття рішення про необхідність і обирання варіантів їх обробляння. Крім того, в окремих випадках, запорукою ідентифікування нових ризиків є можливість зіставлення з подібними ризиками, зокрема, завдяки наявності інформації про них [5].

Отже, нові ризики кібербезпеки характеризуються значною невизначеністю і настанням серйозних наслідків, наприклад, припиненням діяльності організації. Їх поява здебільшого обумовлена часовою мінливістю внутрішніх і зовнішніх обставин. Тож здатністю організації передбачати, готуватися, реагувати на такі зміни обумовлюється ефективність управління новими ризиками кібербезпеки і в кінцевому випадку забезпечується організаційна резильєнтність.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ISO/IEC 27000:2018. Information technology. Security techniques. Information security management systems. Overview and vocabulary. [Valid from 2018-02-07]. URL: https://www.iso.org/standard/73906.html.
2. ISO/IEC FDIS 27032:2023. Cybersecurity. Guidelines for Internet security. [From 2023-05-09]. URL: https://www.iso.org/standard/76070.html.
3. ISO/ TS 31050:2023. Risk management. Guidelines for managing an emerging risk to enhance resilience. [Valid from 2023-10-27]. URL: https://www.iso.org/standard/ 54224.html.
4. ISO 31000:2018. Risk management. Guidelines. [Valid from 2018-02-14]. URL: https://www.iso.org/standard/65694.html.
5. IEC 31010:2019. Risk management. Risk assessment techniques. [Valid from 2019-06-17]. URL: https://www.iso.org/standard/72140.html.