DOI: 10.35681/1560-9189.2022.24.1.262817

УДК 004.5

О. Г. Додонов, О. С. Горбачик, М. Г. Кузнєцова
Інститут проблем реєстрації інформації НАН України
вул. М. Шпака, 2, 03113 Київ, Україна
e-mail: dodonov@ipri.kiev.ua

Підвищення безпеки критичних інфраструктур засобами автоматизованих систем організаційного управління

Розглянуто проблему забезпечення безпеки критичних інфраструктур шляхом підвищення функціональної стійкості їхніх автоматизованих систем організаційного управління (СОУ). Проаналізовано основні завдання та функції СОУ для підвищення безпеки в умовах дії дестабілізуючих факторів. Запропоновано застосування технології динамічної реконфігурації для забезпечення виконання комплексу задач безпеки та гарантування безперервності процесу управління об'єктами критичної інфраструктури навіть за наявності небажаних впливів на інфраструктуру і появу та накопичення відмов у самій автоматизованій СОУ. Представлено реалізацію підсистеми динамічної реконфігурації в автоматизованій СОУ як апаратно-програмного комплексу, до складу якого входять модулі моніторингу, аналізу, локалізації, вибору та прийняття рішень, реалізації рішень, база даних і знань. Комплекс працює в автоматичному режимі, відбувається безперервний процес моніторингу стану системи управління та її елементів за заданими індикаторами. У разі виявлення відхилень від заданого режиму роботи, які можуть призвести до нештатних ситуацій, активізується підсистема динамічної реконфігурації. Відбувається пошук, знаходження та реалізація раціонального варіанту використання наявних ресурсів СОУ для підтримки безперервного управління об'єктом і виконання наявних управлінських завдань.

Ключові слова: *автоматизовані системи організаційного управління, безпека критичних інфраструктур, динамічна реконфігурація.*

Вступ

Зі зростанням залежності від використання комп'ютерної техніки та інформаційних технологій у бізнесі та підприємництві зростають кіберризики та кіберзагрози, і це формує нові завдання по запобіганню виникнення надзвичайних ситуацій на об'єктах критичних інфраструктур. У США як частина національного

дивізіону кібербезпеки (NCSD) функціонує спеціальна програма захисту систем управління та працює спеціальна команда реагування на кіберзагрози в промислових системах (ICS-CERT). Європейською комісією розроблено глобальну стратегію захисту критичної інфраструктури, яка передбачає комплекс заходів з профілактики, запобігання та реагування на терористичні атаки в Європі.

З початком російської агресії в Україні з'явився досвід протидії кібератакам, накопичено великий обсяг інформації, та на жаль неможна говорити про достатній рівень кібербезпеки в країні. Для критичних інфраструктур сьогодні загрозливими факторами є бойові дії на сході України, висока зношеність основних фондів, проблеми екологічної і техногенної безпеки, загрози виникнення аварій на об'єктах підвищеної небезпеки (шахтах, об'єктах електроенергетики, хімічних і металургійних підприємствах, мережах життєзабезпечення) як внаслідок їхнього випадкового пошкодження або втрати контролю над технологічними процесами, так і в результаті терористичних актів і диверсій [1]. У 2014–2021рр. в Україні неодноразово мали місце порушення у функціонуванні критичних інфраструктур: для тисяч споживачів припинялося постачання електроенергії, виходили з ладу електронні системи «Укрзалізниці», перед плануванням соцвиплат і пенсій на межі знищення були дані Держказначейства, блокувалася робота сайтів держустанов тощо.

Для створення дієвого механізму протидії кіберзагрозам Україна бере за приклад існуючу практику зарубіжних країн, узгоджуючи її із українськими реаліями. Українські фахівці активно співпрацюють з фахівцями із США. Україна заявила про своє бажання приєднатися до співтовариства Cyber Flag, що дозволить сильно розширити тренування та навчання фахівців з кібербезпеки і співпрацювати з розвинутими країнами щодо створення системи колективної безпеки в кіберпросторі під егідою Cyber Flag.

Стан проблеми

Достатньо складно оцінити безпечність критичної інфраструктури в цілому через різнорідність її складових, емержентність інфраструктури, неповноту знань про можливі відмови та наявні ризики, отримання в різних кваліметричних шкалах даних про стан і функціонування об'єктів китичної інфраструктури.

Найчастіше для оцінки ризиків для критичних систем застосовують методи детерміністського аналізу DSA (Deterministic Safety Assesment) та ймовірнісного аналізу PSA (Probabilistic Safety Analysis) [2]. DSA передбачає послідовний аналіз поведінки інфраструктури на множині правдоподібних сценаріїв розвитку аварій із застосуванням визначених правил і гіпотез стосовно стану підсистем, їхніх характеристик, дій оператора і т.д. з обмеженням щодо технічної можливості настання певної аварії. Та цей підхід не дозволяє врахувати усі існуючі невизначеності.

Імовірнісний аналіз PSA застосовується для оцінки ймовірності великих аварій, зокрема на атомних електростанціях. Основою PSA є системний аналіз можливих сценаріїв, а також послідовне дослідження аварій, включаючи вихідні події, шляхи розвитку аварійних ситуацій з урахуванням накладення відмов систем. Спершу визначаються послідовності подій, які можуть призвести до аварії, а потім виконується оцінювання стану критичного об'єкта та можливе розповсюдження наслідків аварії. На останньому етапі здійснюється оцінка впливу аварії на

здоров'я людей. Оскільки великі аварії є досить рідкісними подіями, статистичних даних недостатньо для застосування класичного ймовірнісного підходу.

Метод аналізу виду та наслідків критичних відмов FMECA (Failure Modes, Effects and Critical Analysis) передбачає систематичне, шляхом послідовного розгляду інфраструктурних підсистем, визначення усіх можливих видів відмов, пошкоджень, аварійних ситуацій і їхнього результуючого впливу на інфраструктуру й оточуюче середовище. Суть FMECA полягає у визначенні впливу кожного потенційного дефекту (відмови) на функціональність інфраструктури як системи у цілому та впорядкуванні відмов відповідно до величини очікуваного збитку. Це трудомісткий метод, та він дозволяє провести досить повний якісний аналіз причин і наслідків відмов елементів інфраструктури, не враховуючи можливу деградацію об'єктів критичної інфраструктури, час настання та залежність відмов [4].

Для аналізу ризиків іноді застосовують модифікації зазначених вище основних методів, частково долаючи їхні недоліки. Сьогодні все частіше починають залучати для аналізу методи штучного інтелекту, лінгвістичні методи, нечіткі моделі для уточнення основних видів невизначеностей, урахування залежності подій, зміни критичності відмов за наявності залежності відмов. Методи нечіткої математики, такі як нейронні мережі, нечітка логіка, генетичні алгоритми вбудовуються у технології нового покоління — «м'яких обчислень» (soft computing) [5], які застосовують для управління складними системами з дефіцитом апріорної інформації в умовах невизначеності і які дозволяють залучити досвід експертів, їхні знання для ризик-аналізу в процесі управління.

Складність і трудомісткість методів аналізу ризиків, складність математичних моделей критичних інфраструктур, неможливість врахування широкого спектра факторів, зокрема можливостей дистанційного ураження об'єктів критичної інфраструктури, реалізації загроз виникнення аварій залишають актуальними питання розробки методів підвищення безпеки критичних інфраструктур.

Формулювання цілей (постановка завдання)

Безпека критичних інфраструктур України та їхній захист мають забезпечуватися комплексом заходів, реалізованих у нормативно-правових, організаційних, технологічних інструментах і спрямованих на забезпечення як фізичної (фізичний захист), експлуатаційної, так і операційної безпеки та стійкості критичної інфраструктури [1]. Завдання статті — показати спосіб забезпечення безпеки критичних інфраструктур шляхом підвищення функціональної стійкості автоматизованих систем організаційного управління об'єктів критичних інфраструктур. Під безпекою критичної інфраструктури в такому випадку розуміють незалежність від неприйнятного ризику [6], тобто забезпечення такого стану інфраструктури, в якому ризик нанесення шкоди людині, суспільству, країні скорочується до прийнятного рівня.

Основний матеріал досліджень

Автоматизовані системи організаційного управління є складовими будь-якої сучасної критичної інфраструктури. Вони належать до класу соціотехнічних систем і включають, зокрема, комплекси апаратних і програмних засобів, інформа-

ційних систем і інформаційно-телекомунікаційних мереж, орієнтовані на вирішення задач оперативного управління та контролю за різними процесами та технічними об'єктами в рамках організації виробництва або технологічного процесу об'єкта критичної інфраструктури й інфраструктури в цілому. Тенденції розвитку автоматизованих СОУ свідчать про зростання долі важливих для безпеки критичних інфраструктур функцій, що реалізуються на базі комп'ютерних систем.

Функціонування СОУ відбувається в умовах постійної взаємодії із зовнішнім середовищем, при цьому значна частина таких взаємодій являє собою різноманітні конфлікти, що призводять до руйнації інформаційних ресурсів, порушення штатних інформаційних процесів і відповідно до унеможливлення виконання функцій системи. На СОУ, як складову критичної інфраструктури, у рамках забезпечення безпеки об'єктів критичної інфраструктури і власне інфраструктури покладається виконання наступних функцій:

— реалізація процесів організаційного управління таким чином, щоб не допустити перехід інфраструктури або її складових у потенційно небезпечний стан;

— відключення технічного об'єкта в разі появи або реалізації загрози переходу його у небезпечний (аварійний) стан;

— прогнозування, оцінювання та мінімізація ризиків безпеки під час функціонування об'єкта, напрацювання відповідних управлінських рішень.

Засобами СОУ виконується інтерпретація даних щодо стану інфраструктури і окремих її об'єктів, діагностика з виявлення та розпізнавання загроз безпеці, моніторинг у реальному масштабі часу для виявлення відхилень параметрів функціонування, а також прогнозування наслідків певних подій або явищ, планування дій щодо об'єктів інфраструктур, здатних виконати в повному обсязі чи частково свої функції. СОУ має підтримувати один із визначених для неї режимів функціонування, проводити контроль ходу та результатів виконання управлінських рішень, забезпечувати напрацювання та прийняття рішень виконанням відповідних процедур, необхідною інформацією та ресурсами.

Від функціонування автоматизованої СОУ залежить безпека функціонування об'єктів критичних інфраструктур, особливо у разі виникнення та розвитку аварійної ситуації, в умовах, коли відсутня можливість чіткого передбачення результатів управляючих впливів.

Засоби автоматизованої СОУ повинні дозволити своєчасне розпізнавання загрози та моменту настання критичної (надзвичайної, нештатної) ситуації, обрати адекватний рівень опрацювання, ініціювати процеси протидії, компенсації чи адаптації до ситуації, створити умови продовження функціонування критичної інфраструктури у повному або частковому обсязі, в разі необхідності активувати процедури поступової деградації чи безпечної зупинки функціонування інфраструктури. Функціональна стабільність/стійкість СОУ в такому випадку стає фактором і умовою безпеки об'єктів критичних інфраструктур. За показник функціональної стійкості СОУ може слугувати оцінка живучості її як системи, адже живучість характеризує можливості системи до збереження своєї функціональності у постійно змінних умовах внутрішнього та зовнішнього середовища. Завдяки притаманній їй живучості, система може зберігатись як ціле у непередбачуваних, іноді екстремальних, умовах, пристосовуватися до них, змінюючи свою поведінку, структуру чи загальносистемну ціль функціонування [7]. Якісні оцінки та кількіс-

ні показники живучості автоматизованих СОУ є інтегральними характеристиками щодо збереження чи відновлення системою виконання своїх функцій в умовах дії різного роду несприятливих впливів.

У загальному випадку живучість системи залежить від множини параметрів системи, задач, які вирішуються нею, зовнішнього середовища та типу, ступеню і динаміки їхньої взаємодії. Якщо система $\Im$ перебуває у «стані живучості», то це означає, що системою досягається ціль функціонування, тобто виконується заданий комплекс задач $\varphi = (\varphi_1, \varphi_2, ..., \varphi_n)$ із необхідною якістю та ефективністю. Несприятливі впливи повинні компенсуватися наявними в системі механізмами підтримки живучості, що передбачає виконання функцій моніторингу, ідентифікації, діагностики, відновлення тощо. «Стан живучості» характеризується стабільністю та передбачуваністю функціонування системи $\Im$. Оцінкою живучості системи може слугувати функціонал, заданий на деякій множині параметрів, які впливають на стан системи $\Im$, а саме:

$$\Psi = f(S, B, |S|, \Delta T, U, Q, W, \Lambda),$$

де S — структура системи $\Im$; B — поведінка системи; $|S|$ — «стан живучості» системи; ΔT — часова надмірність; U — управління; Q — вектор допустимої якості виконання функцій; W — множина станів, у які може перейти система $\Im$ через впливи зовнішнього середовища; Λ — множина параметрів, що визначають характер, ступінь, топологію та динаміку впливу зовнішнього середовища на систему $\Im$.

Якщо система $\Im$ переходить у стан, коли забезпечується рішення деякого комплексу задач $\varphi = (\varphi_1, \varphi_2, ..., \varphi_n)$, то це означає здатність системи $\Im$ реалізувати будь-яку задачу φ_i з комплексу задач $\varphi = (\varphi_1, \varphi_2, ..., \varphi_n)$ у будь-якому зі станів $w_j \in W$, зокрема, і у станах $w_j \in (w_1, w_2, ..., w_d)$, що характеризуються як відмовами технічних засобів (відмовами у техніко-технологічній складовій), так і «хибними діями» — порушеннями (навмисними/ненавмисними) чи помилками обслуговуючого або управлінського персоналу. Серед «станів живучості» $|S|$, в які може перейти система $\Im$ через впливи зовнішнього середовища, принципово розрізняють три типи, а саме [7]:

1) стани, в яких у системі забезпечується вирішення усього комплексу задач $\varphi = (\varphi_1, \varphi_2, ..., \varphi_n)$ із заданою якістю та необхідною ефективністю;

2) стани, в яких у системі забезпечується вирішення лише деякої підмножини $\varphi^* \subset \varphi$;

3) стани, в яких у системі забезпечується вирішення лише якоїсь однієї із задач комплексу $\varphi = (\varphi_1, \varphi_2, ..., \varphi_n)$.

Для автоматизованої СОУ об’єкта критичної інфраструктури перехід в один зі станів типу 2) чи 3) означає наявність порушень у роботі технічних засобів або «хибних дій» з боку персоналу, які призводять до звуження множини задач, що може виконувати СОУ. Такий перехід означає певну деградацію системи. Доцільно виключити елементи, які функціонально відмовили, перебудувати структуру

автоматизованої СОУ і адаптувати параметри системи до нових умов функціонування.

У загальному випадку здатність системи $\Im$ до вирішення комплексу задач $\varphi = (\varphi_1, \varphi_2, ..., \varphi_n)$ і відповідно досягнення цілі функціонування можна достатньо повно характеризувати наступною матрицею:

$$\mathrm{M}(|S|) = \left\| m_{ij}(|S|) \right\|, \quad i = \overline{1,n}, \quad j = \overline{1,d},$$

$$m_{ij}(|S|) = \begin{cases} 1, & \textit{якщо у системі, що знаходиться у стані } w_j, \\ & \textit{існує можливість виконання задачі } \varphi_i \textit{ з необхідною якістю}, \\ 0, & \textit{в іншому випадку}. \end{cases}$$

Побудова матриці $\mathrm{M}(|S|)$, елементи якої булеві функції, задані на множині параметрів, що впливають на стан системи, досить складна задача, та якщо сформувати матрицю $\mathrm{M}(|S|)$ і задати розподіл імовірності знаходження системи $\Im$ в будь-якому зі станів $w_j \in (w_1, w_2, ..., w_d)$, то живучість системи $\Im$ буде визначено, і тоді для системи $\Im$ як оцінку її живучості замість функціонала Ψ можна використати простіший, записаний у матричній формі:

$$\Psi = V \times M(|S|) \times P,$$

де $V = \left\| v_1, v_2, ..., v_n \right\|$ — вектор коефіцієнтів важливості задач з множини φ, що реалізуються системою $\Im$; $P = \left\| p_1, p_2, ..., p_d \right\|$ — вектор імовірності стану w_j. Коефіцієнт важливості задачі може характеризувати втрати щодо безпеки критичної інфраструктури (відносні) у випадку невиконання СОУ цієї задачі.

Вирішення комплексу задач безпеки породжує певну структуру в автоматизованій СОУ, математичною моделлю якої може слугувати неорієнтований граф, оскільки зв'язки між автоматизованими робочими місцями двосторонні:

$$S^{\text{sec}}(V, L), \quad V = \{v_i\}, \quad L = \{l_{ij}\}, \quad i, j = \overline{1,m},$$

де V — множина вершин, що відповідає множині автоматизованих робочих місць (АРМ), на яких працюють управлінці/користувачі, які задіяні в напрацюванні та реалізації функцій забезпечення безпеки критичної інфраструктури; L — множина ребер, відповідає множині зв'язків між АРМ.

Унеможливити виконання комплексу задач безпеки на АРМ посадових осіб всіх рівнів управління може непрацездатність АРМ чи втрата зв'язків між АРМ унаслідок їхнього фізичного руйнування або порушення цілісності даних, відсутності посадової особи; погіршення характеристик технічної складової автоматизованої СОУ (продуктивності, пропускної спроможності ліній зв'язку та ін.); спотворення алгоритмів функціонування; зменшення структурної надлишковості, запасу ресурсів; погіршення функціонування елементів і керованості автоматизованої СОУ; фатальна втрата працездатності складових СОУ або системи в цілому.

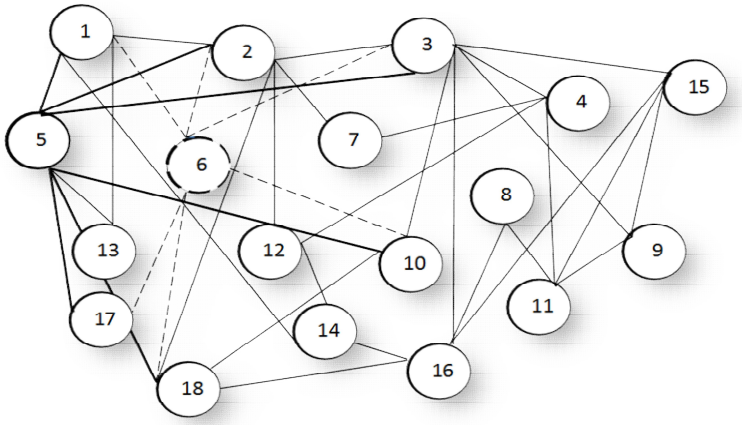
В автоматизованій СОУ кожний АРМ можна розглядати як підсистему, структура якої визначається її функціональним призначенням. Спеціалізація АРМ

відбувається шляхом інсталяції відповідного програмного забезпечення та налагодження зв'язків між складовими системи. Модульний принцип розробки програмного забезпечення, який зазвичай застосовується, дозволяє досить легко сформувати необхідну конфігурацію АРМ, як підсистеми СОУ, для виконання певних управлінських функцій. Функціональність АРМ можна розширювати в разі потреби, підключаючи нові програмні модулі. Таким чином, створюється гнучке масштабоване середовище реалізації управлінських функцій.

Практика свідчить, що технологія динамічної реконфігурації серед засобів забезпечення функціональної стійкості складних систем займає одне з першорядних місць. Впровадження технології динамічної реконфігурації для підструктури S^{sec}, що забезпечує виконання комплексу задач безпеки функціонування критичної інфраструктури є доцільним, оскільки необхідно гарантувати безперервність процесу управління об'єктами критичної інфраструктури та критичною інфраструктурою в цілому навіть за наявності небажаних впливів на інфраструктуру та появу й накопичення відмов у самій автоматизованій СОУ.

Динамічна реконфігурація в автоматизованій СОУ — це не лише технологічне рішення щодо компенсації відмов, а й управлінський процес із забезпечення оперативного перерозподілу функцій управління і необхідних ресурсів між АРМ управлінців для досягнення необхідної ефективності функціонування СОУ в цілому по управлінню об'єктом, зокрема і забезпеченню виконання комплексу задач безпеки.

На рисунку наведено приклад застосування технології динамічної реконфігурації для підструктури S^{sec} автоматизованої СОУ об'єкта критичної інфраструктури при виході з ладу одного із ключових АРМ (АРМ № 6). Підсистема динамічної реконфігурації в автоматичному режимі винайшла та реалізувала нову конфігурацію, при цьому функціональні задачі та інформаційні зв'язки АРМ № 6 були відповідно автоматично перерозподілені та спрямовані на АРМ № 5.



Приклад застосування технології динамічної реконфігурації для підструктури S^{sec} автоматизованої СОУ об'єкта критичної інфраструктури при виході з ладу АРМ № 6

Підсистему динамічної реконфігурації в автоматизованій СОУ можна реалізувати як апаратно-програмний комплекс, до складу якого входять такі основні компоненти: модуль моніторингу, модуль аналізу, модуль локалізації, модуль ви-

бору та прийняття рішень, модуль реалізації рішень, база даних і знань [8]. Апаратно-програмний комплекс працює, як правило, в автоматичному режимі. Відбувається безперервний процес моніторингу стану системи управління та її елементів за заданими індикаторами. У разі виявлення відхилень від заданого штатного режиму роботи, які можуть призвести або призвели до нештатних ситуацій, активізується підсистема динамічної реконфігурації. В умовах виникнення функціональних відмов відбувається пошук, знаходження та реалізація раціонального варіанту використання наявних ресурсів СОУ для підтримки безперервного управління об'єктом і виконання наявних управлінських завдань.

Висновки

Практичний досвід супроводу автоматизованих СОУ свідчить, що впровадження процедури динамічної реконфігурації дозволяє підвищити функціональну стійкість автоматизованої СОУ і відповідно якість виконання управлінських завдань щодо забезпеченню безпеки функціонування об'єктів критичної інфраструктури й інфраструктури в цілому.

1. Зелена книга з питань захисту критичної інфраструктури в Україні. Київ, 2015. 35 с.

2. Безопасность критических инфраструктур: математические и инженерные методы анализа и обеспечения / под ред. Харченко В.С. МОН Украины, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», 2011. 641 с.

3. Failure Mode, Effects & Criticality Analysis (FMECA). URL: https://quality-one.com/fmeca/

4. Dodonov, O., Gorbachyk, O., Kuznietsova, M. Increasing the survivability of automated systems of organizational management as a way to security of critical infrastructures. In: XVIII International Scientific and Practical Conference «Information Technologies and Security» (ITS 2018), CEUR Workshop Proceeding (ISSN 1613-0073). 2018. Vol. 2318. P. 26–270. [Online]. Available: http://ceurws.org/Vol-2318//.

5. Dogan Ibrahim. An Overview of Soft Computing. URL: https://www.sciencedirect.com/science/article/pii/S1877050916325467

6. Basilio A., Landrini F., Novelli G., Landrini G., Baldrighi M. Functional Safety of Safety-Related Systems. Manual for Plant Engineering and Maintenance. Italy, G.M. International S.r.l, Villasanta, 2008. 388 p.

7. Харченко В.С., Яковлев С.В., Горбачик О.С., и др. Обеспечение функциональной безопасности критически важных информационно-управляющих систем. Харьков: Константа, 2019. 272 с.

8. Dodonov, O., Gorbachyk, O., Kuznietsova, M. Dynamic Reconfiguration in Automated Organizational Management Systems // Selected Papers of the XX International Scientific and Practical Conference «Information Technologies and Security» (ITS 2020), Kyiv, Ukraine, December 10, 2020. P. 129–141 [Online]. Available: http://ceur-ws.org/Vol-2859

Надійшла до редакції 15.04.2022