DOI: 10.58254/viti.8.2025.21.269

УДК 681.35

канд. техн. наук Хусаінов П. В. ORCID: 0000-0002-0675-0369 (ВІТІ ім. Героїв Крут)
канд. техн. наук, доцент Штаненко С. С ORCID: 0000-0001-9776-4653 (ВІТІ ім. Героїв Крут)

ОБҐРУНТУВАННЯ ІНФОРМАЦІЙНОЇ ПІДТРИМКИ ФАХІВЦЯ З РЕАГУВАННЯ НА ІНЦИДЕНТИ КІБЕРБЕЗПЕКИ ОБ’ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ

До розгляду пропонується висвітлення основних положень науково-методичного апарату інформаційної підтримки фахівців із реагування на інциденти кібербезпеки, які виконують свої обов’язки у складі групи реагування на комп’ютерні надзвичайні події об’єкта критичної інфраструктури.

У першій змістовній частині статті оприлюднено: принципи будови об’єкта критичної інфраструктури з позиції системного аналізу; системні риси основних компонентів об’єкта критичної інформаційної інфраструктури у контексті реалізації управління; реалізація функціонування об’єкта критичної інфраструктури як процесу управління; констатація обов’язковості врахування наявності з’єднання внутрішньої комунікаційної системи з мережею Інтернет (публічний кіберпростір) для забезпечення трактів утворення каналів прямого (зворотного) зв’язку; особливості вироблення керуючих впливів на основі програмного, оптимального та адаптивного управління; особливості реалізації автоматичного та автоматизованого управління технологічним процесом; умови своєчасного вироблення органом управління об’єкта критичної інфраструктури правильних керуючих впливів; цикл управління технологічним процесом, ролі та функції компонентів його забезпечення; опис показника ефективності процесу управління.

Друга частина висвітлює такі аспекти дослідження: доцільність розгляду компонентів забезпечення циклу управління технологічним процесом як мережі масового обслуговування; зв’язок відмов основних компонентів об’єкта критичної інформаційної інфраструктури з погіршенням ефективності управління технологічним процесом; характеристика відмов із зазначенням можливості їх компенсації шляхом апріорного аналізу надійності; констатується непридатність зменшення апріорної невизначеності на етапі проєктування для компенсації відмов внаслідок несанкціонованого втручання у формі кібератак через публічний кіберпростір; необхідність реалізації інформаційної підтримки рішень фахівця з реагування на інциденти кібербезпеки на етапі експлуатації об’єкта критичної інфраструктури.

Ключові слова: *об’єкт критичної інфраструктури, процес управління, інформаційна підтримка рішень.*

P. Khusainov, S. Shtanenko. Justification of information support for specialists responding to cybersecurity incidents at critical infrastructure facilities

The following is proposed for consideration: highlighting the main provisions of the scientific and methodological apparatus for information support of cybersecurity incident response specialists who perform their duties as part of a computer emergency response team for critical infrastructure facilities.

The first substantive part of the article reveals: the principles of critical infrastructure facility design from the perspective of system analysis; the systemic features of the main components of critical information infrastructure facilities in the context of management implementation; the implementation of critical infrastructure facility operation as a management process; the statement of the necessity to take into account the connection of the internal communication system to the Internet (public cyberspace) to ensure the formation of direct (reverse) communication channels; features of the development of control influences based on programmatic, optimal, and adaptive management; features of the implementation of automatic and automated management of the technological process; conditions for the timely development of correct control influences by the management body of the critical infrastructure object; the cycle of technological process management, the roles and functions of its support components; description of the management process efficiency indicator.

The second part highlights the following aspects of the study: the feasibility of considering the components of the technological process management cycle as a mass service network; the relationship between the failure of key components of critical information infrastructure and the deterioration of technological process management efficiency; the characteristics of failures with an indication of the possibility of compensating for them through a priori reliability analysis; it is stated that reducing a priori uncertainty at the design stage is not suitable for compensating for failures due to unauthorized interference in the form of cyberattacks through public cyberspace; the need to implement information support for decisions made by specialists responding to cybersecurity incidents at the stage of critical infrastructure facility operation.

Keywords: *critical infrastructure facility, management process, information support for decisions.*

Постановка завдання. Останні зміни до Закону України “Про основні засади забезпечення кібербезпеки України” запровадили у нормативно-правове поле поняття “реагування на кіберінциденти” як структуровану сукупність дій, спрямованих на підготовку до кіберінцидентів, їх виявлення та аналіз, мінімізацію шкоди від кіберінциденту та запобігання їх повторенню у майбутньому. Забезпечення реагування на кіберінциденти (кібератаки, кіберзагрози) для об’єктів кіберзахисту, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, об’єктів критичної інформаційної інфраструктури покладається на Національну систему реагування на кіберінциденти, кібератаки, кіберзагрози. Її організаційною основою є команди реагування на кіберінциденти, кібератаки, кіберзагрози або команди реагування на комп’ютерні надзвичайні події (Computer Security Incident Response Team, CSIRT). Введення у нормативно-правове поле означення “CSIRT” за термінологією The Forum of Incident Response and Security Teams (FIRST) спрямоване на гармонізацію (впровадження) нормативно-правового регулювання з урахуванням розподілу ролей, завдань, функцій та відповідальності публічного сектору, операторів, власників або розпорядників об’єктів критичної інформаційної інфраструктури, сумісності з відповідними стандартами Європейського Союзу та НАТО [1–4].

Об’єкт критичної інформаційної інфраструктури – інформаційна, електронна комунікаційна, інформаційно-комунікаційна або технологічна система, яка необхідна для стійкого та безперервного функціонування об’єкта критичної інфраструктури, істотно впливає на безперервність та стійкість процесу надання життєво важливих функцій та/або послуг та відсутній альтернативний об’єкт (спосіб) їх надання. До об’єктів критичної інфраструктури відносять об’єкти інфраструктури, системи (сукупність систем, їх частини), які забезпечують функції та/або послуги у сферах: урядування; енергозабезпечення; водопостачання, водовідведення; продовольчого забезпечення; охорони здоров’я; фармацевтичної промисловості; виготовлення вакцин, функціонування біолабораторій; розповсюдження інформації; електронних комунікацій; фінансів; транспорту; оборони, державної безпеки; правопорядку, правосуддя; цивільного захисту, порятунку; космічної діяльності; хімічної промисловості; дослідницької діяльності [5; 6].

Відповідно до чинного законодавства Державною службою спеціального зв’язку та захисту інформації України визначений рекомендаційний порядок реагування на кіберінциденти/кібератаки для суб’єктів Національної системи захисту критичної інфраструктури в контексті, що стосується забезпечення кіберзахисту об’єктів критичної інфраструктури. Безпосереднє виконання заходів порядку реагування на кіберінциденти/кібератаки (підготовка, виявлення та аналіз, стримування, усунення, відновлення, аналіз ефективності) здійснюється фахівцями CSIRT операторів об’єктів критичної інфраструктури. Відповідні трудові функції фахівців CSIRT, а також необхідні для цього компетенції та результати навчання визначені у професійному стандарті “Фахівець з реагування на інциденти кібербезпеки” [7–9].

Сукупність факторів виникнення подій ненавмисного характеру та/або таких, що мають ознаки несанкціонованого втручання у функціонування об’єкта критичної інфраструктури (з відповідними можливими наслідками інциденту безпеки критичної інфраструктури) за допомогою засобів електронних комунікацій об’єкта критичної інформаційної інфраструктури у кіберпросторі, уособлює поняття “кіберінцидент/кібератака”. Реагування на кіберінциденти/кібератаки об’єкта критичної інформаційної інфраструктури спрямоване на недопущення (мінімізацію наслідків) порушення сталого, надійного та штатного режиму функціонування такого об’єкта та/або порушення безпеки критичної технологічної інформації в умовах кіберзагроз.

Аналіз останніх публікацій. Для ознайомлення з науково-методичним апаратом інформаційної підтримки рішень оператора технічної системи, зокрема фахівця з реагування

на інциденти інформаційної безпеки, необхідно звернутися до [10–12]. Призначення, цілі, задачі, принципи будови, структура, процеси діяльності та засоби CSIRT із розкриттям досвіду організації реагування на кіберінциденти/кібератаки, ролей, компетенції та необхідних умінь відповідної групи фахівців деталізується в [13; 14].

Формулювання мети статті. Метою статті є висвітлення напрямку дослідження наукових проблем забезпечення інформаційної підтримки прийняття рішень фахівців з реагування на інциденти кібербезпеки об’єктів критичної інформаційної інфраструктури.

Основна частина. Будь-яке порушення безперервності, стійкості, штатного режиму функціонування критичної інфраструктури чи окремого її об’єкта, реагування на яке потребує залучення додаткових сил і ресурсів, уособлює поняття “кризова ситуація”. Негативний тренд розвитку кризової ситуації функціонування об’єкта критичної інфраструктури у часі може призвести до загрози для населення, суспільства, соціально-економічного стану, національної безпеки і оборони України. Якщо виникнення кризової ситуації стало наслідком незаконних дій, тоді такі дії називають несанкціонованим втручанням (у функціонування об’єкта критичної інфраструктури). Подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки несанкціонованого втручання у функціонування об’єкта критичної інфраструктури, прийнято називати “інцидент безпеки критичної інфраструктури”.

Режим (умови та вимоги залежно від стану і динаміки розвитку ситуації) функціонування об’єкта критичної інфраструктури визначається її оператором. Оператор критичної інфраструктури є юридичною особою, що здійснює управління об’єктом критичної інфраструктури, відповідає за його поточне функціонування, захист та реагування на кризові ситуації. Захист критичної інфраструктури – всі види діяльності, що виконуються перед або під час створення, функціонування, відновлення і реорганізації об’єкта критичної інфраструктури, спрямовані на своєчасне виявлення, запобігання і нейтралізацію загроз безпеці об’єктів критичної інфраструктури, а також мінімізацію та ліквідацію наслідків у разі їх реалізації. Реагування на кризові ситуації визначається оператором критичної інфраструктури шляхом введення відповідного режиму для забезпечення стійкості об’єкта критичної інфраструктури за відповідних умов, обставин і чинників.

Функціонування об’єкта критичної інфраструктури (безперервне, стійке, штатне) повинно забезпечувати реалізацію важливих для національної безпеки функцій та/або послуг певного органу державної влади, місцевого самоврядування, установи, суб’єкта господарювання та організацій будь-якої форми власності. Спрямованість на досягнення цілі (цілей) національної безпеки (державний суверенітет; територіальна цілісність; демократичний конституційний лад; прогресивний демократичний розвиток; безпечні умови життєдіяльності і добробут її громадян) характеризує об’єкти критичної інфраструктури як цілеспрямовані системи.

Основною властивістю цілеспрямованої системи є її здатність до реалізації управління, тобто здійснення послідовності зміни стану об’єкта управління для досягнення цілі існування системи або одержання очікуваного результату на визначеному часовому інтервалі функціонування системи. Важливо зазначити, що тут поняття “система” застосовується для констатації використання системного підходу при розгляді об’єкта критичної інфраструктури безвідносно до його призначення, функцій та/або послуг.

Процес управління (послідовність переходів між станами об’єкта управління) має циклічний характер. Циклічність такого процесу забезпечується органом управління. Узагальнено цикл управління полягає у послідовному здійснені чотирьох складових етапів: формулювання цілі (постановка задачі); вибір рішення; реалізація рішення; оцінювання досягнення результату. Ціль – очікуваний (ідеалізований, уявний) результат психологічної діяльності людини (органу управління) на певному інтервалі часу. Формулювання цілі

виникає як певний стимул змінити поточну ситуацію (процесу управління) у потрібному напрямку з урахуванням набутого досвіду. Постановка задачі характеризується використанням кількісних даних (параметрів) очікуваного результату на відміну від більш ідеалізованого (уявного) формулювання цілі. При формулюванні цілі (постановці задачі) здійснюється: збирання даних про стан об’єкта управління та зовнішнього середовища; прогнозування можливих змін (цільової функції поточної ситуації процесу управління) та вироблення (на основі обраних критеріїв) альтернативних стратегій керуючих впливів на об’єкт управління у формі відповідної послідовності операцій. Операція – впорядкована та взаємопов’язана сукупність дій, спрямованих на досягнення цілі (вирішення задачі). Вибір за одним чи кількома критеріями однієї з можливих альтернативних стратегій уособлює етап вибору рішення. Етап реалізації рішення полягає у виконанні операцій за планом обраної стратегії (керуючих впливів) досягнення цілі (вирішення задачі). Реалізація рішення (керуючих впливів на об’єкт управління) зазвичай здійснюється в умовах можливого прояву внутрішніх і зовнішніх дестабілізуючих факторів, що викликає певну невідповідність фактичного результату очікуваному. Визначення такої невідповідності, аналіз причин та вироблення рекомендацій щодо її усунення (зменшення) на наступному циклі управління уособлює етап оцінювання досягнення результату (вирішення задачі).

Під поняттям “орган управління” будемо розглядати функціональний компонент об’єкта критичної інфраструктури, який здійснює формулювання цілі (постановку задачі), підготовку, вибір, реалізацію та оцінку результату рішення циклу управління технологічним процесом (об’єкт управління) основної послуги, яка надається оператором критичної інфраструктури у певному секторі/підсекторі (рис. 1). Дестабілізуючі фактори охоплюють сукупність явищ, які можуть мати негативний прояв для досягнення цілі (вирішення задачі) на певному часовому інтервалі функціонування об’єкта критичної інфраструктури. Прояв того чи іншого дестабілізуючого фактора на певному часовому інтервалі функціонування об’єкта критичної інфраструктури є випадковою подією реального світу. Випадкова подія (реального світу) – подія, яка при фіксованих умовах випробування (експерименту) може як відбутися, так і не відбутися зі стабілізацією частоти такого результату у ряді випробувань. Можливість настання випадкової події характеризується числовим значенням її ймовірності.

Рис. 1. Об’єкт критичної інфраструктури як предмет системного аналізу

Ймовірність випадкової події залежить від комплексу умов, в яких здійснюється випробування (експеримент). Пояснення невідповідності фактичного результату процесу управління очікуваному проявом випадковості дестабілізуючих факторів або їх скритої закономірності є вельми складною задачею. Ефективним засобом рішення складних, недостатньо чітко сформульованих проблем є системний аналіз. Предмет системного аналізу ґрунтується на загальносистемних характеристиках і взаємодії системи із зовнішнім середовищем. Основною концепцією системного аналізу є системний підхід, де система – цілісний комплекс взаємозв’язаних компонентів (орган управління; об’єкт критичної інформаційної інфраструктури; об’єкт управління, зовнішнє середовище), які взаємодіють:

шляхом передачі інформації керуючого впливу від органу до об’єкта управління через тракт каналу прямого зв’язку (рис. 1, *а, б*) та інформації про стан об’єкта до органу управління через тракт каналу зворотного зв’язку (рис. 1, *в, г*);

шляхом обміну інформацією про параметри обміну речовиною (енергією) об’єкта управління із зовнішнім середовищем у контексті реалізації технологічного процесу об’єкта критичної інфраструктури.

Сукупність зв’язаних один з одним об’єктів (елементів) системи, здатних приймати, зберігати, перероблювати та передавати інформацію, уособлює кібернетичний аспект системного підходу до дослідження складних систем. Передавання/приймання інформації передбачає наявність у компонентів складної системи передавача/приймача та каналу зв’язку між ними, здатного відображати стан передавача та стан приймача, для зберігання інформації – наявність фізичного середовища, яке здатне фіксувати, зберігати і відтворювати свій стан. Перероблення інформації полягає у виконанні певного алгоритму, вхідні дані якого ототожнюються зі станом фізичного середовища для запам’ятовування.

У цьому контексті об’єкт критичної інформаційної інфраструктури уособлює сукупність систем електронних комунікацій, які забезпечують тракти утворення каналів прямого та зворотного зв’язку між пристроєм зв’язку з об’єктом управління та обчислювальною машиною органу управління через комунікаційну систему (об’єкта критичної інформаційної інфраструктури) і/або мережу Інтернет (рис. 2). Під поняттям “тракт каналу прямого (зворотного) зв’язку об’єкта критичної інфраструктури” будемо розглядати послідовне з’єднання сукупності технічних засобів комунікаційної системи і/або мережі Інтернет для забезпечення електронних комунікацій між пристроєм зв’язку з об’єктом управління та обчислювальною машиною органу управління.

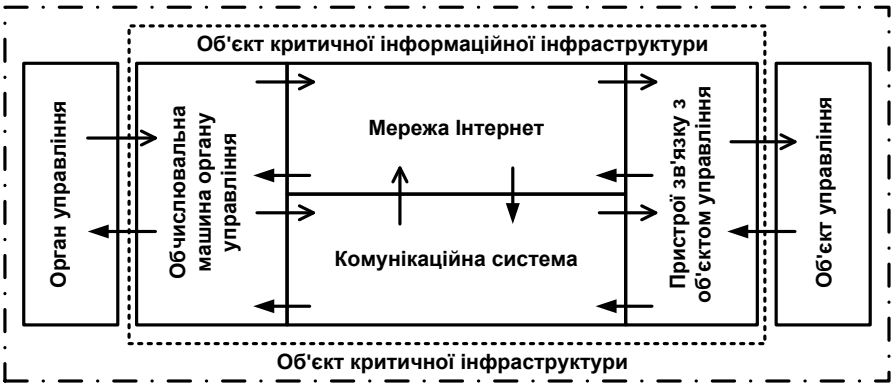

Рис. 2. Декомпозиція об’єкта критичної інформаційної інфраструктури

Компонент “комунікаційна система” уособлює складну систему передавання, комутації або маршрутизації, обладнання та інші ресурси (включаючи пасивні мережеві елементи, які дають змогу передавати сигнали за допомогою проводових, радіо-, оптичних або інших електромагнітних засобів, мережі мобільного, супутникового зв’язку, електричні кабельні мережі в частині, в якій вони використовуються для цілей передачі сигналів), що забезпечують електронні комунікації (передачу електронних інформаційних ресурсів), у тому числі засоби і пристрої зв’язку, комп’ютери, інша комп’ютерна техніка, інформаційно-комунікаційні системи, які мають доступ до мережі Інтернет та/або інших глобальних мереж передачі даних. Електронна комунікація (телекомунікація, електрозв’язок) – передавання та/або приймання інформації незалежно від її типу або виду у вигляді електромагнітних сигналів за допомогою технічних засобів електронних комунікацій. Мережа Інтернет (Інтернет) – глобальна електронна комунікаційна мережа, що призначена для передачі даних і складається з фізично та логічно взаємоз’єднаних окремих електронних комунікаційних мереж, взаємодія яких

базується на використанні єдиного адресного простору та на використанні інтернет-протоколів, визначених міжнародними стандартами [15; 16].

Усі методи управління зводяться до вироблення органом управління інформації керуючого впливу на підставі інформації від пристрою зв’язку з об’єктом управління. Пристрій зв’язку з об’єктом управління здійснює перетворення та передачу через канал зворотного зв’язку інформації про сукупність значень фізичних величин опису стану об’єкта управління, а також перетворення інформації керуючого впливу з каналу прямого зв’язку в операції надання необхідних значень регульованим фізичним величинам об’єкта управління. Обчислювальна машина органу управління здійснює одержання інформації від пристрою зв’язку з об’єктом управління, її перетворення у форму, придатну для вибору, забезпечення вибору керуючого впливу (органом управління) з множини можливих варіантів (програмного, оптимального управління чи авторегулювання) та відправлення інформації керуючого впливу через канал прямого зв’язку.

За змістовною природою об’єкта управління досягнення цілі функціонування об’єкта критичної інфраструктури може здійснюватися методами програмного, оптимального управління та авторегулювання. Програмне управління полягає у реалізації певної траєкторії (з множини сприятливих) послідовної зміни станів об’єкта управління, спрямованої на досягнення цілі (очікуваного результату постановки задачі) або якомога близького наближення до неї. Оптимальне управління спрямоване на забезпечення максимального чи мінімального значення деякої цільової функції, авторегулювання – на забезпечення заданого значення такої функції.

Поняття “цільова функція” уособлює функціональне відображення на кількісну величину ступеня наближення до цілі управління (постановки задачі) внаслідок керуючого впливу. Визначення ступеня наближення до цілі управління (постановки задачі) внаслідок керуючого впливу здійснюється шляхом оцінки корисності результату вирішення задачі. Залежність ступенів наближення вирішення задачі до цілі (постановки задачі) для всієї множини одержаних результатів називається функцією корисності. Математичне очікування множини дискретних або неперервних значень функції корисності є кількісною мірою ефективності, тобто показником ефективності (вирішення задачі).

Методичним базисом оцінки корисності результату вирішення задач є дослідження операцій, експертне оцінювання, імітаційне моделювання. За умови постановки задачі управління у контексті понятійного апарату розділів дослідження операцій кількісна велична цільової функції має найкраще обґрунтування, зокрема в частині, що стосується: розподілу ресурсів; масового обслуговування; пошуку; конкурентних ігор; складання розкладів; визначення маршрутів; постачання ресурсів; заміни обладнання і т. д. Експертне оцінювання полягає у залученні групи фахівців із необхідним рівнем знань та досвіду, імітаційне моделювання – у використанні результатів машинного експерименту.

Реалізація вибору керуючого впливу у формі алгоритму програмного компонента обчислювальної машини органу управління уособлює об’єкт критичної інфраструктури як автоматичну систему управління. Вибір керуючого впливу за участю людини у ролі органу управління є ключовою ознакою розгляду об’єкта критичної інфраструктури як автоматизованої системи управління. Різновид автоматичних та автоматизованих систем управління організаційними і/або технологічними процесами об’єктів критичної інфраструктури віднесений до класу систем управління технологічними процесами. Також слід зазначити, що переважна кількість таких систем належить до автоматизованого типу.

Участь людини-оператора в процесі управління технологічним процесом (об’єкта критичної інфраструктури) обумовлена необхідністю усунення невизначеності вибору рішення. Причинами невизначеності (неповноти, недостатності, обмеженості, неточності) інформації для вибору рішення можуть бути: неможливість точного передбачення наслідків; неможливість повторення або експериментальної перевірки; немає можливості контролю всіх

факторів; наявність множини альтернативних рішень. Вибір рішення є прерогативою людини і принципово не може мати формального подання. Особа, яка приймає рішення, керується міркуваннями передбачення, досвіду, інтуїції професійної підготовленості та кваліфікації, а також суб’єктивними уявленнями, судженнями, емоціями.

Людина-оператор (органу управління) – людина, яка бере участь в управлінні об’єктами і системами як складовий елемент ергатичної системи. Може виступати в ролі приймача, ретранслятора і перетворювача інформації, приймати рішення, вироблювати команди, здійснювати контроль роботи системи та бути виконавцем команд. Відрізняється багатоканальністю сприйняття, раціональним використанням інформації, здатністю до навчання, малою пропускною здатністю, обмеженою швидкістю та втомлюваністю.

Розглянемо кілька прикладів технологічних процесів критичної інфраструктури, управління якими передбачає застосування автоматизованого підходу при побудові відповідних систем:

управління системами передачі, енергопостачання, розподілом електричної енергії, експлуатації гідротехнічних споруд;

видобуток, передача (транзит), очищення, переробка, зберігання та постачання нафти, нафтопродуктів, газу;

експлуатація нафтопроводів та газотранспортної системи;

управління повітряним рухом, авіаперевезення (робота авіаційного транспорту);

перевезення пасажирів метрополітеном;

пасажирські, вантажні залізничні перевезення;

експлуатація та технічне обслуговування залізниці, забезпечення роботи вокзалів та вузлових станцій;

постачання теплової енергії, постачання гарячої води, централізоване питне водопостачання, централізоване водовідведення, управління побутовими відходами;

виробництво промислового газу, добрив або азотистих сполук, пестицидів, агрохімічних продуктів, вибухових, основних органічних, неорганічних речовин і т. д.

Умови (виконання функцій) своєчасного вироблення органом управління (об’єкта критичної інфраструктури) правильних керуючих впливів для об’єкта управління (рис. 3):

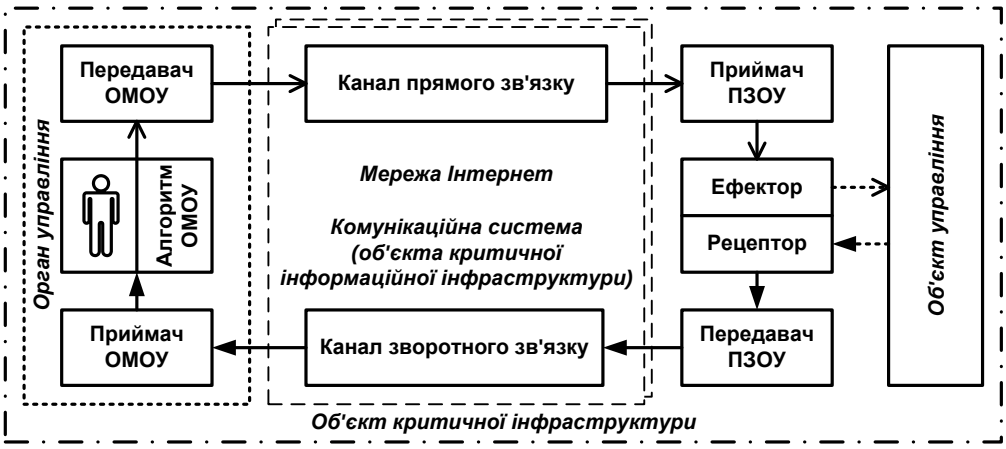

Рис. 3. Компоненти забезпечення циклу управління технологічним процесом

передача за визначений час інформації про стан об’єкта управління від пристрою зв’язку з об’єктом управління (ПЗОУ) через канал зворотного зв’язку якомога повної інформації про стан об’єкта управління;

своєчасний і правильний вибір людиною-оператором (автоматизована система управління) варіанту керуючого впливу з множини можливих варіантів сформованих

управляючим програмним алгоритмом обчислювальної машини органу управління (ОМОУ), який правильно функціонує або автоматичний вибір рішення самим таким алгоритмом без участі людини-оператора (автоматична система управління);

передача за визначений час інформації керуючого впливу від ОМОУ через канал прямого зв’язку;

правильне функціонування (справність, працездатність) програмно-апаратного компонента ефектора ПЗОУ (перетворення інформації з каналу прямого зв’язку в значення регульованих фізичних величин об’єкта управління за визначений час);

правильне функціонування (справність, працездатність) програмно-апаратного компонента рецептора ПЗОУ (перетворення значень фізичних величин опису стану об’єкта управління в інформацію для каналу зворотного зв’язку за визначений час).

Впорядкована сукупність операцій передавання (обробки, перетворення) інформації у контурі послідовного охоплення компонентів ОМОУ, каналу прямого зв’язку, ПЗОУ та каналу зворотного зв’язку утворюють цикл управління технологічним процесом (ЦУТП), що багатократно повторюється в процесі управління (об’єктом критичної інфраструктури). Тривалість ЦУТП дорівнює сумарній середній тривалості операцій передавання (обробки, перетворення) інформації в ОМОУ, ПЗОУ та каналів прямого (зворотного) зв’язку.

Ефективність ЦУТП є кількісним показником (мірою) математичного очікування множини значень фактичної тривалості циклів управління технологічним процесом при штатному режимі функціонування апаратних, програмних (програмно-апаратних) компонентів об’єкта критичної інформаційної інфраструктури, зокрема, ОМОУ, каналів прямого (зворотного) зв’язку та ПЗОУ. Математично очікувана тривалість ЦУТП не повинна перевищувати деякої максимально допустимої величини для об’єкта критичної інфраструктури як системи ієрархічного управління в реальному масштабі часу на етапі проєктування процесів оброблення інформації для забезпечення необхідного темпу змін станів технологічного процесу (об’єкта управління). Методичним базисом обґрунтування часових ЦУТП є теорія систем масового обслуговування (модель мережі масового обслуговування), при застосуванні якої ОМОУ, ПЗОУ та канали прямого (зворотного) зв’язку розглядаються як прилади обслуговування.

Раніше вже було зазначено, що режим функціонування об’єкта критичної інфраструктури визначається її оператором (юридична особа, що здійснює управління об’єктом критичної інфраструктури, відповідає за його поточне функціонування, захист та реагування на кризові ситуації) як процес забезпечення реалізації певних визначених для такого об’єкта функцій (послуг). Під поняттям “функція” (об’єкта) – властивість (об’єкта) відповідно до вимог нормативної та (чи) конструкторської (проєктної) документації (на етапі розробки вимог, проєктування, виробництва, використання і ремонту об’єкта), де об’єкт – самостійна одиниця з погляду надійності (технічні система, програмний засіб, людино-машинна система, споруда, машина, підсистема, апаратура, функційна одиниця, пристрій, елемент чи будь-яка їх частина). Надійність – властивість об’єкта зберігати у часі в установлених межах значення всіх параметрів, які характеризують здатність виконувати потрібні функції в заданих режимах та умовах застосування, технічного обслуговування, зберігання та транспортування. Методичним базисом застосування методів розрахунку надійності технічних систем, виробів, способів оптимізації і підвищення ефективності їх експлуатації є теорія надійності [17–19].

Параметри штатного режиму функціонування апаратних, програмних (програмно-апаратних) компонентів забезпечення циклу управління технологічним процесом (ОМОУ, канал прямого зв’язку, ПЗОУ, канал зворотного зв’язку) в заданих умовах визначаються як складова частина відповідності системи управління технологічним процесом (об’єкта критичної інфраструктури) проєктному цільовому призначенню. Подія, яка полягає у втраті об’єктом здатності виконувати потрібну функцію, тобто порушення працездатного стану

об’єкта, називається відмовою. Причини відмов (обставини під час проєктування, виробництва чи використання об’єкта, які призвели до відмови):

недосконаліть чи порушення встановлених правил і/або норм проєктування та конструювання (конструкційна відмова);

невідповідність виготовлення проєкту нормам виробництва (виробнича відмова);

поступові зміни значень одного чи декількох параметрів (поступова відмова);

внаслідок відмови чи несправності іншого об’єкта (залежна відмова);

однозначно пов’язана з необхідністю модифікації проєкту, виробництва, правил експлуатації, документації чи інших чинників, що враховуються (систематична відмова);

діяння під час використання об’єкта навантажень, що перевищують його встановлену спроможність (відмова через перевантаження);

неправильне чи необережне поводження (відмова через неправильне поводження);

неміцність самого об’єкта, коли діяння навантаження на об’єкт не перевищують встановлену спроможність об’єкта (відмова через неміцність);

процеси деградації в об’єкті при дотриманні всіх встановлених правил і/або норм його проєктування, виготовлення та експлуатації (деградовна відмова);

непередбачуване стихійне лихо (відмова внаслідок стихійного лиха).

Виникнення відмови є випадковою подією, що викликана проявом зазвичай складної комбінації типових класів обставин (викладені у поєднанні з причинами відмов) та випадкових об’єктивних і суб’єктивних (обумовлені ймовірністю помилкових рішень осіб, які приймають рішення при створенні та експлуатації об’єктів) факторів експлуатаційного, технологічного та організаційного характеру. Традиційними підходами (теорії надійності) до зменшення негативного впливу об’єктивних і суб’єктивних факторів прояву відмов компоненті технічних систем є резервування, оптимальне управління запасними елементами, термінами експлуатації, технічна діагностика, обслуговування тощо за результатами апріорного аналізу надійності. Апріорний аналіз надійності здійснюється шляхом вибору одного з можливих варіантів проєктування (створення) об’єкта (технічної системи) за умови наявності повної інформації про ймовірність відмов її компонентів, апостеріорний аналіз – на основі обробки статистичних даних випробування (експлуатації) за умови незалежності випадкових величин, що спостерігаються. На практиці спостерігається наявність невизначеності (неповнота, невірогідність) вихідної інформації про закони розподілу випадкових величин, що характеризують надійність окремих елементів, складових частин (компонентів) та об’єкта в цілому. Найбільш актуальні напрямки зменшення (усунення) “апріорної невизначеності” в задачах надійності досліджені авторським колективом під керівництвом Креденцера Б. П. шляхом комплексного застосування наукових результатів Стойкової Л. С., Каштанова В. О. В якості принципових положень наукового дослідження “апріорної невизначеності” вихідних даних апріорного аналізу надійності було зафіксовано:

надійність задається при проєктуванні (апріорний аналіз), уточняється на основі даних випробування (апостеріорний аналіз), враховується при виробництві та реалізується в процесі експлуатації об’єкта (технічної системи);

відсутність (недостатність) знання про складні залежності між складовими елементами (компонентами) об’єкта, об’єму достовірної вибірки експериментальних даних експлуатації аналога створюваного об’єкта (технічної системи) внаслідок його унікальності;

невідповідність (слабка адекватність) між розрахунковими результатами апріорного аналізу надійності одержаних на основі довідкових даних та фактичними даними досвіду експлуатації об’єкта (технічної системи) в реальних умовах.

Раніше вже було зазначено, що характерною експлуатаційною рисою переважної кількості об’єктів критичної інфраструктури є використання публічного (загальнодоступного, відкритого) кіберпростору для забезпечення обміну інформацією управління через тракти утворення каналів прямого (зворотного) зв’язку. Під поняттям “кіберпростір” уособлюється

середовище (віртуальний простір), утворене в результаті функціонування сумісних (з’єднаних) комунікаційних систем і забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних. Наявність з’єднання компонентів забезпечення ЦУТП об’єкта критичної інформаційної інфраструктури з кіберпростором обумовлює ймовірність спрямованих (навмисних) дій несанкціонованого втручання у формі кібератаки [20–22].

Розгляд інших подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) експлуатації об’єкта критичної інфраструктури за умови апріорної невизначеності уособлює всю широту поняття “кіберінцидент”. Порушення безперервності, стійкості, штатного режиму функціонування компонентів забезпечення ЦУТП виникненням відмов належить до класу кризових ситуацій (об’єкта критичної інфраструктури). При виникненні відмови (компонентів забезпечення ЦУТП) оператором критичної інфраструктури вводиться режим реагування на виникнення кризової ситуації із застосуванням заходів реагування.

Фахівець з реагування на інциденти кібербезпеки здійснює неперервний контроль за штатним режимом функціонування об’єкта критичної інформаційної інфраструктури та активно втручається в процес при виникненні кризових ситуацій. Вирішення наукових задач організації ефективної діяльності фахівців із реагування на кіберінциденти/кібератаки об’єктів критичної інформаційної інфраструктури здійснено на основі науково-методичного апарату створення систем інформаційної підтримки прийняття рішень Герасимова Б. М. та узагальнення результатів дисертаційних досліджень представників цієї наукової школи.

Висновки. Штатний режим функціонування об’єкта критичної інфраструктури в реальному масштабі часу може бути відображений ефективністю на основі оцінки тривалості циклу управління технологічним процесом, компоненти забезпечення якого розглядаються пристроями мережі масового обслуговування. Погіршення ефективності через відмову таких компонентів може бути компенсовано на етапі проєктування шляхом апріорного аналізу надійності із застосуванням наукових результатів усунення (зменшення) апріорної невизначеності. Цей апробований підхід є недієвим для визначення ймовірностей кібератак на етапі експлуатації конкретного об’єкта через неможливість одержання достовірної статистики і обумовлює необхідність реагування на кіберінциденти/кібератаки (на виникнення кризової ситуації) на основі апарату інформаційної підтримки прийняття рішень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII // Відомості Верховної Ради України. 2017. № 45. С. 42. Ст. 403.

2. NIST Special Publication 800-61. Computer Security Incident Handling Guide.

3. Про затвердження Положення про організаційно-технічну модель кіберзахисту: постанова Каб. Міністрів України від 29.12.2021 № 1426 // Офіційний вісник України. 2022. № 4. С. 247. Ст. 219.

4. Computer Security Incident Response Team Services Framework, Service Role and Competencies. URL: https://www.first.org/standards/frameworks/.

5. Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX // Офіційний вісник України. 2021. № 98. С. 23. Ст. 6341.

6. Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури: постанова Каб. Міністрів України від 19.06.2019 № 518 // Офіційний вісник України. 2019. № 50. С. 53. Ст. 1697.

7. Деякі питання реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі: постанова Каб. Міністрів України від 04.04.2023 № 299 // Офіційний вісник України. 2023. № 39. С. 54. Ст. 2061.

8. Про затвердження Методичних рекомендацій щодо реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі: наказ Адміністрації Державної служби спеціального

зв’язку та захисту інформації України від 03.07.2023 № 570 // URL: https://zakon.rada.gov.ua/rada/show/v0570519-23#Text.

9. Професійний стандарт “Фахівець з реагування на інциденти кібербезпеки”, затв. наказом Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 23.01.2024 № 38 // URL: https://register.nqa.gov.ua/uploads/0/571-fahivec_z_reaguvanna_na_incidenti_kiberbezpeki_v_2.pdf.

10. Хусаінов П. В. Система інформаційної підтримки адміністратора безпеки: структура, задачі, оцінка ефективності // Збірник наукових праць ВІТІ НТУУ “КПІ”. Вип. 3. Київ: ВІТІ НТУУ “КПІ”, 2007. С. 146–155.

11. Герасимов Б. М., Локазюк В. М., Оксіюк О. Г., Поморова О. В. Інтелектуальні системи підтримки прийняття рішень: навч. посіб. К.: Вид-во Європ. ун-ту, 2007. 335 с.

12. Герасимов Б. М., Камишин В. В. Організаційна ергономіка: методи і алгоритми дослідження та проектування. К.: Інфосистем, 2009. 212 с.

13. Ten Strategies of a World-Class Cybersecurity Operations Center. Carson Zimmerman. ISBN: 978-0-692-24310-7. URL: https://a.co/d/gyPR2WW.

14. The Modern Security Operations Center: The People, Process, and Technology for Operating SOC Services Joseph Muniz, Aamir Lakhani, Omar Santos, Moses Frost ISBN-10:0135619858, ISBN-13: 978-0135619858 Addison-Wesley Professional.

15. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР // Відомості Верховної Ради України. 1994. № 31. Ст. 286.

16. Про електронні комунікації: Закон України від 16.12.2020 № 1089-IX // Офіційний вісник України. 2021. № 6. С. 10. Ст. 306.

17. ДСТУ 2860-94. Надійність техніки. Терміни та визначення. [Чинний від 1996-01-01]. URL: https://dbn.co.ua/load/normativy/dstu/dstu_2860_94_nadijnist_tekhniki_termini_ta_viznachennja/5-1-0-1209.

18. Основи теорії надійності та експлуатації радіоелектронних систем: навч. посіб. / В. І. Василишин, С. В. Женжера, О. В. Чечуй, А. П. Глушко. Х.: ХНУПС, 2018. 208 с.

19. Креденцер Б. П., Вишнівський В. В., Жердєв М. К., Могилевич Д. І., Стойкова Л. С. Оцінка надійності резервованих систем при обмеженій вихідній інформації / Під наук. редак. д-ра техн. наук, проф. Б. П. Креденцера. К.: Фенікс, 2013. 336 с.

20. Adversarial Tactics, Techniques & Common Knowledge. URL: https://attack.mitre.org.

21. Common Attack Pattern Enumerations and Classifications. URL: https://capec.mitre.org.

22. Common Weakness Enumeration. URL: https://cwe.mitre.org.