УДК 004.056

А. В. Давидюк, В. Ю. Зубок
Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова
вул. Генерала Наумова, 15, 03164 Київ, Україна
тел. (+38044) 4241063, e-mail: andrey19941904@gmail.com
тел. (+38044) 4241063, e-mail: vitaly.zubok@gmail.com

Застосування логіки предикатів для верифікації артефактів кіберзахисту підчас проєктування систем критичного призначення

З розвитком інформаційних технологій важливим аспектом стабільності функціонування систем критичного призначення стало забезпечення кібербезпеки об'єктів критичної інформаційної інфраструктури. Для захисту інформації законодавством України передбачено побудову комплексних систем захисту інформації і систем управління інформаційної безпеки. Проте щодо систем критичного призначення такі підходи мають загальний характер і можуть бути ефективно використані при забезпеченні кіберзахисту окремих сегментів таких систем. Під час проєктування систем критичного призначення значна увага приділяється виконанню вимог до надійності і якості на кожній стадії. Водночас вплив внутрішнього та зовнішнього факторів на функціонування таких систем і їхні імовірнісні характеристики іноді залишаються без належної уваги. Враховуючи можливі наслідки порушення функціонування таких систем (значні матеріальні та нематеріальні збитки), для врахування можливого впливу невизначеності на результати їхньої роботи (ризику) запропоновано використати логіку предикатів для створення зв'язків властивостей артефактів. Саме автоматизація процесів захисту дасть можливість значно підвищити ефективність існуючих механізмів захисту.

Ключові слова: *системи критичного призначення, автоматизовані системи управління технологічними процесами, кібербезпека, кіберзахист, ризик, об'єкт критичної інформаційної інфраструктури, предикат.*

Вступ

Системами критичного призначення називають автоматизовані системи, які має критичні для життя людей функції. Такі системи визначаються за певними ха-

рактеристиками та мають відповідати встановленим вимогам, які затверджуються нормативними документами, національними та міжнародними стандартами.

Верифікація артефактів кіберзахисту систем критичного призначення дозволяє знизити ризики інформаційної безпеки підчас експлуатації як елементів, так і всієї системи в цілому. На жаль, підхід досі не отримав широкого розповсюдження в Україні, попри те, що існують як національні, так і загальновизнані іноземні нормативні документи, що визначають систему критичного призначення як об'єкт інформаційно-комунікаційних технологій і можуть бути використані для визначення необхідних критеріїв верифікації.

Законом України «Про основні засади забезпечення кібербезпеки України» [1] визначено поняття «критична інформаційна інфраструктура» як сукупність об'єктів критичної інформаційної інфраструктури. Водночас «об'єкт критичної інформаційної інфраструктури» цим же Законом визначається як комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури.

У Законі України «Про критичну інфраструктуру» [2] на відміну від попереднього документа поняття «об'єкти критичної інфраструктури» пояснюється як об'єкти інфраструктури, системи, їхні частини та їхня сукупність, які є важливими для економіки, національної безпеки і оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам. Таке визначення є більш повним і чітким, що дає змогу виокремити необхідні об'єкти, при проєктуванні яких варто приділити пріоритетну увагу їхній верифікації.

Цим документом вперше введено термін «проєктна загроза об'єкту критичної інфраструктури», який визначає властивості, характеристики реальних і потенційних загроз об'єкту критичної інфраструктури, на зниження ймовірності реалізації яких має бути спрямовано функціонування системи захисту критичної інфраструктури. Оскільки об'єкт критичної інформаційної інфраструктури (надалі — об'єкт КІІ, або ОКІІ) є частиною об'єкта критичної інфраструктури, поняття «проєктна загроза» може бути застосованим і до ОКІІ.

З огляду на зазначене вище, метою дослідження є розробка підходів до визначення артефактів кіберзахисту та їхньої верифікації для їхнього застосування в управлінні ризиками при проєктуванні та експлуатації ОКІІ.

Аналіз предметної області визначення артефактів проєктування

З метою визначення груп і систематизації елементів проєктування систем критичного призначення проведемо декомпозицію поняття «проєктна загроза об'єкта критичної інфраструктури». Опис проєктної загрози повинен містити відомості щодо властивостей, характеристики реальних і потенційних загроз об'єкта критичної інфраструктури, оцінки ймовірності реалізації таких загроз, інформацію про системи захисту критичної інфраструктури.

Джерелами даних для опису артефактів є технічне завдання, технічний проєкт, технічні специфікації та інструкції розробників систем і їхніх елементів. Підґрунтям для розробки таких документів є ГОСТ 34 серії [3–10]. Безпосередньо вимоги до технічного завдання та змісту технічної документації визначаються ГОСТ 34.602-89 та ГОСТ 34.698-90 [8, 10].

Варто звернути увагу на нормативні документи технічного захисту інформації (НД ТЗІ) [11], зокрема [12], що визначає порядок проведення робіт зі створення комплексної системи захисту інформації в інформаційно-комунікаційній системі.

Характеристики реальних і потенційних загроз при побудові комплексної системи захисту інформації [12] описані в моделі загроз відповідно до вимог НД ТЗІ 1.4-001-2000 [13] та з урахуванням ДСТУ ISO/IEC 27005 [14] і ДСТУ ISO 31000:2018 [15].

Процес оцінювання імовірності таких загроз є частиною процедур з оцінювання ризиків інформаційної безпеки відповідно до [14], тому що поняття «ризику» визначається ДСТУ ISO/IEC 27000 комбінацією ймовірності події та її наслідків [16]. Варто зазначити, що рекомендація щодо оцінювання ризиків наявна і в Постанові Кабінету Міністрів України [17].

Системи захисту критичної інфраструктури, зокрема їхніх об'єктів критичної інформаційної інфраструктури, в нашій державі визначаються Законом України «Про захист інформації в інформаційно-комунікаційних системах» [18]. Таким чином, з метою виконання нормативних вимог створюються комплексні системи захисту інформації і системи управляння інформаційною безпекою. Додатково вимоги щодо систем захисту представлені Постановою Кабінету Міністрів України [19] та наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України [20].

Слід зазначити, що окрім комплексних систем захисту інформації і систем управління інформаційною безпекою в документах [17] та [20] відповідно використовуються поняття «системи захисту інформації» та «системи інформаційної безпеки». Останнє має безпосереднє відношення до об'єкта критичної інформаційної інфраструктури та визначається як сукупність організаційних і технічних заходів, а також засобів і методів захисту інформації, які впроваджуються на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури з метою запобігання кіберінцидентам, виявлення кібератак і захисту від них, порушення конфіденційності, цілісності та доступності інформаційних ресурсів, що обробляються (передаються, зберігаються) на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури, запобігання порушенню режиму функціонування та (або) недоступності служб (функцій) об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури, порушенню функціонування компонентів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури; забезпечення спостережності за діями користувачів об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури та функціонуванням засобів захисту об'єкта критичної інформаційної інфраструктури об'єкта критичної інфраструктури [17]. Таке визначення, охоплює засоби та заходи, що використовуються при впровадженні комплексних систем захисту інформації і систем управління інформаційною безпекою.

Зважаючи на те, що процес проєктування систем захисту систем критичного призначення нераціонально розглядати окремо від процесу проєктування самих систем критичного призначення, вбачаємо доцільним сфокусуватися на системах управління технологічними процесами, або Industrial Control Systems (ICS) [21], Industrial automation and control systems (IACS) [22]. Визначення терміну «система

управління технологічними процесами», тобто автоматизована або автоматична система, що є сукупністю обладнання, засобів, комплексів і систем обробки, передачі та приймання, призначена для організаційного управління та (або) управління технологічними процесами (включаючи промислове, електронне, комунікаційне обладнання, інші технічні та технологічні засоби) незалежно від наявності доступу системи до мережі Інтернет та (або) інших глобальних мереж передачі даних, наведено у роботі [1].

З метою уникнення невизначеності пропонується далі замість інтегрального поняття «система критичного призначення» використовувати «система управління технологічними процесами» та тотожне йому ICS. З огляду на те, що ICS можуть включати компоненти, розроблені за окремими проєктами, зокрема системи диспетчерського контролю та збору даних (Supervisory Control And Data Acquisition, SCADA), розподілені системи керування (Distributed Control System, DCS) та більш дрібні компоненти чи підсистеми, наприклад виробничий майданчик (site), мережа на виробництві (fieldnetwork), контролер з програмованою логікою (PLC), датчик (sensor), виконавчий пристрій (actuator), архіватор даних (data historian) так інші, процес верифікації проєктування таких систем може бути досить складним [21].

Щоби зменшити кількість помилок при проєктуванні таких систем запроваджується покрокове (багатостадійне) проєктування. Здебільшого верифікацію артефактів такого процесу можна розділити на два етапи, а саме — верифікацію до введення системи в експлуатацію та верифікацію під час експлуатації у рамках модернізації, масштабування тощо. До введення в експлуатацію процеси верифікації здійснюються під час попередніх випробувань і дослідної експлуатації [7, 12].

Аудит як джерело даних для верифікації артефактів кіберзахисту

Джерелом даних для верифікації артефактів при модернізації є процеси аудиту систем управління інформаційною безпекою [23] або державної експертизи комплексних систем захисту інформації [24].

Метою аудиту таких систем є пошук оптимальних рішень, що зможуть підвищити рівень їхньої захищеності, не порушуючи технологічних процесів. Вирішення таких завдань є досить складним з огляду на значну кількість застарілого програмного забезпечення. Перехід на оновлені версії в окремих випадках є неможливим або економічно недоцільним через вартість і складність.

Для забезпечення безпеки сегменту управління процесами, до базових завдань будь-якого аудиту можна віднести визначення методів покращення характеристик об’єкта аудиту відповідно до його критеріїв [23]. Такими покращеннями можна вважати прийняття оптимальних і більш ефективних технічних і організаційних рішень щодо захисту інформації. Зокрема, впроваджена в організації політика безпеки сприяє реалізації визначеної моделі менеджменту як свого роду артефакту. Водночас модель процесів управління ризиками є основою для розробки системи менеджменту в організації [14].

Результат формування аудитором незалежної об’єктивної думки щодо відповідності системи управління інформаційної безпеки визначеним критеріям аудиту у вигляді рекомендацій (схеми) щодо покращень є артефактом процесу ау-

диту. Основними критеріями такого артефакту повинні бути незалежність і об'єктивність. Кращим підтвердженням об'єктивності результатів аудиту є докази, отримані від третьої сторони, наприклад організації партнера, конкурента тощо.

Як бачимо, артефакти аудиту систем управління інформаційною безпекою об'єктів критичної інформаційної інфраструктури можуть бути наявними та похідними. Зокрема результати аудиту є похідними від наявних задокументованих процесів і процедур. У такому випадку виникає питання верифікації похідних артефактів, особливо їхньої відповідності критеріям застосовності, об'єктивності та ефективності. Для такої верифікації можна використати якісне та кількісне оцінювання.

Кожен похідний артефакт може бути оцінений стосовно відповідності критерію аудиту (наприклад, відповідає, не відповідає, частково відповідає, або кількісно у відсотковому вимірі) з урахуванням рівня критичності системи об'єкта КІІ. Таке оцінювання повинно враховувати результати попередніх аудитів для оцінки розвитку процесів безпеки в організації. До таких показників розвитку можна віднести:

— зменшення кількості інцидентів кібербезпеки;

— підвищення професійних якостей персоналу;

— наявність задокументованих процесів і процедур щодо забезпечення безперервності функціонування критичних процесів і відновлення після виникнення обставин непереборної сили.

Для формування необхідних артефактів при аудиті систем управління інформаційної безпекою на об'єктах КІІ під час їхнього функціонування основою є ризик-орієнтований підхід. Водночас, виконання елементів циклу управління ризиками [14] є можливим і на етапі проєктування систем критичного призначення. Зокрема, процеси категоризації системи за різними показниками, вибір заходів що-до забезпечення захищеності та їхнього впровадження, оцінювання ефективності такої їхньої імплементації, внесення змін, постійний моніторинг з використанням індикаторів стану є невід'ємною частиною операційних процедур, направлених на стійкість таких систем. Документування таких процесів, їхній систематичний перегляд, направлений на оптимізацію та підвищення ефективності, є складовими моделі оцінювання ризиків як артефакту процесу проєктування. Наявність такого артефакту є корисною для аналізу наявних переваг і недоліків при модернізації систем, їхньому масштабуванні, внесенні змін до функціонального призначення.

Спосіб верифікації артефактів кіберзахисту при проєктуванні систем критичного призначення із використанням логіки предикатів

Незважаючи на досить ґрунтовне документальне забезпечення процесу проєктування ICS, даний процес є досить складним і відповідальним. Тому варто враховувати, що для нього не є виключенням людський фактор, який може бути першопричиною можливих помилок у функціонуванні таких систем. З метою контролю артефактів і для підтримки прийняття об'єктивних рішень необхідно розробити методи автоматизованого синтезу формальних специфікацій функціональ-

них характеристик системи критичного призначення, що постачатиме вихідні дані для роботи методу формальної верифікації.

Для підвищення якісних характеристик процесу верифікації пропонується наступна система тверджень:

— за наявності у будь-яких об’єктів однакових властивостей їхній стан може бути змінений одним і тим же фактором впливу;

— наслідки такого впливу визначаються умовами та фактором впливу;

— умови впливу визначаються об’єктом впливу та фактором впливу.

Отже фактор впливу, об’єкт впливу, умови та наслідки впливу є взаємопов’язаними величинами. При цьому можуть виникати наступні прості відношення, для створення яких ключовим аргументом є множини властивостей об’єктів:

1) об’єкт – наслідки (один до багатьох);
2) об’єкт – фактори (один до багатьох);
3) об’єкт – умови (один до багатьох);
4) умови – наслідки (багато до багатьох);
5) фактори – умови (багато до багатьох);
6) фактори – наслідки (багато до багатьох).

Для уникнення невизначеності при подальшому викладенні результатів дослідження формалізуємо зазначені зв’язки у вигляді рис. 1, що зображує вищевказані відношення.

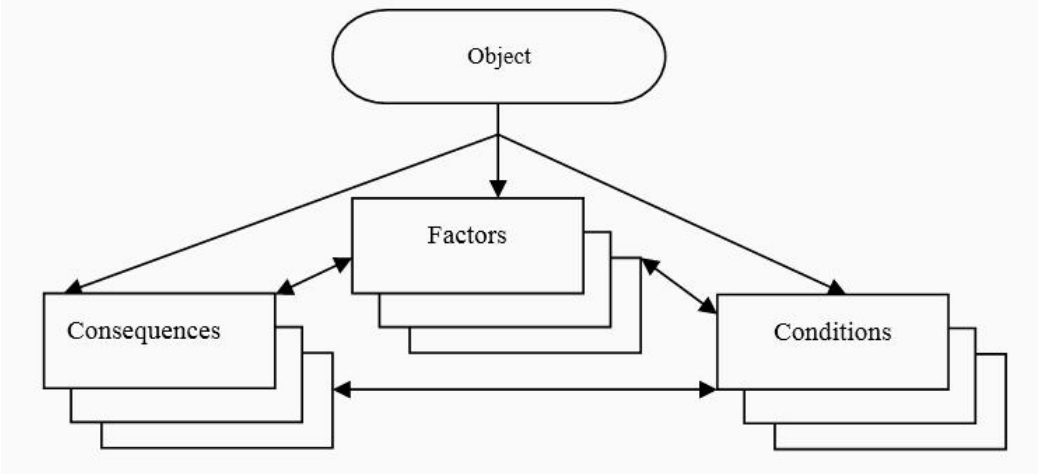

Рис. 1. Структура відносин між об’єктом впливу та характеристиками впливу, де Factor — фактори впливу; Consequences — наслідки впливу; Conditions — умови настання наслідків

З огляду на зазначене використаємо логіку предикатів [25] для розробки алгоритму пошуку спільних факторів, умов, наслідків для множини об’єктів, до яких також можуть належати й артефакти (створення відношень багато – багато до багатьох).

Суть запропонованого способу верифікації артефактів за допомогою логіки предикатів полягає в наявності у кожного елемента системи (апаратна, програмно-апаратна складова тощо) певної вразливості, що пов’язана з порушеннями його властивостей. Наприклад, нехай x-змінна, що визначена на множині операційних

систем (D), а $P(x)$ — предикат «x –». Задане словесне формулювання предикатної формули матиме такий вигляд: $\forall x P(x)$.

Формула $\forall x P(x)$ означає «всі операційні системи вразливі». Вона не залежить від змінної x, а лише характеризує всі операційні системи вцілому.

Може мати місце і такий варіант: нехай x — змінна, що визначена на множині операційних систем (D), а $P(x)$ — предикат «x – вразлива операційна система». Задамо словесне формулювання предикатної формули $\exists x P(x)$ та визначимо його істинність.

Формула $\exists x P(x)$ означає «в множині операційних систем є вразлива операційна система». Множина операційних систем містить вразливі системи, тому дане висловлювання істинне.

Так само можуть бути описані наслідки, фактори і умови, що дасть можливість визначити спільність умов, факторів і наслідків у відношенні до певного конкретного об’єкта.

Ефективність способу залежатиме від обсягу наборів вхідних даних, що можуть формуватися як на основі існуючого досвіду, так і з використанням знань і досвіду експертів галузі. За допомогою цих наборів визначаються всі властивості компонентів системи, після чого компоненти системи групуються за однаковими властивостями (виникають предикати). Елементи, що мають однакові властивості є потенційно вразливими до однакових вразливостей (факторів). Кожен фактор може бути реалізованим за певних умов. Таким чином, будуються зв’язки між елементами системи та створюються ланцюги елементів, їхніх властивостей, факторів та умов, за яких фактори можуть бути реалізовані та призвести до відповідних наслідків. При зміні властивостей одного з елементів ланцюга виникає висока ймовірність порушення властивостей інших. Тому стає доцільним перевірити можливість впливу факторів, що вплинули на зміну властивостей одного елемента на весь ланцюг. Функціональна схема даного способу зображена на рис. 2.

Використання такого підходу є основою для створення систем машинного навчання, які в перспективі можуть будувати ланцюги умов і впливів для досягнення конкретної цілі (об’єкта), визначаючи артефакти процесу реалізації таких послідовностей, що, у свою чергу, можуть належати до множин властивостей і факторів впливу систем критичного призначення. З використанням параметрів оцінювання ризиків (імовірність, величина збитку) [14], відомостей про наявні вразливості тощо такі алгоритми можуть бути використані для прогнозування настання тих чи інших наслідків залежно від умов і факторів впливу.

Підхід до верифікації артефактів кіберзахисту за допомогою логіки предикатів може слугувати для підтримки прийняття рішень про впровадження засобів і заходів з підвищення стійкості систем критичного призначення, оскільки дає змогу швидко створити максимальний перелік можливих варіантів для аналізування. На основі отриманих даних всі об’єкти критичної інформаційної інфраструктури (системи критичного призначення) можна розділити за рівнями зрілості (низький, високий, середній). На низькому рівні будуть розташовані об’єкти критичної інформаційної інфраструктури, що матимуть найбільшу кількість факторів (вразливостей), а на високому — найменшу. Така оцінка зрілості можна використовувати для оцінювання ефективності впроваджуваних заходів захисту.

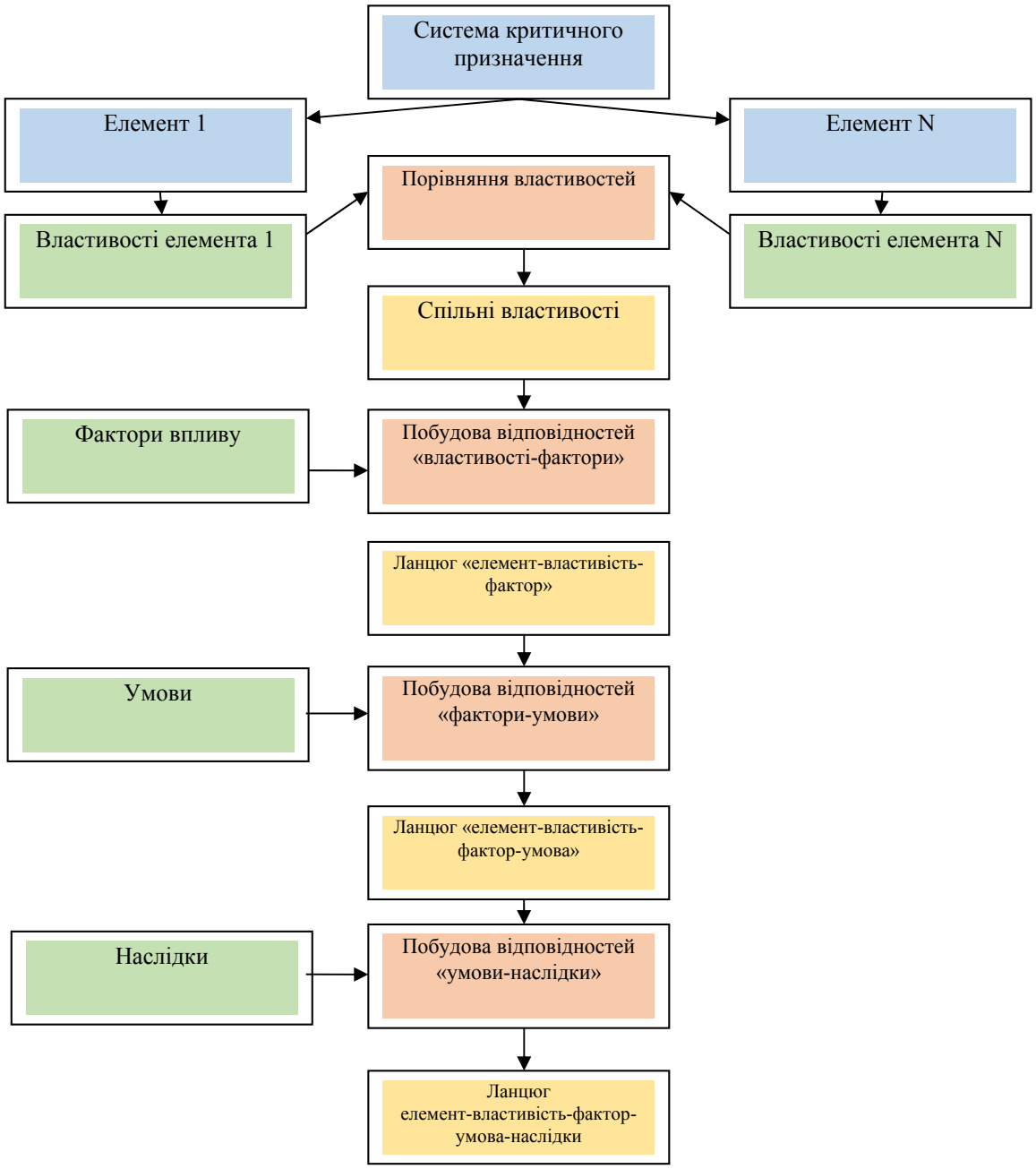

Рис. 2. Функціональна схема верифікації артефактів кіберзахисту

Висновки

Розроблений підхід до верифікації артефактів кіберзахисту за допомогою логіки предикатів, за наявності великого обсягу спеціалізованих даних (властивості, умови, фактори впливу, наслідки), може бути використано для верифікації артефактів кіберзахисту систем критичного призначення.

Застосування логіки предикатів до оброблення даних про властивості складових систем можуть спростити причинно-наслідковий аналіз за рахунок його автоматизації. Розширення та приорітизація існуючих ланцюгів може значно під-

вищити результати аналізування ризиків і класифікації об'єктів КІІ за рівнем зрілості.

1. Закон України «Про основні засади забезпечення кібербезпеки України». 2017. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

2. Закону України «Про критичну інфраструктуру». 2021. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text

3. ГОСТ 34.003-90. Інформаційна технологія Комплекс стандартів на автоматизовані системи. Автоматизовані системи. Терміни та визначення. 1992. URL: https://docs.cntd.ru/document/1200006979

4. ГОСТ 34.201-89. Види, комплектність та позначення документів при створенні автоматизованих систем. 1990. URL: https://www.swrit.ru/doc/gost34/34.201-89.pdf

5. ГОСТ 34.320-96. Концепції та термінологія для концептуальної схеми та інформаційної бази. 1996. URL: https://www.swrit.ru/doc/gost34/34.320-96.pdf.

6. ГОСТ 34.321-96. Інформаційні технології. Система стандартів з баз даних. Еталонна модель керування. 2001. URL: https://www.swrit.ru/doc/gost34/34.321-96.pdf

7. ГОСТ 34.601-90. Автоматизовані системи. Стадії створення. 1992. URL: https://www.swrit.ru/doc/gost34/34.601-90.pdf

8. ГОСТ 34.602-89. Технічне завдання на створення автоматизованої системи (замість ГОСТ 24.201-85). 1990. URL: https://www.swrit.ru/doc/gost34/34.602-89.pdf

9. ГОСТ 34.603-92. Інформаційна технологія. Види випробувань автоматизованих систем. 1993. URL: https://www.swrit.ru/doc/gost34/34.603-92.pdf

10. РД 50-34.698-90. Автоматизовані системи. Вимоги щодо змісту документів. 1992 URL: https://www.swrit.ru/doc/gost34/50_34_698_90.pdf

11. Перелік документів системи технічного захисту інформації (НД ТЗІ). 2021. URL: https://cip.gov.ua/ua/news/perelik-dokumentiv-sistemi-tekhnichnogo-zakhistu-informaciyi-nd-tzi

12. НД ТЗІ 3.7-003-2005. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. Наказ ДСТСЗІ СБ України від 08.11.2005 № 125 (Зміна № 1 наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806). 2005. URL: https://tzi.com.ua/downloads/3.7-003-2005.pdf.

13. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованих системах. Наказ ДСТСЗІ СБУ від 04.12.2000 № 53 (Зміна № 1 наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806). 2000. URL: https://tzi.com.ua/downloads/1.4-001-2000.pdf

14. ДСТУ ISO/IEC 27005:2015. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2011, IDT). 2015. ДП «УкрНДНЦ». URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66912

15. ДСТУ ISO 31000:2018. Менеджмент ризиків. Принципи та настанови (ISO 31000:2018, IDT). 2018. URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=80322

16. ДСТУ ISO/IEC 27000:2019. Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів (ISO/IEC 27000:2018, IDT). 2018. URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=85795

17. Постанова Кабінету Міністрів України від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури». 2019. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text

18. Закон України «Про захист інформації в інформаційно-комунікаційних системах». 1994. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

19. Постанова Кабінету Міністрів України від 29 березня 2006 р. № 373. Київ. «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах». 2006. URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text

20. Наказ Адміністрації Держспецзв'язку від 06 жовтня 2021 року № 601 «Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури». 2021. URL: https://cip.gov.ua/ua/docs/nakaz-administraciyi-derzhspeczv-yazku-vid-06-

zhovtnya-2021-roku-601-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-pidvishennya-rivnya-kiberzakhistu-kritichnoyi-informaciinoyi-infrastrukturi.

21. Stouffer K., Pillitteri V., Abrams M., Hahn A. NIST Special Publication 800-82 Guide to Industrial Control Systems (ICS) Security. NIST. 2015. No. 2. P. 1–247.

22. Understanding IEC 62443. IEC. 2021. Resource access mode: https://www.iec.ch/blog/understanding-iec-62443

23. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту системи управління інформаційною безпекою. (ISO/IEC 27001:2013; Cor 1:2014, IDT) Вимоги. 2015. URL: http://online.budstandart.com/ua/catalog/doc-page?id_doc=66910

24. Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України «Про затвердження Положення про державну експертизу в сфері технічного захисту інформації» від 16.05.2007 № 93. URL: https://zakon.rada.gov.ua/laws/show/z0820-07#Text

25. The Syntax of Predicate Logic. LX 502 – Semantics. 2008. Resource access mode: https://www.bu.edu/linguistics/UG/course/lx502/_docs/lx502-predicate%20logic%201.pdf

Надійшла до редакції 01.12.2021