КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.28.859
УДК 004. 004.056.5:623.74

Толюпа Сергій Васильович
д.т.н., професор, професор кафедри кібербезпеки та захисту інформації
Київський національний університетімені Тараса Шевченка, Київ, Україна
ORCID ID: 0000-0002-1919-9174
serhii.toliupa@knu.ua

Кулько Андрій Аркадієвич
аспірант кафедри кібербезпеки та захисту інформації
Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID ID:0009-0006-1185-0774
kulko452@gmail.com

ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОСТІ СКЛАДНИХ ІНФОРМАЦІЙНИХ ТА ТЕХНОЛОГІЧНИХ СИСТЕМ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація. У даному матеріалі висвітлюються критичні аспекти забезпечення захищеності складних інформаційних систем об'єктів критичної інфраструктури (КІ) в умовах сучасних загроз, зокрема збройної агресії та кібератак. Зазначається висока взаємозалежність елементів КІ та їхня вразливість до нових типів загроз попри значні зусилля із захисту. Визначено чотири типи об'єктів за рівнем потенційної небезпеки та особливості функціонування КІ як сукупності взаємопов'язаних кіберфізичних елементів, що вимагають комплексного підходу до захисту. Детально аналізуються три основні підходи до забезпечення захищеності: нормативний підхід, який базується на використанні чітко визначених норм, стандартів та регламентів. Ймовірнісний підхід (надійності): грунтується на оцінці ймовірності досягнення граничного стану при кібервпливі. Ризиковий підхід (управління ризиком): інтегральний підхід, що базується на оцінці ймовірності реалізації граничних станів (P) та можливих збитків (L) від такої реалізації. У статті проведено порівняльний аналіз цих підходів, відзначено їхні переваги та недоліки, а також розглянуто умови, за яких вони можуть бути еквівалентними. Показано, що хоча нормативний підхід є базовим, ймовірнісний та ризиковий підходи надають більш обґрунтовані та математично коректні засоби врахування невизначеностей та оптимізації захисту. Зазначено необхідність поєднання переваг різних підходів для створення по-справжньому захищених систем КІ.

Ключові слова: безпека; кібербезпека; захищеність; ризик; можливість відмови; інформаційна система; критична інфраструктура; кіберпростір; кібератака.

ВСТУП

В умовах триваючої збройної агресії росії проти України, забезпечення безпеки людини, суспільства та держави значною мірою залежить від стабільної роботи об'єктів критичної інфраструктури. Окрім використання летальної зброї для фізичного впливу, росія разом із союзниками активно застосовує кіберзброю для атак на системи управління таких об'єктів через кіберпростір. Особливе занепокоєння викликає той факт, що об'єкти критичної інфраструктури, які діють у єдиному інформаційному просторі та використовують сучасні інформаційні технології, попри значні зусилля для протидії втручанню через кіберпростір, залишаються вразливими до нових типів загроз. Така ситуація ускладнює перспективи забезпечення стійкості та безпеки на тривалий час. Забезпечення захисту складних технічних систем, які функціонують на об'єктах критичної інфраструктури, є єдиним з ключових умов стабільного розвитку сучасного суспільства. Критична інфраструктура охоплює об'єкти та системи, від яких залежить

безпека, економічна стабільність та добробут держави і населення, такі як енергетика, транспорт, телекомунікації, охорона здоров'я та інші галузі [1].

Аналіз останніх досліджень і публікацій. Питання захисту критичної інфраструктури (КІ) перебуває в центрі уваги науковців, що підкреслюється значною кількістю досліджень у цій галузі. Сучасні загрози, особливо в умовах гібридної війни та кібератак, роблять цю тему надзвичайно актуальною як для теоретичної розробки, так і для практичного впровадження рішень.

Аналіз наявних публікацій демонструє широкий спектр досліджень, що охоплюють різноманітні аспекти захисту КІ. Наприклад, деякі роботи, як-от [2], зосереджуються на методологіях синтезу інтелектуальних систем управління та безпеки для об'єктів КІ, які суттєво відрізняються за своїми властивостями. Інші, такі як [3], приділяють увагу проблемам виявлення вторгнень та розробці методологічних основ для аналізу та синтезу функціонально стійких розподілених інформаційних систем**.** Це досягається завдяки використанню мультиагентних технологій, що забезпечують своєчасне виявлення та блокування кібернетичних впливів.

Публікації також глибоко занурюються в теорію та практику інтелектуального аналізу даних**.** У роботі [4] розглядаються алгоритми, моделі, задачі класифікації, кластерного аналізу, пошуку, а також глибинний аналіз даних і теорія складних мереж (Complex Networks). Це надає необхідні відомості для математичного та комп'ютерного моделювання й аналізу складних систем та мереж у сфері кібербезпеки. Крім того, дослідження, подібні до [6], вивчають сучасний стан та перспективи розвитку механізмів кібербезпеки, інформаційної безпеки, безпеки інформації та інформаційних технологій як ключових складових загальної безпеки.

У цілому, наукові публікації за цією темою охоплюють широкий діапазон проблем, починаючи від фундаментальних теоретичних підходів і закінчуючи конкретними технічними рішеннями та організаційними заходами, що відображає комплексний характер викликів, пов'язаних із захистом критичної інфраструктури.

Особливий акцент у публікаціях робиться на системному характері проблеми та необхідності комплексного підходу. Це пов'язано з тим, що КІ — це не просто сукупність окремих об'єктів, а складна взаємопов'язана мережа, збій в одному елементі якої може мати каскадні наслідки для всієї системи та держави в цілому. Багато публікацій присвячені розробці національних стратегій кібербезпеки та їх адаптації до умов воєнного стану. Обговорюються моделі та фреймворки (наприклад, NIST Cybersecurity Framework), що можуть бути використані для оцінки та покращення рівня захищеності. Досліджуються питання гармонізації українського законодавства у сфері КІ з міжнародними стандартами та найкращими практиками (наприклад, Директива NIS2 Європейського Союзу). Значна увага приділяється концепції «кіберстійкості» (cyber resilience), яка передбачає не тільки запобігання атакам, а й здатність системи швидко відновлюватися після інцидентів та зберігати основні функції. Публікації розглядають міждисциплінарний підхід, що поєднує технічні, організаційні, правові та кадрові аспекти захисту КІ.

Дослідження активно вивчають нові типи кіберзагроз, включаючи атаки на промислові системи управління (ICS/SCADA), використання штучного інтелекту для атак, зростання кількості атак, спонсорованих державами.

Аналізуються вразливості кіберфізичних систем, які поєднують IT-компоненти з фізичними процесами, що робить їх особливо чутливими до кібервпливу (наприклад, атаки на енергетичні системи, транспортні мережі).

Окремо розглядаються «людський фактор» як джерело вразливостей (інженерія соціальних мереж, недостатня обізнаність персоналу) та методи протидії йому.

Проводиться аналіз конкретних інцидентів та кібератак на українську КІ, що дозволяє вивчати тактики та інструменти агресора та розробляти ефективніші заходи захисту.

Велика увага науковців приділяється технічним рішенням та методам захисту КІ. Системи виявлення вторгнень (IDS/IPS): Досліджуються нові архітектури та алгоритми для підвищення ефективності IDS, зокрема, використання ансамблевих класифікаторів та машинного навчання для ідентифікації аномалій та відомих типів атак. Це включає застосування таких алгоритмів, як баєсівські мережі, наївний Баєс, JRip, MLP, IBK, PART, J48. Використання графів (DAG) та топологічного сортування: публікації демонструють застосування орієнтованих ациклічних графів (DAG) для моделювання залежностей, потоків даних та ланцюжків атак у системах КІ. Алгоритм Кана та DFS-based алгоритми використовуються для аналізу послідовності подій, визначення пріоритетів усунення вразливостей та планування оновлень. Безпека промислових систем управління (ICS/SCADA): це окремий, дуже важливий напрямок, оскільки традиційні ІТ-засоби безпеки не завжди ефективні для цих систем. Розробляються специфічні підходи до сегментації мереж, моніторингу трафіку та виявлення аномалій у технологічних процесах. Криптографічні методи: забезпечення конфіденційності, цілісності та автентифікації даних у системах КІ. Резервування та відмовостійкість: розробка архітектур, що забезпечують безперервність функціонування навіть у разі часткових відмов або атак. Також в наукових публікаціях по захисту критичної інфраструктури приділяється велика увага математичнному моделюванню та кількісній оцінці захищеності. Дослідження зосереджені на розробці математичних моделей для оцінки ризиків та ймовірності досягнення граничних станів. Це включає використання теорії ймовірностей, марковських процесів, дерев відмов. Публікації прагнуть подолати суб’єктивність нормативного підходу, пропонуючи кількісні методи оцінки захищеності та ефективності заходів безпеки. Аналізується взаємозв’язок між запасом міцності (нормативний підхід) та ймовірністю відмови (ймовірнісний підхід), що дозволяє інтегрувати ці концепції.

Сучасні публікації чітко вказують на зміну парадигми захисту КІ: від орієнтації виключно на запобігання атакам до формування комплексної кіберстійкості, що включає здатність до виявлення, реагування, відновлення та адаптації. Акцент зміщується від суто технічних рішень до інтегрованих підходів, що поєднують математичне моделювання, інтелектуальні системи, організаційні заходи та постійний моніторинг.

В умовах повномасштабної війни, особливого значення набуває досвід України у протидії кібератакам на КІ, який стає предметом вивчення та обговорення на міжнародному рівні. Це веде до подальшого розвитку досліджень у напрямку адаптивних систем захисту, що здатні реагувати на нові, невідомі раніше загрози, а також до розробки ефективних стратегій відновлення після інцидентів.

На сьогодні вирішення питань забезпечення безпеки в ІС та управління станом їх захищеності висвітлені в роботах вітчизняних та закордонних дослідників, а саме: Бучика С.С., Бурячка В.Л., Грищука Р.В., Ланде Д.В., Горбенка І.Д., Гнатюка С.О., Корченко О.Г., Євсеєва С.П., Кучука Г.А., Субача І.Ю., Кузнецова О.О., AlbersP., Begni A. та інших.

Постановка проблеми дослідження. Складні технічні системи, інтегровані в критичну інфраструктуру, мають традиційно високу взаємозалежність, включають елементи кіберфізичних систем і функціонують в умовах постійного підвищення ризиків. Це можуть бути кібератаки, техногенні аварії, природні катаклізми або людський фактор. У

цьому контексті особливо актуальним є розроблення та впровадження підходів до забезпечення їхньої захисту, що враховують як технічні, так і організаційні.

При аналізі та забезпеченні захищеності критичних інфраструктур також як і техносфери загалом, прийнято виділяти об'єкти чотирьох типів, які відрізняються за рівнем потенційної небезпеки та вимогами щодо забезпечення їх захищеності: об'єкти технічного регулювання, небезпечні виробничі об'єкти, критично важливі об'єкти, захищеність яких забезпечується у відповідності до категорізації ОКІ [6], стратегічно важливі об'єкти, захищеність яких впливає на стан національної безпеки.

Зазначені об'єкти відносяться до категорії складних технологічних систем (СТС) як із погляду складності їх структури, і з погляду складного характеру взаємодії їх елементів Для зазначених систем характерні різні граничні стану та механізми їх досягнення, вивчення яких використовуються принципово різні методи.

Критична інфраструктура (CI — critical infrastructure) підтримує основні послуги, необхідні для функціонування складного сучасного суспільства. Серйозний збій в наданні таких інформаційних послуг, як транспорт та енергетика, не говорячи вже про військові об'єкти, може зробити великі групи населення уразливими до дестабілізації та впливу на обороноздатність країни. Залежність від своєчасних автоматизованих логістичних ланцюжків поставок також може погіршити наслідки. Об'єкти критичної інфраструктури формуються на основі об'єднання інформаційно-комунікаційних технологій комп'ютерних систем з елементами кіберпростору на основі технологій безпровідних мереж та мобільних інтернет-технологій. Саме це поєднання дозволяє стверджувати, що такі системи відносяться до об'єктів критичної інфраструктури – сукупність взаємопов'язаних елементів, об'єднаних в єдине ціле, правильність функціонування та взаємодії яких значно впливає на кібернетичну безпеку держави протягом певного інтервалу часу [7].

На рис. 1 наведений взаємозв'язок структури об'єктів критичної інфраструктури, на прикладі організацій транспортного сектору.

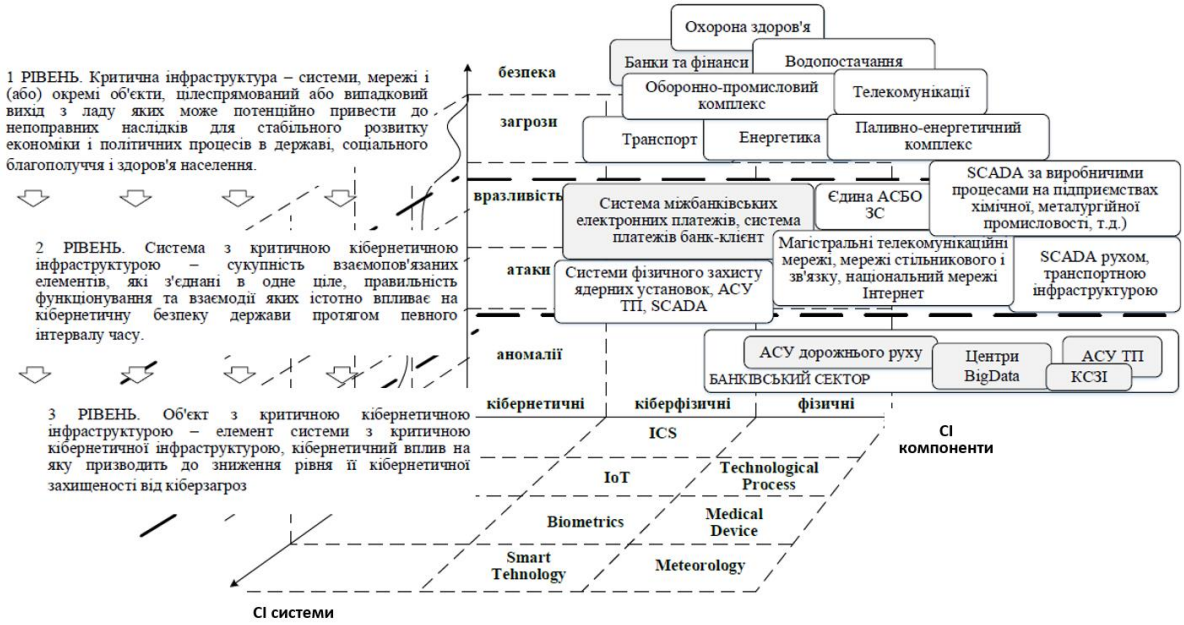

Рис. 1 Схема взаємозв'язку структури об'єктів критичної інфраструктури на прикладі організацій транспортного сектору [1]

Захищеність об'єктів критичної інфраструктури визначається її здатністю протистояти реалізації різних граничних станів її елементів, а також не допускати катастрофічних відмов на етапах функціонування системи після досягнення граничних станів її окремими елементами. Захищеність обєктів СІ доводиться забезпечувати за умов високого рівня невизначеності щодо інтенсивності експлуатаційних навантажень та зовнішніх впливів на систему (природнього характеру, вибухової хвилі) з одного боку, а також несучої здатності відповідальних елементів критичної інфраструктури на різних етапах циклу її експлуатації, з іншого. Джерелами невизначеностей є: природна варіативність параметрів системи та зовнішнього середовища, обмеженість знань про події та процеси, що протікають у складних системах СІ; неточність наявних статистичних даних та існуючих оцінок; недосконаліть контрольно-вимірювального обладнання та математичних моделей [8].

Широке розмаїття методів забезпечення захищеності під час проектування складних інформаційно-технологічних систем розробляється у межах трьох принципово різних підходів.

Нормативний підхід. Перший підхід це нормативний, який здійснює забезпечення захищеності на основі забезпеченні стійкості за основними механізмами досягнення граничних станів.

Він базується на використанні чітко визначених норм, стандартів [9] і регламентів, які спрямовані на забезпечення стабільного функціонування систем в умовах наближення до граничних станів. Цей підхід враховує наявність критичних меж, за якими інформаційна система може втратити працездатність або перейти до аварійного стану [10].

Суть підходу заключається в ідентифікації граничних станів інформаційної інфраструтури: граничний стан — це стан, за якого система або її окремі компоненти втрачають здатність виконувати задані функції. Граничні стани інформаційної інфраструктури можуть характеризуватися за різними критеріями: пов'язані з продуктивністю та навантаженням, з надійністю та відмовостійкістю, з безпекою, функціональністю та зручністю використання.

У межах нормативного підходу встановлюються чисельні показники (норми), які визначають допустимі рівні навантаження, показники продуктивності (час відгуку (response time), кількість транзакцій в секунду (TPS — Transactions Per Second), кількість запитів в секунду (RPS — Requests Per Second), пропускна здатність (Throughput), завантаження процесора (% CPU Utilization), використання оперативної пам'яті (% Memory Usage); показники надійності та доступності (Reliability and Availability Metrics): час безвідмовної роботи (Uptime), середній час між відмовами (MTBF — Mean Time Between Failures), середній час відновлення (MTTR — Mean Time To Recovery), кількість інцидентів і т. ін. Резервування ресурсів і механізмів: забезпечення захищеності та кіберстійкості досягається через створення запасів за основними параметрами системи. Це можуть бути: резервні потужності; запас комплектуючих; резервні компоненти для дублювання функцій у разі відмови основних. Механізми забезпечення стійкості до навантажень: у рамках цього підходу враховуються не лише поточні режими роботи системи, але й сценарії надзвичайних ситуацій [11]. Для цього розробляються механізми, які дозволяють: контролювати параметри системи в реальному часі; забезпечувати автоматичний перехід до аварійних режимів без втрати працездатності; впроваджувати алгоритми адаптивного керування для уникнення критичних станів, а також використання методів інтелектуального анлізу даних [12] для протидії вторгненням в дані системи. Нормативно-правове регулювання: забезпечення відповідності

технологічних систем встановленим стандартам і нормам є важливою складовою підходу. Це включає міжнародні стандарти (ISO, IEC) та національні регламенти, які визначають: вимоги до проєктування та експлуатації систем критичної інфраструктури; порядок оцінки ризиків і планування заходів захисту [13]; обов'язки операторів критичної інфраструктури. Оцінка і моніторинг ризиків: граничні стани часто пов'язані з ризиками, які необхідно виявляти й аналізувати. Нормативний підхід передбачає регулярний моніторинг основних параметрів системи, щоб передбачити момент, коли вона може досягти критичних меж.

Переваги підходу: чітка регламентація дій і процедур, зменшення ймовірності критичних збоїв через завчасне резервування; прогнозованість функціонування системи навіть у складних умовах. Недоліки: може бути недостатньо гнучким у динамічно змінних умовах; високі витрати на створення та підтримку резервів.

Можна зробити висновок, що нормативний підхід є базовим у забезпеченні захищеності складних інформаційних систем, оскільки дає змогу чітко визначити критичні межі функціонування і вжити завчасних заходів для їх подолання. Він ефективний у поєднанні з іншими методологіями, які враховують оперативне реагування та адаптацію до нестандартних ситуацій та кібервпливу.

Ймовірнісний підхід. Другий підхід оснований на забезпеченні захищеності за критерієм надійності, що ґрунтується на оцінці ймовірності досягнення граничного стану (ймовірнісний підхід) при кібервпливі.

В даному випадку розглядається розробка та застосування ансамблевих класифікаторів для підвищення ефективності систем виявлення вторгнень (СВВ) у критичній інфраструктурі. З огляду на зростаючу складність кібератак і високі вимоги до надійності та безперебійності функціонування об'єктів критичної інфраструктури, традиційні методи виявлення вторгнень часто виявляються недостатньо ефективними. Пропонується використання підходу, що базується на комбінуванні рішень декількох індивідуальних класифікаторів, що дозволяє значно покращити точність і зменшити кількість хибних спрацьовувань СВВ. Досліджуються різні методи побудови ансамблів, а також їх застосування до специфічних типів мережевого трафіку та загроз, характерних для критичної інфраструктури. Оцінюється продуктивність запропонованих моделей на реальних або синтетичних наборах даних, демонструючи їхню здатність ефективно ідентифікувати аномалії та відомі типи атак, підвищуючи тим самим кіберстійкість критичної інфраструктури. Фреймворк виявлення вторгнень використовується для розрізнення та аналізу системних атак, тому IDS (система виявлення вторгнень) повинна бути оновлена, щоб вона могла моніторити фреймворк і викликати сповіщення в системі. Багато алгоритмів було запропоновано різними авторами для покращення виконання IDS, але вони все ще не можуть надати належного або повного рішення. У запропонованій фреймворку запропоновано дослідження різних комбінацій класифікаторів баєсівської мережі, наївного Баєса, JRip, MLP, IBK, PART та J48. Більше того, для кожної комбінації будуть застосовані дві процедури попередньої обробки: нормалізація та дискретизація. Перевагою запропонованого підходу є об'єднання виявлення більшості атак з відповідною технікою попередньої обробки. Таким чином, будь-який тип атаки в мережі може бути виявлений з найкращою точністю.

Таким чином даний метод грунтується на ймовірності досягнення критичного стану при кібервпливі, є важливим інструментом для прогнозування та попередження збоїв у складних інформаційних системах. Основна ідея полягає у використанні математичних методів і теорії ймовірностей для оцінки й управління ризиками, пов'язаними з функціонуванням системи [14].

Суть підходу обумовлюється наступними складовими: граничний стан як основа аналізу. Граничний стан — це стан системи, за якого вона втрачає працездатність або переходить у аварійний режим. При цьому важливо визначити: основні параметри, які характеризують цей стан; умови, за яких ці параметри досягають критичних значень. Оцінка ймовірності відмови: використовуючи статистичні дані та моделі надійності, оцінюється ймовірність того, що система або її компоненти досягнуть граничного стану протягом заданого проміжку часу. Це включає: аналіз відмов компонентів системи; розрахунок сукупної ймовірності відмови для всієї системи; оцінку часових інтервалів між відмовами. Розробка моделей надійності [15] для прогнозування функціонування системи використовуються математичні моделі, наприклад: марковські процеси, що дозволяють моделювати зміну станів системи у часі; моделі дерев відмов, які ідентифікують можливі сценарії виходу з ладу; функції щільності ймовірності, які описують розподіл часу до настання відмови. Доцільно використовувати баєсові мережі (Bayes Network) [16], засновані на ймовірнісній моделі. Вона представляє набір випадкових змінних з їх умовними залежностями за допомогою орієнтованого ациклічного графа (DAG) [17]. Вона використовує різні алгоритми пошуку та метрики якості. Баєсова мережа пов'язує лише той конкретний вузол, який імовірно пов'язаний деякими причинно-наслідковими залежностями, що значно економить обчислення. Немає необхідності зберігати всі можливі конфігурації стану, єдине, що потрібно, це пов'язати з усіма можливими пов'язаними комбінаціями множин. Це значно економить обчислення та пам'ять. Ще одна причина використання баєсової мережі полягає в тому, що вони є адаптивними [18]. Вона починає з невеликих та обмежених знань про домен і отримує нові знання. Отже, не потрібно зберігати повні знання про екземпляр або домен. Перевага використання баєсової мережі полягає в тому, що ймовірності не обов'язково повинні бути точними. Це повинні бути приблизні ймовірності. Вона використовує причинно-наслідкові умовні ймовірності, а не зворотні, для оцінки. Тому що краще оцінювати ймовірності «у прямому напрямку».

Орієнтовані ациклічні графи (DAG) знаходять широке застосування в кібербезпеці завдяки своїй здатності моделювати послідовні залежності, потоки та причинно-наслідкові зв'язки без циклічних повторень. Математичний апарат DAG дозволяє формалізувати, аналізувати та візуалізувати складні взаємодії в системах безпеки.

Покажемо застосування графа для наших цілей $G = (V, E)$, де: V - це множина вершин (активи: сервери, робочі станції, мережеві пристрої, бази даних, програми, користувачі; вразливості: CVE-ідентифікатори, неправильні конфігурації; загрози/атаки: конкретні методи атаки (наприклад, фішинг, SQL-ін'єкція, експлуатація вразливості), інциденти безпеки; контролі безпеки: фаєрволи, системи виявлення вторгнень (IDS), антивіруси, політики доступу; дії зловмисника: кроки в «ланцюжку атаки» (kill chain); події безпеки: логи, алерти SIEM. E — це множина орієнтованих ребер, які моделюють: відносини «має уразливість»: від активу до вразливості; відносини «використовує»: від однієї служби до іншої; відносини «залежить від»: залежність між компонентами системи; відносини «спричиняє/може призвести до»: від уразливості до потенційної компрометації, від дії зловмисника до наступної дії; послідовність подій: у логах або інцидентах; потік даних: у мережевих з'єднаннях.

Також тут доцільно використовувати матриці та списки суміжності, а також топологічне сортування.

Матриця суміжності A: $A_{ij}=1$ може означати, що актив i має уразливість j, або що подія i передує події j, або що зловмисник може перейти з активу i на актив j.

Застосовується для виявлення прямих зв'язків. Наприклад, щоб швидко перевірити, які активи вразливі до певного типу атаки, або які системи безпосередньо взаємодіють.

Список суміжності: ефективний для представлення залежностей, коли система дуже велика, але зв'язків між окремими елементами відносно мало (наприклад, у мережевих графах). Застосовується для побудови графів мережевих залежностей, де кожна вершина — це пристрій, а ребро — мережеве з'єднання.

Топологічне сортування — це ключова операція для DAG-ів у сфері кібербезпеці. Воно дозволяє визначити послідовність, у якій події або кроки атаки відбуваються, що є критично важливим для розуміння інцидентів та планування захисту.

Так алгоритм Кана або DFS-based може бути використаний для: відтворення ланцюжка атаки (Kill Chain Reconstruction): впорядкування зафіксованих подій безпеки у хронологічному або логічному порядку, щоб зрозуміти, як розвивалася атака. Наприклад, з логів подій можна побудувати DAG залежностей, а потім топологічно відсортувати їх для отримання послідовності атаки; аналіз залежностей між уразливостями/активами: визначення пріоритету виправлення уразливостей, коли одна вразливість може бути експлуатована для доступу до іншої, або для компрометації наступного активу; планування патчів та оновлень: якщо оновлення одного компонента системи залежить від іншого, топологічне сортування допоможе визначити правильний порядок встановлення; аналіз потоків виконання програм: для виявлення потенційних логічних бомб або вбудованих зловмисних функцій.

Розглянемо математичний апарат алгоритму Кана та DFS-based алгоритму для топологічного сортування орієнтованого ациклічного графа (DAG).

Алгоритм Кана (Kahn's algorithm) заснований на ідеї поступового видалення вершин, які не мають вхідних залежностей. Це ітеративний алгоритм.

Вхідні дані: орієнтований ациклічний граф (DAG) $G = (V, E)$, вхідний ступінь (In-degree) вершини v: позначається indegree (v) — це кількість ребер, що входять у вершину u.

Ключові концепції та структури даних: indegree (v) для всіх $v \in V$: для кожної вершини необхідно обчислити її вхідний ступінь. Це можна зробити за час $O(|V|+|E|)$ шляхом ітерування по всіх ребрах та інкрементування лічильника для кінцевої вершини кожного ребра; черга Q (Queue): структура даних для зберігання вершин, готових до обробки (тобто тих, що мають вхідний ступінь 0); список результатів L (Result List): список, в якому буде зберігатися топологічно відсортована послідовність вершин.

Алгоритмічні кроки. Ініціалізація: обчислити indegree (v) для всіх $v \in V$. Ініціалізувати чергу Q усіма вершинами v такими, що indegree (v)=0, ініціалізувати порожній список L, ініціалізувати лічильник count = 0 (кількість вершин, доданих до L).

Поки черга Q не порожня: видалити вершину u з початку черги Q, додати u до списку L. Збільшити count на 1. Для кожної вершини v такої, що існує ребро $(u,v) \in E$ (тобто v є сусідом u): зменшити indegree(v) на 1. Якщо indegree (v) стає 0, додати v до черги Q.

Після завершення циклу, якщо count $v = |V|$ (загальній кількості вершин у графі), це означає, що граф містить щонайменше один цикл, і топологічне сортування неможливе. В іншому випадку, список L містить топологічно відсортовану послідовність вершин.

Алгоритм Кана гарантує, що кожна вершина додається до списку L лише після того, як всі її попередники (вершини, з яких йдуть ребра до неї) вже були додані. Це забезпечує виконання умови топологічного сортування: якщо існує ребро (u,v), то u завжди з'явиться в L раніше за v.

Коли indegree (v) стає 0, це означає, що всі вхідні ребра до v були оброблені (тобто їх початкові вершини вже були додані до L). Складність заключається в тому, що час:

$O(|V|+|E|)$, оскільки кожна вершина додається та видаляється з черги один раз, і кожне ребро обробляється один раз (коли зменшується вхідний ступінь його кінцевої вершини).

Використання математичного апарату DAG дозволяє перейти від інтуїтивного розуміння до формального аналізу складних взаємодій у кібербезпеці, що є критично важливим для проактивного захисту та ефективного реагування на інциденти.

Резервування для підвищення надійності: оцінка ймовірності досягнення граничного стану дозволяє обґрунтувати необхідність резервування ключових елементів системи. Резервування може бути: активним (усі резерви функціонують паралельно); пасивним (резерви активуються у разі відмови основного компонента) [18]. Контроль і моніторинг стану: використання підходу передбачає постійний моніторинг системи для своєчасного виявлення ознак наближення до граничного стану. Дані з сенсорів, логів і інших джерел аналізуються для оцінки поточного рівня надійності та ризику відмови. Критерій прийнятності ризику: визначається допустимий рівень ризику відмови системи. Якщо оцінена ймовірність перевищує цей рівень, вживаються додаткові заходи захисту, такі як модернізація компонентів, посилення систем безпеки або підвищення якості обслуговування.

Переваги підходу: забезпечує кількісну оцінку ризиків, дозволяє прогнозувати час до відмови, підвищує ефективність управління захищеністю через оптимізацію резервів і ресурсів та застосування інтелектуального підходу в управлінні. Недоліки: високі вимоги до точності вхідних даних; складність реалізації для систем із багатьма взаємозалежними процесами.

Таким чином можна зробити висновок, що підхід до забезпечення захищеності за критерієм надійності дозволяє зосередитися на ймовірнісному аналізі ризиків та розробці заходів, спрямованих на зменшення імовірності досягнення граничного стану. Це забезпечує системний і науково обґрунтований підхід до захисту складних інформаційних та технологічних систем.

Підхід на основі управління ризиками. Третій підхід до забезпечення захищеності за критерієм ризиків ґрунтується на оцінці ймовірності реалізації граничних станів та збитків від такої реалізації (далі підхід, заснований на управлінні ризиком).

Він базується на оцінці ймовірності реалізації граничних станів і можливих збитків, є інтегральним підходом до управління безпекою складних інформаційних систем. Його основна мета — не лише знизити ймовірність виникнення критичних ситуацій, а й мінімізувати наслідки від їх реалізації.

Основними підходами реалізації даного підходу є: ризик як ключовий параметр у межах якого він визначається як комбінація двох складових: ймовірності реалізації граничного стану (P) — наскільки ймовірно, що система або її компоненти досягнуть критичного стану через відмови чи враження, зовнішні впливи або людські помилки; можливих збитків (L) від реалізації цього стану — включає матеріальні втрати, шкоду довкіллю, загрозу здоров'ю або життю людей.

Ризик можна виразити формулою:

$$R = P \times LR \ = \ P / times \ L$$

Оцінка ймовірності граничних станів: використовуються методи аналізу надійності системи, моделі загроз та зловмисника, моделювання сценаріїв розвитку аварійних ситуацій; теоретико-імовірнісні моделі, такі як марковські процеси чи дерева подій.

Оцінка збитків: прямі, непрямі, непоправні збитки.

1. Пріоритезація ризиків: ризики класифікуються за критеріями «високий», «середній» і «низький» залежно від їх величини RR. Пріоритет надається заходам, спрямованим на зменшення ризиків із високим значенням.

Заходи управління ризиками: у рамках підходу передбачено чотири основні стратегії: уникнення ризику, тобто зміна проєктних рішень чи процесів для виключення критичних ситуацій; зменшення ймовірності через впровадження технологій і процедур для підвищення надійності системи; зменшення збитків за рахунок застосування систем захисту (міжмережевих екранів, адаптивних систем), страхування ризиків; прийняття ризику через резервування ресурсів для покриття збитків у разі реалізації.

2. Моніторинг і аналіз ризиків: постійний контроль ризиків забезпечує адаптацію заходів захисту до змін у системі або зовнішньому середовищі. Це включає регулярний перегляд оцінок ризиків і внесення коректівів у стратегії їх зниження.

Переваги підходу: інтегральний підхід, що враховує як імовірність, так і наслідки, дозволяє ефективно розподіляти ресурси, концентруючись на найкритичніших загрозах, гнучкість і адаптивність до змін у системі. Недоліки: складність у кількісній оцінці збитків, особливо нематеріальних; залежність від точності вихідних даних і моделей, можливість недооцінки рідкісних, але катастрофічних подій.

Таким чином можна зробити висновок, що підхід за критерієм ризиків є ефективним інструментом для забезпечення захищеності складних систем критичної інфраструктури. Він дозволяє не лише зосередитися на запобіганні відмовам, але й забезпечує підготовку до мінімізації наслідків у разі їх виникнення, що робить систему більш стійкою до зовнішніх і внутрішніх загроз.

Необхідно відзначити, що історично протягом багатьох століть розвивався перший підхід, при якому невизначеності, з якими стикалися при проектуванні та експлуатації систем СІ, враховувалися за допомогою введення системи коефіцієнтів запасу та резервування. Другий підхід набув поширення з розвитком таких дисциплін як теорія ймовірності та теорія надійності, що дозволяють оцінювати невизначеності за допомогою ймовірності досягнення системою граничних станів. З розвитком теорії ризику та обчислювальної техніки, набуває все більшого поширення третій підхід до забезпечення захищеності систем СІ, який дозволяє в математично більш коректній формі враховувати як невизначеності, що зумовлюють можливість досягнення граничних станів, так і розмір збитків, очікуваних під час реалізації граничних станів.

Нижче проведемо порівняльну оцінку перерахованих підходів та розглянуто умови, за яких ці підходи можуть вважатися еквівалентними. Введемо такі позначення: нехай при механізмі досягнення граничних станів, що розглядається, функція граничних станів СІ записується у вигляді:

$$g(x_1, x_2, ..., x_n) = 1 \quad (1)$$

де $g(x_1, x_2, ..., x_n)$ — функція стану системи. Розділимо змінні стани системи $x_1, x_2, ..., x_n$ на дві групи: $y_1, y_2, ..., y_m$ — випадкові змінні стани системи, $\chi_1, \chi_2, ..., \chi_k$ — параметри, що варіюються, значення яких вибираються при проектуванні. Ці параметри можуть вважатися детермінованими.

Тоді функція граничних станів записуватиметься у вигляді

$$g(y_1, y_2, ..., y_m, \chi_1, \chi_2, ..., \chi_k) = 1 \quad (2)$$

причому умова забезпечення захищеності набуває вигляду:

$$g(y_1, y_2, ..., y_n, \chi_1, \chi_2, ..., \chi_k) \le 1 \quad (3)$$

а умова руйнування

$$g(y_1, y_2, ..., y_n, \chi_1, \chi_2, ..., \chi_k) > 1 \quad (4)$$

ISSN 2663 - 4023

Для стислості запису вводяться також вектори випадкових змінних стану $\bar{Y} = (y_1, y_2, ..., y_m)$ і параметрів проектування, що варіюються $\bar{\chi} = (\chi_1, \chi_2, ..., \chi_k)$. Тоді умови (2)-(4) можуть бути записані в короткій формі:

$g(\bar{Y}, \bar{\chi})$ функція граничних станів, $g = (\bar{Y}, \bar{\chi}) \le 1$ — умова забезпечення захищеності та $g = (\bar{Y}, \bar{\chi}) > 1$- умова руйнування.

На графіку представлено залежність захищеності об'єкта від ймовірності досягнення граничного стану.

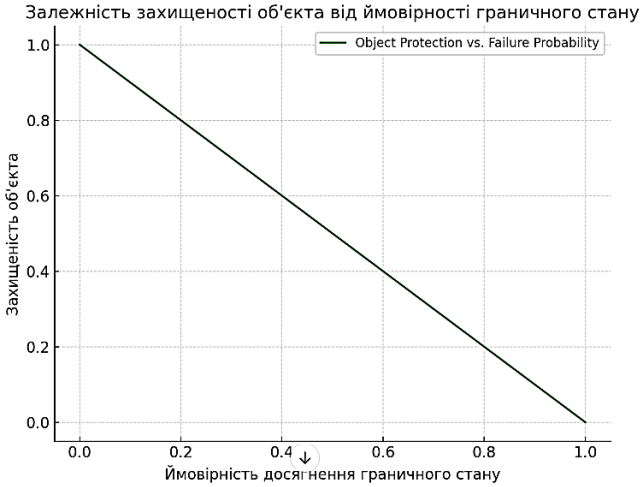

Рис. 2. Залежність захищеності об'єкта від ймовірності досягнення граничного стану

Особливості:

Ймовірність досягнення граничного стану (вісь *X*): чим вище цей показник, тим більший ризик, що система втратить працездатність.

Захищеність об'єкта (вісь *Y*): зменшується із зростанням ймовірності граничного стану, оскільки ризик відмови системи зростає.

Графік демонструє, що максимальна захищеність досягається при мінімальній ймовірності граничного стану. Це підтверджує важливість заходів, спрямованих на зменшення ймовірності відмови для забезпечення стабільності системи.

2. Нормативний підхід щодо забезпечення захищеності нормативного підходу полягає в наступному:

1) випадкові змінні $y_1, y_2, ..., y_m$ у функції станів $g(y_1, y_2, ..., y_m, \chi_1, \chi_2, ..., \chi_k)$ замінюються на відомі детерміновані величини, що характеризують їх розподіли. Зокрема, з цією метою можна використовувати математичні очікування: $E(y_1), E(y_2), ..., E(y_m)$. При такому перетворенні функція випадкових аргументів $g(y_1, y_2, ..., y_m, \chi_1, \chi_2, ..., \chi_k)$ замінюється детермінованою функцією:

$$g_0 = (\chi_1, \chi_2, ..., \chi_k) = g(E(y_1), E(y_2), ..., E(y_m)), \chi_1, \chi_2, ..., \chi_k \quad (5)$$

2) Враховуючи невизначеності, які були присутні в умови забезпечення захищеності до заміни змінних $y_1, y_2, ..., y_m$ з їхньої математичні очікування, у праву частину нерівності вводиться, як множник, передбачений нормативний (гранично допустимий) запас $[n]$.

Таким чином, умова забезпечення захищеності при нормативному підході записується як:

$$[n]\times g_0 = (\chi_1, \chi_2, ..., \chi_k) \le 1 \qquad (6)$$

Це означає, що забезпечення захищеності при нормативному підході передбачає такий вибір параметрів $\chi_1, \chi_2, ..., \chi_k$ щоб при заданому гранично-допустимому нормативному запасі $[n]$ забезпечити виконання нерівності (6).

Питання про вибір $[n]$ є дуже складним. Нормативний запас по граничному стану призначається виходячи з досвіду експлуатації подібних систем; рівня невизначеності (тобто характеру розподілів змінних $y_1, y_2, ..., y_m$ та кількості наявної інформації про ці змінні); соціально-економічних умов; точності розрахункових моделей та величини збитків, очікуваних у разі досягнення граничних станів. Таким чином, величини запасів визначаються як об'єктивними факторами так і суб'єктивними обставинами. Сучасні значення нормативних запасів елементів СІ, які стосуються різних галузей**,** змінюються у різних діапазонах.

Слід відмітити, що значення нормативних запасів варіюються у досить широких діапазонах (як усередині окремих галузей, і між галузями). Це свідчить про відсутність єдиної методологічної основи їх обгрунтування. Використання такого підходу при проектуванні нових (унікальних) об'єктів пов'язане з великими складнощами та високим рівнем невизначеності, пов'язаним із відсутністю досвіду призначення допустимих запасів за граничними станами, які можуть реалізовуватись у системі.

Слід мати на увазі, що для складних систем характерна наявність різних граничних станів $ГС_i, i = 1,2,...,q$, що відповідають різним механізмам руйнування (одноразові навантаження, кумулятивні механізми руйнування втоми і т.д.). У цьому випадку прийнято вводити систему запасів $n_1, n_2, ..., n_q$ за основними механізмами досягнення граничних станів.

Слід враховувати, що запаси по різним граничним станам виявляються не пов'язаними між собою, при цьому система може мати надлишкову захищеність за одними граничними станами і недостатньою за іншими. Для створення захищеної системи при нормативному підході організовується ітераційна процедура (рис. 3), при якій параметри проєктування $\chi_1, \chi_2, ..., \chi_k$ варіюються до того часу, поки умова забезпечення виду (6) не буде виконано.

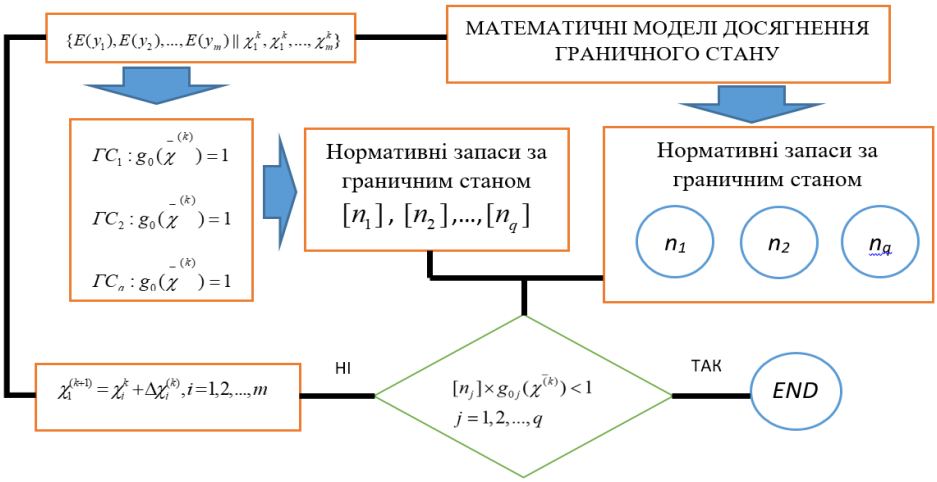

Рис. 3. Алгоритм проектування систем за нормативного підходу до забезпечення захищеності

3. Імовірнісний підхід до забезпечення безпеки СІ.

При забезпеченні захищеності складних систем СІ дедалі ширше використовуються підходи теорії надійності. При цьому система вважається захищеною, якщо виконується умова:

$$P_{\phi} < [P_{\phi}] \tag{7}$$

де P_{ϕ} — розрахункова ймовірність відмови (руйнування) системи, а $[P_{\phi}]$ — запропоноване гранично допустиме значення ймовірності відмови системи цього типу.

Будемо вважати, що для системи, що розглядається, відомі функція граничних станів (2) та функція щільності розподілу ймовірності (8).

$$f(y_1, y_1, ..., y_n | \chi_1, \chi_2, ..., \chi_m) \tag{8}$$

Тоді розрахункова ймовірність відмови буде записана у вигляді:

$$P_{\phi} = P\{g(y_1, y_1, ..., y_n, \chi_1, \chi_2, ..., \chi_m) > | \chi_1, \chi_2, ..., \chi_m\} = \int\limits_{g(Y|\chi)>1} f(y_1, y_1, ..., y_n \mid \chi_1, \chi_2, ..., \chi_m) dy_1, dy_2, ..., dy_m \tag{9}$$

або в короткій формі:

$$P_{\phi} = P\{g(\bar{Y}, \bar{\chi}) > 1 | \bar{\chi}_2\} = \int\limits_{g(Y|\chi)>1} f((\bar{Y} \mid \bar{\chi}) d\bar{Y} \tag{10}$$

Таким чином, умова забезпечення захищеності системи у постановці теорії надійності (7) може бути записана у вигляді:

$$P\{g(\bar{Y}, \bar{\chi}) > 1 | \bar{\chi}_2\} < [P_{\phi}] \tag{11}$$

Тобто забезпечення захищеності елементів СІ за критерієм надійності передбачає, що при проектуванні системи параметри $\bar{\chi}$ вибираються в такий спосіб, щоб забезпечити виконання умови (11).

3. Зіставлення нормативного та ймовірнісного підходів

Слід зазначити, що проектування та забезпечення захищеності ОКІ на основі нормативного підходу, що базується на призначенні запасів, є менш трудомістким, оскільки для того, щоб переконатися, що вираз (6) справедливий, необхідно лише один раз оцінити $g_0(\bar{\chi})$, тоді як розрахунок за критерієм надійності (11) вимагає проведення багаторазової оцінки $g_0(\bar{Y}, \bar{\chi})$. На жаль, нормативному підходу, незважаючи на його простоту, бракує суворості та точності аналізу та обліку невизначеностей. Істотний вплив в оцінці захищеності грають суб'єктивний чинник та наявність досвіду експлуатації систем даного класу у подібних умовах довкілля. Проектування та забезпечення захищеності інформаційних систем СІ за критерієм надійності, навпаки, є досить суворою математичною процедурою обліку невизначеностей, пов'язаних з навантаженнями та несучою здатністю системи. Він дозволяє приймати обґрунтовані рішення при проектуванні системи в умовах невизначеності, проводити порівняльні оцінки рівня захищеності при різних параметрах $\bar{\chi}$ системи, що проектується, і здійснювати оптимізацію системи. Однак використання ймовірнісного підходу пов'язане зі значними трудовитратами і вимагає високої кваліфікації проектувальника.

Тому було б дуже корисно поєднати переваги обох підходів, отримавши, у тих випадках, коли це можливо, залежність між запасом та ймовірністю відмови. Це дозволило

б, зокрема, спроектувавши систему із заданим запасом, оцінити її захищеність за критеріями надійності. Зіставлення областей захищених станів Ω_n та Ω_p , отриманих відповідно за критерієм запасу та критерієм надійності, є окремим актуальним завданням.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ.

В умовах триваючої збройної агресії росії проти України, забезпечення стабільної роботи об'єктів критичної інфраструктури (КІ) є життєво важливим для безпеки людини, суспільства та держави. Агресор не обмежується фізичними атаками, активно застосовуючи кіберзброю для впливу на системи управління КІ. Це створює нові виклики для стійкості та безпеки, оскільки сучасні КІ, що функціонують у єдиному інформаційному просторі з використанням передових інформаційних технологій, залишаються вразливими до нових типів загроз, попри значні зусилля із протидії.

Складні інформаційно-технологічні системи, інтегровані в КІ, характеризуються високою взаємозалежністю, включають кіберфізичні елементи та функціонують в умовах постійно зростаючих ризиків (кібератаки, техногенні аварії, природні катаклізми, людський фактор). Це підкреслює актуальність розробки та впровадження комплексних підходів до їхнього захисту, що поєднують технічні та організаційні аспекти.

Критична інфраструктура охоплює широкий спектр об'єктів та систем (енергетика, транспорт, телекомунікації, охорона здоров'я), від яких залежить безпека, економічна стабільність та добробут держави.

Розрізняють об'єкти технічного регулювання, небезпечні виробничі об'єкти, критично важливі об'єкти та стратегічно важливі об'єкти, кожен з яких вимагає специфічного підходу до захисту.

Всі ці об'єкти є складними технологічними системами (СТС), що функціонують в умовах високої невизначеності (варіативність параметрів, обмеженість знань, неточність даних, недосконаліть моделей), що ускладнює забезпечення їх захищеності.

Взаємозв'язок та необхідність комбінування підходів. Проектування та забезпечення захищеності КІ за нормативним підходом є менш трудомістким, але йому бракує математичної суворості. Ймовірнісний підхід, навпаки, є суворою математичною процедурою, але вимагає значних ресурсів.

Існує потреба в поєднанні переваг всіх підходів. Це дозволило б, наприклад, оцінювати захищеність системи, спроектованої із заданим запасом (нормативний підхід), за критеріями надійності (ймовірнісний підхід). Зіставлення областей захищених станів, отриманих за різними критеріями, є актуальним завданням.

Підсумовуючи, ефективне забезпечення захищеності об'єктів критичної інфраструктури в умовах гібридної війни вимагає не просто застосування одного з підходів, а їхнього інтегрованого використання, що дозволить створити більш стійкі та адаптивні системи до постійно зростаючих загроз.

Перспективними напрямками подальших досліджень є більш глибокий аналіз класифікаторів для системи виявлення вторгнень та побудова моделі безпеки систем критичної інфраструктури з урахуванням взаємозв'язків між об'єктами захисту та зловмисниками.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Evseev, S.P. (). *Methodology for synthesizing models of intelligent control and security systems for critical infrastructure facilities*: *monograph.* Kharkiv: Novyi Svit-2000 Publishing House.
2. Yevseev, S.P., Zakovorotnyi, O.Y., Milov, O.V., Kuchuk, G.A., Galuza, O.A., Koval, M.V., Voitko, O.V., & Hryshchuk,R.V.(2024).*Methodology for synthesizing models of intelligent control and security systems for critical infrastructure facilities:monograph.* Kharkiv: Novyi Svit-2000 Publishing House.
3. Lukova-Chuyko, N. V, Toliupa, S.V., Nakonechnyi, V.S., & Brailovsky, M.M. (2021). *Intrusion Detection Systems and Functional Resilience of Distributed Information Systems to Cyber Threats: monograph.* K.: Format.
4. Lande, D.V., Subach, I.Y., & Boyarynova, Y.E. (2018). *Fundamentals of the theory and practice of data mining in the field of cybersecurity: a textbook.* K.: ISZZI KPI.5.
5. Brailovskyi, M.M., Zybin, S.V., Kobozeva, A.A., Khoroshko, V.O., & Khokhlachova, Y.E. (2021). *Analysis of cybersecurity of information systems: monograph.* K.: FOP Yamchynskyi O.V.
6. Abdalla, A., Aleshyn, G.V., Vdovychenko, I.N., et al. (2020). *Cybersecurity and Information Technology: a monograph.* Kh.: DISA PLUS LLC.
7. On Approval of Methodological Recommendations for Categorization of Critical Infrastructure Objects. (n.d.). https://zakon.rada.gov.ua/rada/show/v0023519-21#Text
8. On Critical Infrastructure, Law of Ukraine No. 1882-IX (2021) (Ukraine). https://zakon.rada.gov.ua/laws/show/1882-20#Text.
9. Yang, Z., Barroca, B., Laffréchine, K., Weppe, A., Bony-Dandrieux, A., Daclin N. (2023). A multi-criteria framework for critical infrastructure systems resilience. *International Journal of Critical Infrastructure Protection, 42, 100616*.
10. Information Technology. Methods and means of security. Information security management systems. Requirements. (DSTU ISO/IEC 27001:2022) (2022). https://my-itspecialist.com/iso-iec-27001-2022-standard.
11. Vorona, V.A., Kravchenko, M.O. (2017). *Decision support systems in information security management: KNURE.*
12. Jain, R. (2016). *The Art of Computer Systems Performance Analysis: Techniques for Experimental Design, Measurement, Simulation, and Modeling*. Wiley.
13. Lukova-Chuyko, N.V., Tolyupa, S.V., Nakonechnyi, V.S., & Brailovsky, M.M. (2021). *Intrusion Detection Systems and Functional Resilience of Distributed Information Systems to Cyber Threats: monograph.* K.: Format.
14. Gulkov, M. & Gannenko, S. (2024). An improved method for determining the residual risk in information and communication systems in assessing information vulnerability. *Modern Information Technologies in the Field of Security and Defense, 50(2),* 29–36. https://doi.org/10.33099/2311-7249/2024-50-2-29-36.
15. Sidorenko, V., & Maksymets, A. (2025). Model of ensuring the stability of critical information systems under the influence of internal and external destabilizing factors. *Electronic professional scientific publication "Cybersecurity: Education, Science, Technology", 3(27),* 560–571. https://doi.org/10.28925/2663-4023.2025.27.779/
16. Mandziy, B. A. (2013). Software implementation of the reliability model of a renewable technical system with a constant loaded reserve. *East-European Journal of Advanced Technologies, 3(9),* 18–23.
17. Murphy, K. (2011). *A brief introduction to graphical models and Bayesian networks*. Technical report 2001-5-10, department of computer science, University of British Columbia. http://genie.sis.pitt.edu/
18. Douglas, B. (2014). *West. Introduction to Graph Theory.* 2nd edition.
19. Siewiorek, D. P., & Swarz, R. S. (1998). *Reliable Computer Systems: Design and Evaluation*. A K Peters/CRC Press.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (28), 2025
ISSN 2663 - 4023

Serhii Toliupa
Doctor of Technical Sciences, Professor
Professor of the Department of Cybersecurity and Information Protection
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
ORCID ID: 0000-0002-1919-9174
serhii.toliupa@knu.ua

Andrii Kulko
Postgraduate Student of the Department of Cybersecurity and Information Protection
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
ORCID ID:0009-0006-1185-0774
kulko452@gmail.com

ENSURING THE SECURITY OF COMPLEX INFORMATION AND TECHNOLOGICAL SYSTEMS OF CRITICAL INFRASTRUCTURE FACILITIES

Abstract. This article highlights the critical aspects of ensuring the security of complex information systems of critical infrastructure (CI) facilities in the face of modern threats, in particular, armed aggression and cyberattacks. The author emphasizes the high interdependence of CI elements and their vulnerability to new types of threats despite significant protection efforts. The author identifies four types of objects according to the level of potential danger and the peculiarities of CI functioning as a set of interconnected cyber-physical elements that require an integrated approach to protection. Three main approaches to ensuring security are analyzed in detail: the normative approach, which is based on the use of clearly defined norms, standards and regulations. Probabilistic approach (reliability): based on an assessment of the probability of reaching a threshold state under cyber impact. Risk approach (risk management): an integral approach based on an assessment of the probability of realization of limit states (P) and possible losses (L) from such realization. The article provides a comparative analysis of these approaches, identifies their advantages and disadvantages, and considers the conditions under which they may be equivalent. It is shown that although the normative approach is basic, the probabilistic and risk approaches provide more reasonable and mathematically correct means of taking into account uncertainties and optimizing protection. The author emphasizes the need to combine the advantages of different approaches to create truly secure CI systems.

Keywords: security, cybersecurity; security; risk; failure; information system; critical infrastructure; cyberspace; cyberattack.

REFERENCES(TRANSLATED AND TRANSLITERATED)

1. Evseev, S.P. (). *Methodology for synthesizing models of intelligent control and security systems for critical infrastructure facilities*: *monograph.* Kharkiv: Novyi Svit-2000 Publishing House.
2. Yevseev, S.P., Zakovorotnyi, O.Y., Milov, O.V., Kuchuk, G.A., Galuza, O.A., Koval, M.V., Voitko, O.V., & Hryshchuk,R.V.(2024).*Methodology for synthesizing models of intelligent control and security systems for critical infrastructure facilities:monograph.* Kharkiv: Novyi Svit-2000 Publishing House.
3. Lukova-Chuyko, N. V, Toliupa, S.V., Nakonechnyi, V.S., & Brailovsky, M.M. (2021). *Intrusion Detection Systems and Functional Resilience of Distributed Information Systems to Cyber Threats: monograph.* K.: Format.
4. Lande, D.V., Subach, I.Y., & Boyarynova, Y.E. (2018). *Fundamentals of the theory and practice of data mining in the field of cybersecurity: a textbook.* K.: ISZZI KPI.5.
5. Brailovskyi, M.M., Zybin, S.V., Kobozeva, A.A., Khoroshko, V.O., & Khokhlachova, Y.E. (2021). *Analysis of cybersecurity of information systems: monograph.* K.: FOP Yamchynskyi O.V.
6. Abdalla, A., Aleshyn, G.V., Vdovychenko, I.N., et al. (2020). *Cybersecurity and Information Technology: a monograph.* Kh.: DISA PLUS LLC.
7. On Approval of Methodological Recommendations for Categorization of Critical Infrastructure Objects. (n.d.). https://zakon.rada.gov.ua/rada/show/v0023519-21#Text

8. On Critical Infrastructure, Law of Ukraine No. 1882-IX (2021) (Ukraine). https://zakon.rada.gov.ua/laws/show/1882-20#Text.
9. Yang, Z., Barroca, B., Laffréchine, K., Weppe, A., Bony-Dandrieux, A., Daclin N. (2023). A multi-criteria framework for critical infrastructure systems resilience. *International Journal of Critical Infrastructure Protection, 42, 100616*.
10. Information Technology. Methods and means of security. Information security management systems. Requirements. (DSTU ISO/IEC 27001:2022) (2022). https://my-itspecialist.com/iso-iec-27001-2022-standard.
11. Vorona, V.A., Kravchenko, M.O. (2017). *Decision support systems in information security management: KNURE.*
12. Jain, R. (2016). *The Art of Computer Systems Performance Analysis: Techniques for Experimental Design, Measurement, Simulation, and Modeling*. Wiley.
13. Lukova-Chuyko, N.V., Tolyupa, S.V., Nakonechnyi, V.S., & Brailovsky, M.M. (2021). *Intrusion Detection Systems and Functional Resilience of Distributed Information Systems to Cyber Threats: monograph.* K.: Format.
14. Gulkov, M. & Gannenko, S. (2024). An improved method for determining the residual risk in information and communication systems in assessing information vulnerability. *Modern Information Technologies in the Field of Security and Defense, 50(2),* 29–36. https://doi.org/10.33099/2311-7249/2024-50-2-29-36.
15. Sidorenko, V., & Maksymets, A. (2025). Model of ensuring the stability of critical information systems under the influence of internal and external destabilizing factors. *Electronic professional scientific publication "Cybersecurity: Education, Science, Technology", 3(27),* 560–571. https://doi.org/10.28925/2663-4023.2025.27.779/
16. Mandziy, B. A. (2013). Software implementation of the reliability model of a renewable technical system with a constant loaded reserve. *East-European Journal of Advanced Technologies, 3(9),* 18–23.
17. Murphy, K. (2011). *A brief introduction to graphical models and Bayesian networks.* Technical report 2001-5-10, department of computer science, University of British Columbia. http://genie.sis.pitt.edu/
18. Douglas, B. (2014). *West. Introduction to Graph Theory.* 2nd edition.
19. Siewiorek, D. P., & Swarz, R. S. (1998). *Reliable Computer Systems: Design and Evaluation*. A K Peters/CRC Press.