УДК 004.056 http://doi.org/10.15407/pp2024.01.096

Ф.О. Коробейніков

КОНЦЕПТУАЛЬНА РАМКА РЕЗИЛЬЄНТНОЇ ПОВЕДІНКИ ІНФОРМАЦІЙНИХ СИСТЕМ

Пропоноване дослідження присвячене розробленню концептуальної рамки для опису резильєнтної поведінки інформаційних систем, яка визначає основні операційні фази реакції систем у контексті протидії реалізованим ризикам у момент інциденту. Фази включають у себе як заходи попередньої підготовки та безпосередньої протидії загрозам, так і механізми відновлення та адаптації після інцидентів. Досягнення зазначеної мети передбачає виявлення основних цілей і задач резильєнтності, які безпосередньо пов'язані з процесами нейтралізації потенційних загроз і впливають на стратегію управління ризиками, і зумовлюють необхідність всебічного аналізу критично значущих функцій організацій. У процесі дослідження особливу увагу було приділено створенню моделей резильєнтних і нерезильєнтних сценаріїв реакцій на інцидент та виокремленню поведінкових відмінностей. Застосування дельта-функції дало змогу деталізувати фазу резильєнтної відповіді на загрози, включно з етапами адаптації та подальшого відновлення. Дослідження робить значний внесок у сферу інформаційної безпеки, пропонуючи багаторівневий підхід до підвищення резильєнтності інформаційних систем.

Ключові слова: резильєнтність, захист інформації, інформаційна безпека

Вступ

Розбудова фреймворку підвищення резильєнтності будь-якої інформаційної системи, незалежно від її специфіки - чи то система захисту інформації, чи то система обробки та зберігання інформації, що належить організації, місії, або спільноті, - розпочинається з формулювання ключових цілей і задач. Процес їх визначення тісно пов’язаний зі стратегією управління ризиками організацій і вимагає глибокого розуміння того, що саме має бути захищено і які саме загрози можуть впливати на критичні функції організацій і пов’язані з ними інформаційні системи. Метою даного наукового дослідження є розробка концептуальної рамки резильєнтної поведінки інформаційних систем, яка не тільки відповідає вимогам резильєнтної парадигми, а й вміщує методи ідентифікації, ренжування та управління етапами протидії загрозам, віднесеним до категорії критичних, враховуючи їхнє співвідношення з цілями і задачами резильєнтності.

Цілі резильєнтності

Кожна ціль резильєнтності - це твердження високого рівня, що фокусується на одному з аспектів (наприклад, передбачити, витримати, відновити, адаптуватися) у визначенні резильєнтності [1].

На відміну від цілей інформаційної безпеки, які зосереджені на захисті конфіденційності, доступності та цілісності інформаційних активів, цілі резильєнтності виходять із передумови, що реалізація загроз є, хоча й небажаним, але неминучим елементом життєвого циклу системи. Ця концептуальна різниця підкреслює, що в той час як інформаційна безпека прагне запобігти реалізації загроз, резильєнтність визнає і приймає можливість їх виникнення, акцентуючи увагу на збереженні працездатності та швидкому відновленні після порушень.

Цілі резильєнтності, таким чином, визначають принципово інший підхід до управління ризиками, який передбачає розробку стратегій і рішень, які сприяють адаптивності системи в умовах мінливого середовища і несподіваних подій. Це не означає відмову від заходів із забезпечення безпеки, але підкреслює важливість додаткових заходів, спрямованих на забезпечення працездатності критичних функцій системи, коли стандартні методи безпеки виявляються неефективними [2].

Сукупно всі цілі резильєнтності націлені на протидію критичним ризикам і гарантоване підтримання працездатності основних функцій організації, місії або

системи. Кожна з цілей може бути співвіднесена з одним із ключових етапів протидії ризику, загроза якого реалізується або може бути реалізована: підготовка, протидія або абсорбування, відновлення та адаптація.

Використання дельта-функції для опису етапів протидії інциденту

На малюнку (Рис.1) інцидент представлений як миттєве збурення, яке можна змоделювати за допомогою дельта-імпульсу. Ця подія викликає негайне зниження продуктивності системи.

Дельта-імпульс, у рамках цього дослідження пропонується використовувати як для деталізації цілей резильєнтності, так і в контексті розробки моделі їхньої взаємодії. Ця концепція являє собою ідеалізований опис миттєвих, короткострокових подій, що мають високий рівень впливу. Це особливо актуально для сценаріїв критичних HILP-ризиків, які підлягають опрацюванню відповідно до парадигми резильєнтності.

Класична концепція дельта-імпульсу часто асоціюється з дельта-функцією Дірака [3]. У цьому контексті δ-імпульс є ідеалізованим, миттєвим, нескінченно коротким і сильним сигналом або впливом, який відбувається в певний момент часу.

Особливості дельта-імпульсу:

- Миттєвість: дельта-імпульс відбувається за нескінченно короткий проміжок часу.
- Локалізація в часі: Імпульс має місце в конкретний момент часу T, і поза цим моментом його вплив дорівнює нулю.
- Нескінченна амплітуда: У момент імпульсу його амплітуда прагне до безкінечності, але так, що інтеграл від імпульсу за часом залишається скінченним і зазвичай нормалізується до одиниці.

Дельта-функція Дірака $\delta(t-T)$, визначається такими властивостями:

- $\delta(t-T) = 0$ для всех $t \neq T$
- $\int_{-\infty}^{+\infty} \delta(t-T)dt = 1$

Дельта-функція може бути використана в контексті резильєнтності для моделювання миттєвих подій або шоків, що впливають на систему. У цьому контексті вона ілюструє критичні інциденти, які впливають на систему раптово і з сильним ефектом, але за дуже короткий проміжок часу:

- Моделювання зовнішніх шоків: Дельта-функція може бути використана для представлення раптових подій, таких як

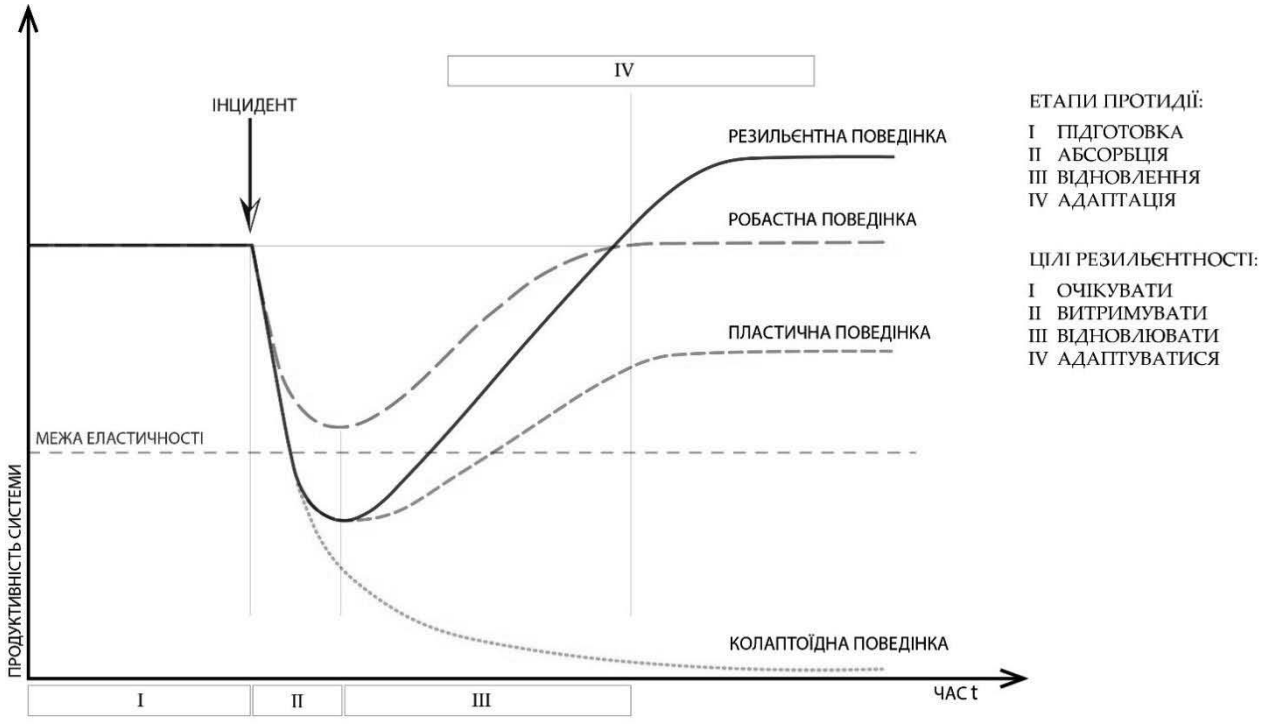

Рис. 1 Співвіднесення цілей резильєнтності і етапів протидії ризику

природні катастрофи, технологічні збої, економічні кризи та інші критичні інциденти. Ці події можуть бути представлені як миттєві імпульси, що впливають на систему.

- Аналіз реакції системи: Використання дельта-функції дає змогу аналізувати, як система реагує на миттєві збурення. Це може допомогти у визначенні ефективності заходів резильєнтності, таких як здатність системи до швидкого відновлення після шоку.
- Інтеграція з іншими моделями: Дельта-функція може бути інтегрована з іншими математичними моделями для створення комплексної моделі резильєнтності, що враховує як миттєві збурення, так і тривалі процеси відновлення та адаптації.

Важливі зауваження:

- Дельта-функція - це ідеалізована математична абстракція. Реальні події можуть мати більш тривалий вплив і не завжди точно відповідати миттєвому імпульсу.
- Реальні системи часто мають складні взаємодії та залежності, які можуть бути не повністю охоплені спрощеним поданням через дельта-функцію.

Таким чином, хоча дельта-функція є корисним інструментом для моделювання деяких аспектів резильєнтності, її слід використовувати з розумінням притаманних їй обмежень і часто в поєднанні з іншими методами та моделями.

Розглянемо дві моделі реакції системи на реалізацію критичного ризику. Одна з моделей є нерезильєнтною, а інша - резильєнтною, що включає всі парадигматичні етапи реагування на інцидент, ототожнювані з цілями резильєнтності. Обидві ці моделі використовують дельта-функцію для представлення інциденту і застосовують додаткові математичні функції для опису основних етапів реакції системи на цю подію.

Припустимо, що аналізується реакція супутникової системи передачі даних на миттєвий зовнішній вплив, наприклад, на потужний сонячний спалах. Це збурення може являти собою, наприклад, великий технологічний збій критичних функцій системи внаслідок коронального викиду маси на Сонці з індексом Dst -1500 нТл.

Сценарії нерезильєнтної поведінки

У контексті моделювання нерезильєнтної системи, яка стикається з миттєвим, коротким, але критичним інцидентом, модель може бути сформульована таким чином:

$$S(t) = P + \delta(t - T_0) \cdot I_0 + R(t)$$

де:

$S(t)$ - стан системи в часі t.

P - рівень підготовки системи до інциденту, що являє собою постійне значення, яке відображає базовий стан системи.

$\delta(t - T_0)$ - дельта-функція Дірака, використовувана для моделювання миттєвого впливу інциденту в момент часу T_0.

I_0 - інтенсивність інциденту, що відображає величину його миттєвого впливу на систему.

$R(t)$ - функція відновлення, що описує процес відновлення системи після інциденту. Ця функція може бути лінійною або експоненційною, залежно від характеру системи та її здатності до відновлення.

Наприклад:

$$R(t) = -R_0 \times e^{-k(t-T_r)} \text{ для } t \geq T_r$$

У цій моделі миттєвий критичний інцидент чинить істотний і негайний вплив на систему в момент часу, що може викликати короткочасне, але серйозне порушення.

Відновлення $R(t)$ являє собою процес, протягом якого система намагається повернутися до свого початкового стану.

Однак у контексті нерезильєнтної системи, цей процес може бути недостатнім або затяжним і відображає обмежену здатність системи до ефективного відновлення і призвести до реалізації трьох сценаріїв поведінкових реакцій:

- *Робастна поведінка* [4]: Система, що демонструє робастну поведінку, зберігає свою функціональність на первісному рівні навіть після впливу зовнішнього шоку, не виявляючи помітного зниження продуктивності - не опускаючись нижче рівня еластичності. Це свідчить про достатність заходів підготовки до інциденту - про наявність у системі вбудованої стійкості або надмірності, що дають змогу абсорбувати раптові

впливи без значних порушень у її роботі. Така система зазвичай характеризується високим ступенем надійності, завдяки чому вона здатна підтримувати критично важливі функції навіть в умовах екстремальних збурень.

- *Пластична поведінка* [5]: У разі пластичної поведінки, система відчуває тимчасове зниження продуктивності у відповідь на шок, після чого відбувається її часткове відновлення. Однак система не здатна повністю відновитися до рівня продуктивності вихідного стану, що вказує на відсутність достатніх механізмів підготовки, адаптації та відновлення.

- *Колапсоідна поведінка* (Collapsing Behavior): Означений тип поведінки характеризується нездатністю системи впоратися з раптовим шоком, унаслідок чого вона втрачає свою функціональність. Така поведінка може призвести до повного краху системи або вимагати фундаментальної реорганізації та перебудови для відновлення її працездатності. Це підкреслює критичну важливість включення заходів запобігання катастрофічним подіям у загальну стратегію управління ризиками та резильєнтності.

Тобто, аналіз нерезильєнтних реакцій систем на шокові події дає змогу глибше зрозуміти рівень їхньої гарантоспроможності і виявити потенційно слабкі місця в структурі та функціонуванні, що є ключовим аспектом ефективного управління ризиками та стратегії резильєнтності.

Резильєнтний сценарій реакції

В рамках концептуалізації моделі системи, що зазнає впливу миттєвого, короткочасного, проте критично значущого інциденту, представлення моделі передбачає систематичний і всебічний підхід до моделювання резильєнтності, заснований на точному кількісному та якісному аналізі динаміки системи в умовах невизначеності й потенційних ризиків, і може бути здійснене в такий спосіб:

$$S(t) = P + \delta(t - T_0) \cdot I_0 + W(t) \cdot H(t - T_w) + R(t) \cdot H(t - T_r) + A(t) \cdot H(t - T_a)$$

де:

$S(t)$ - стан системи в часі t.

P - рівень підготовки системи до інциденту, що являє собою постійне значення, яке відображає базовий стан системи.

$\delta(t - T_0) \cdot I_0$ - модель миттєвого інциденту в момент часу T_0 , де I_0 - інтенсивність впливу інциденту.

$W(t)$ - функція протидії або абсорбції інциденту.

$H(t - T_x)$ - ступінчаста функція Хевісайда, що активує відповідні процеси в момент часу T_x

$R(t)$ - функція відновлення, що починається після часу T_r і триває до досягнення стабільного стану.

$A(t)$ - функція адаптації, що починається після часу T_a і відображає поліпшення системи на основі досвіду інциденту.

В цій моделі ступінчаста функція Хевісайда, також відома як одинична ступінчаста функція, - це математична функція, що має значення нуль до певного моменту (назвемо його t_0) і значення один після цього моменту [6]. У математичному записі:

$$\begin{cases} 0, & \text{якщо } t < t_0 \\ 1, & \text{якщо } t \geq t_0 \end{cases}$$

Ця функція використовується для моделювання ситуацій, коли відбувається раптова зміна стану в певний момент часу. У контексті моделі резильєнтності, ступінчасті функції Хевісайда використовували для активації певних процесів тільки після настання певних подій.

T_w , T_r , T_a являють собою часові точки початку процесів абсорбції, відновлення та адаптації відповідно.

Протидія/абсорбція $W(t)$ відображає заходи, яких вживає система негайно після інциденту для пом'якшення його впливу.

Відновлення $R(t)$ показує, як система повертається до нормальної функціональності та можливо досягає поліпшеного стану після інциденту.

Адаптація $A(t)$ підкреслює процес поліпшення системи у відповідь на досвід, отриманий під час інциденту, посилюючи загальну резильентність системи.

Модель охоплює основні етапи протидії та ілюструє, як резильєнтна система може ефективно реагувати на миттєві

інциденти, швидко відновлюватися й адаптуватися, щоб поліпшити свою здатність протистояти майбутнім загрозам.

Однак не всі інциденти в контексті резильєнтності, особливо ті, що стосуються кіберпростору, можуть бути адекватно представлені через дельта-функцію Дірака, яка символізує миттєвий вплив.

Наприклад, APT-атаки (Advanced Persistent Threats) зазвичай розвиваються поступово і можуть залишатися непоміченими протягом тривалого часу, перш ніж їхні наслідки стануть явними.

У таких випадках інцидент характеризується тривалим періодом, протягом якого загроза поступово посилюється, і може не бути виявлена доти, доки не завдасть значної шкоди.

Замість використання дельта-функції для представлення APT-атак, ми можемо використовувати функцію, яка збільшується з часом або змінюється залежно від виявлення і впливу атаки. Наприклад, можна використовувати безперервну функцію $I(t)$, яка починається з моменту T_0 і збільшується з часом:

$$\begin{cases} a \cdot (t - T_0)^b, & \text{якщо } t \geq T_0 \\ 0, & \text{якщо } t < T_0 \end{cases}$$

де: a і b - параметри, що визначають швидкість зростання та інтенсивність впливу атаки. T_0 - час початку інциденту або атаки. t - поточний час.

Інтерпретація: До T_0 інцидент ще не почався, і його вплив на систему дорівнює нулю. Після T_0 інцидент починається і його вплив на систему поступово збільшується. Степенева функція $(t - T_0)^b$ дає змогу моделювати різні сценарії розвитку інциденту - від тих, що повільно наростають, до більш стрімких.

Припустимо, що на кіберсистему було здійснено APT-атаку в момент часу T_0. Формула для $I(t)$:

$$I(t) = a \cdot (t - T_0)^b, \text{ якщо } t \geq T_0$$

До T_0 атака ще не почалася, і її вплив на систему відсутній. У Момент T_0 і після - атака починається. Спочатку її вплив може бути незначним, але з часом він збільшується. Наприклад, зловмисники можуть спочатку отримати доступ до некритичних частин системи, але поступово проникають глибше, отримуючи доступ до важливіших даних або ресурсів.

Параметри a і b: Параметр a: Визначає початковий рівень впливу атаки. Якщо a малий, початковий вплив атаки невеликий. Параметр b: Визначає, наскільки швидко посилюється вплив атаки. Більше значення b означає більш швидке зростання загрози.

Наприклад, якщо атака почалася в момент $T_0 = 5$ (наприклад, 5 днів після початку спостереження), з параметрами $a = 0.1$ і $b = 2$, то через 10 днів після початку спостереження ($t = 10$) вплив атаки буде:

$$I(10) = 0.1 \cdot (10 - 5)^2 = 0.1 \cdot 25 = 2.5$$

Це означає, що вплив атаки на систему посилюється з часом, що вимагає безперервного моніторингу та переосмислення стратегії застосування адаптивних заходів реагування для забезпечення ефективної відповіді на загрозу.

Інтегрувавши функцію $I(t)$, яка описує лонгітюдний перебіг інциденту в запропоновану раніше модель резильєнтності, що містить етапи підготовки, реагування/абсорбції, відновлення та адаптації, отримаємо:

$$S(t) = P + I(t) \cdot H(t - T_0) + W(t) \cdot H(t - T_w) + R(t) \cdot H(t - T_r) + A(t) \cdot H(t - T_a)$$

Ця інтегрована модель враховує як миттєві, так і тривалі загрози, ілюструючи динаміку реакції резильєнтної системи на різноманітні інциденти та її здатність до відновлення й адаптації.

Серед усіх розглянутих моделей поведінки системи у відповідь на різні сценарії впливу критичних загроз, резильєнтна модель, що характеризується адаптивною поведінкою, демонструє найбільшу ефективність. Ця модель виходить за рамки простого відновлення після шоку, передбачаючи активну адаптацію системи, що передбачає поліпшення її функцій і продуктивності через процеси навчання і самоорганізації. Адаптивна поведінка системи передбачає розробку і впровадження нових структур, функцій, зворотних зв'язків і джерел залучення ресурсів, що приводить не тільки до відновлення, а й до фундаментальної

трансформації системи, зміцнюючи її стійкість до майбутніх шоків і загроз.

Особливої значущості резильєнтна модель набуває в довгостроковій перспективі, оскільки вона сприяє сталому розвитку і підвищенню загальної здатності системи адаптуватися до мінливих умов і непередбачених обставин. Системи, що володіють адаптивною поведінкою, не тільки ефективно долають поточні проблеми, а й безперервно розвиваються, посилюючи свою резильєнтність протягом усього життєвого циклу.

Детальний аналіз резильєнтної поведінки системи виявляє наявність чотирьох критичних і невід'ємних етапів, які корелюють з основними цілями резильєнтності, визначеними відповідно до її концептуальної парадигми. Ці етапи включають: підготовка (ціль - очікувати), абсорбція (витримати), відновлення (відновити) та адаптація (адаптуватися) [7]. Кожна з цих цілей характеризується унікальними атрибутами та функціями:

- *Очікувати*. Ітеративне вдосконалення методик виявлення та опрацювання критичних ризиків, значущих у контексті резильєнтності. Поінформована готовність, що передбачає планування на випадок непередбачуваних ситуацій, включно з планами мітигації та уникнення загроз, а також реагування на виявлення вразливостей або порушення ланцюга постачання. Розвідка нових типів загроз надає важливу інформацію для інформованої готовності

- *Витримати*. Ця ціль акцентується на створенні механізмів забезпечення гарантованої стійкості критичних функцій системи до негативних впливів і здатності зберігати функціональність навіть в умовах серйозних порушень.

- *Відновити*. Вдосконалення процесу відновлення системи після виникнення загрози або інциденту, включно з поверненням до нормального функціонування.

- *Адаптуватися*. На цьому ключовому, в контексті резильєнтності, етапі створюються можливості для швидкої адаптації системи до змін і нових загроз, оновлюються та модифікуються захисні механізми для підвищення загальної стійкості та ефективності всієї системи.

Слід підкреслити, що принципи, методології та стратегії, що застосовуються для досягнення цілей резильєнтності, значно відрізняються від прийнятих у традиційній практиці інформаційної безпеки. Відмітна особливість резильєнтного підходу проявляється вже на початковому етапі побудови резильєнтної системи, де потрібне проведення комплексної та глибокої трансформації методик ризик-менеджменту та переосмислення теоретичних основ виокремлення та опрацювання ризиків. У рамках цієї трансформації розробляються нові методики, що гармоніюють із концепцією резильєнтності та орієнтовані на ідентифікацію ризиків, які мають ключове значення для стабільності та безперервності функціонування систем або організацій. Метою такого підходу є гарантування постійної працездатності критично важливих функцій в умовах непередбачуваності та динамічних загроз. Це передбачає не просто адаптацію наявних інструментів управління ризиками, а й створення нових, гнучкіших і ефективніших підходів, здатних адекватно реагувати на унікальні виклики, характерні для сучасних інформаційних систем у світі, що безперервно змінюється.

Висновки

У статті викладено результати розробки концептуальної рамки, яка описує особливості резильєнтної поведінки інформаційних систем. Вона вміщує як етапи попередньої підготовки та активної протидії загрозам (типові для класичних сценаріїв інформаційної безпеки), так і механізми адаптації та відновлення після інцидентів, характерні для суто резильєнтних сценаріїв. Важливим аспектом роботи стало визначення ключових задач і цілей резильєнтності, які прямо корелюють із ключовими процесами нейтралізації потенційних загроз, що мають значний вплив на стратегію управління ризиками та підкреслюють необхідність всебічного аналізу критично значущих функцій у контексті організацій.

Особливу увагу приділено розробленню та порівнянню моделей резильєнтних і нерезильєнтних сценаріїв поведінки

систем, а також аналізу відмінностей їхніх реакцій на загрози. Застосування дельта-функції сприяло детальному опрацюванню фаз резильєнтної відповіді на загрози, включно з етапами адаптації та подальшого відновлення.

Література

1. NIST Special Publication 800-160, Volume 2. Developing cyber-resilient systems: A systems security engineering approach. NIST, 2021. 254 p. URL: ttps://doi.org/ 10.6028/NIST.SP.800-160v2r1
2. Korobeynikov F., Bakalynskyi O. Defining the Sequence of Integrating Trustworthiness Components Into Information Security Systems. Ukrainian Information Security Research Journal. 2023. Vol. 4, no. 25. P. 268–274. URL: https://jrnl.nau.edu.ua/ index.php/ZI/article/view/18233.
3. Khuri, A. (2004). Applications of Dirac's delta function in statistics. International Journal of Mathematical Education in Science and Technology, 35, 185 - 195. https://doi.org/10.1080/00207390310001638313.
4. Klau, G., & Weiskircher, R., 2004. Robustness and Resilience. , pp. 417-437. https://doi.org/10.1007/978-3-540-31955-9_15.
5. Benzerga, A., Leblond, J., Needleman, A., & Tvergaard, V. (2016). Ductile failure modeling. International Journal of Fracture, 201, 29-80. https://doi.org/10.1007/s10704-016-0142-6.
6. Venetis, J. 2021. An Explicit Form of Heaviside Step Function. . https://doi.org/10.20944/PREPRINTS202106.0132.V1.
7. Bakalynskyi O., Korobeynikov F. Establishing Goals in the Creation of Cyber-Resilient Systems per NIST. 2023 13th International Conference on Dependable Systems, Services and Technologies (DESSERT), Athens, Greece, 13–15 October 2023. 2023. URL: https://doi.org/10.1109/dessert61349.2023.10416540

Одержано: 11.03.2024

Про автора:

Коробейніков Федір Олександрович,
Аспірант Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова,
Київ, Україна
e-mail: admin@cybersecurity.com.ua
https://orcid.org/0009–0003–8127–4379