DOI: 10.58254/viti.9.2026.29.382

УДК 681.35

канд. техн. наук, доцент 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)
Чурілова І. С. ORCID: 0009-0007-6195-9265 (ВІТІ ім. Героїв Крут)

ПРОБЛЕМА РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ ОБ’ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В РЕАЛЬНОМУ МАСШТАБІ ЧАСУ

Кібернетичний підхід до розгляду систем управління базується на визначенні в їхньому складі технічного комплексу управління, каналів прямого (зворотного) зв’язку, пристрою зв’язку з об’єктом. Проходження інформації керуючого впливу на об’єкт управління та інформації про його стан утворюють цикл управління. Управління багатокомпонентним об’єктом управління здійснюється при посередництві множини пристроїв зв’язку з об’єктом та відповідної кількості циклів управління. Непрацездатність і/або неправильна робота технічних засобів циклів управління призводить до втрати (зменшення) якості управління.

Одним із видів цільового призначення об’єктів критичної інфраструктури є управління технологічними процесами в реальному масштабі часу. Використання мережі Інтернет для утворення каналів прямого (зворотного) зв’язку обумовлює загрозу інциденту безпеки критичної інфраструктури у формі кібератаки. Фахівець із реагування на кіберінциденти повинен здійснювати своєчасне виявлення та аналіз, стримування, усунення кібератаки, а також відновлювати штатне функціонування системи управління технологічними процесами у реальному масштабі часу. Наразі існуючий науковий апарат не відповідає вимогам практики, що складає наукову проблему.

До розгляду пропонується пристосування методології підтримки прийняття рішень оперативного персоналу систем управління технологічними процесами реального часу. Новизною викладеного підходу є відокремлення ситуацій непрацездатності та неправильної роботи технічних засобів, викликаних відмовою від наслідків кібератаки. Визначено фактори для оцінки тривалості часового відрізку від виявлення перших ознак до прояву цілі кібератаки.

Ключові слова: *система управління технологічними процесами реального часу, реагування на інциденти.*

P. Khusainov, S. Shtanenko, I. Churilova. The problem real time-based incident response in industrial control system

The cybernetic approach to the analysis of control systems is based on the components comprising the system: the control hardware, forward (and reverse) communication channels, and the interface with the controlled object. The flow of control information to the controlled object and information about its status constitute the control cycle. Control of a multi-component system is carried out through a set of communication devices connected to the system and a corresponding number of control cycles. Failure and/or malfunction of the technical components of control loops leads to a loss (or reduction) in control quality.

One of the primary functions of critical infrastructure facilities is the real-time management of technological processes. The use of the Internet to establish direct (two-way) communication channels poses a risk of unauthorized interference in the form of a cyberattack. A cyber incident response specialist must promptly detect, analyze, contain, and mitigate cyberattacks, as well as restore the normal operation of the process control system in real time. Currently, the existing scientific framework does not meet practical requirements, which poses a scientific challenge.

This paper proposes an adaptation of a decision-support methodology for operational personnel of real-time process control systems. What is novel about this approach is the distinction between situations of system failure and malfunctions of technical equipment caused by the consequences of a cyberattack. Factors have been identified to assess the duration of the time interval from the detection of the first signs to the full manifestation of a cyberattack.

Keywords: *real time-based industrial control system, incident response.*

Постановка проблеми (у загальному вигляді). Об’єкти критичної інфраструктури — об’єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам. Зокрема, на об’єкти критичної інфраструктури покладається забезпечення виконання за функцій та/або послуг управління технологічними процесами у сфері енергозабезпечення, водопостачання, водовідведення, фармацевтики, хімічної промисловості, виготовлення вакцин, транспорту, цивільного захисту і т. д. Сукупність параметрів штатного режиму функціонування критичної інфраструктури

відповідно до проєктного цільового призначення визначається їхнім оператором. 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”. Розглядаються два широких класи причин (факторів) виникнення порушень штатного режиму функціонування об’єкта критичної інфраструктури. До першого класу належать причини (фактори), які обумовлюють події ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора), які становлять загрозу безпеці об’єкта критичної інфраструктури, його системі управління технологічними процесами, до другого класу — всі можливі форми несанкціонованого втручання в його безпечне функціонування [1].

Об’єкти критичної інфраструктури відносяться до класу цілеспрямованих систем. Їхньою основною системною властивістю є здійснення управління — послідовна зміна станів об’єкта управління (об’єкта критичної інфраструктури) для досягнення (наближення до) цілі (одержання очікуваного результату) на визначеному часовому інтервалі функціонування. Процес управління має циклічний характер. Цикл управління є повторюваною послідовністю етапів вироблення, доведення, виконання та оцінювання результату керуючого впливу органом управління (об’єкта критичної інфраструктури) за методом програмного, оптимального управління чи авторегулювання. Зв’язність компонентів, здатних приймати, зберігати, перероблювати та передавати інформацію (керуючий вплив, опис стану об’єкта управління) уособлює справедливість застосування кібернетичного аспекту системного підходу для дослідження об’єктів критичної інфраструктури. Тракт передавання (перетворення) інформації в циклі управління ідеалізованої кібернетичної системи складається з таких функціональних компонентів: програмно-апаратний комплекс (органу управління); тракти каналів прямого (зворотного) зв’язку та пристрою зв’язку з об’єктом управління. За умови сталості (непошкодженості) об’єкта управління непрацездатність і/або неправильна робота функціональних компонентів такого об’єкта не дозволяє забезпечити сам принцип цілеспрямованості кібернетичної системи через неможливість забезпечити своєчасність надходження достовірної інформації про стан об’єкта управління, правильне вироблення та своєчасне доведення керуючого впливу і т. д. [2–4].

Втрата (тимчасове переривання) і/або недостовірність результатів передавання (перетворення) інформації хоча б в одному з множини трактів циклів управління, передбачених технічними умовами для об’єкта критичної інфраструктури, є фактичним проявом кризової ситуації через їхню непрацездатність (неправильну роботу). Ненавмисні причини такої ситуації через відмову програмно-апаратних засобів розглядаються у контексті теорії надійності, технічної діагностики, а негативний вплив відмов може бути нівельований (зменшений) на основі відповідного методичного апарату. Ознаки, аналогічні відмовам, характерні і прояву тактики *Impact* в кіберінцидентах, що обумовлені акціями *Advanced Persistence Threat*. Оперативне (кризове) реагування на кіберінциденти/кібератаки є прерогативою команди реагування на комп’ютерні надзвичайні події [5–11].

Аналіз останніх публікацій. Для одержання більш повної інформації необхідно звернутися до положень щодо організаційно-технічної моделі кіберзахисту [12]; ролі, завдань, функцій та відповідальності *Computer Security Incident Response Team (CSIRT*) під егідою *The Forum of Incident Response and Security Teams (FIRST)* [13; 14]; організації процесу реагування на кіберіцнденти/кібератаки [15]; компетенції та результатів навчання професійного стандарту “Фахівець з реагування на інциденти кібербезпеки” [16].

Формулювання мети статті. Обґрунтування дослідження наукової проблеми, яка полягає в існуванні протиріччя між практичною необхідністю здійснювати оперативне (кризове) реагування на кіберінциденти несанкціонованого втручання в систему управління технологічними процесами реального часу (об’єкта критичної інфраструктури) у формі кібератак та відсутністю відповідного науково-методичного базису. До розгляду пропонується

пристосування методології підтримки прийняття рішень оперативного персоналу систем управління технологічними процесами реального часу у контексті кібернетичного підходу та нівелювання (усунення, зменшення) впливу невизначеності. Новизною викладеного підходу є відокремлення ситуацій непрацездатності та неправильної роботи програмно-апаратних засобів через відмову або внаслідок кібератаки.

Виклад основного матеріалу. Участь фахівця-оператора в управлінні технологічними процесами об’єкта критичної інфраструктури обумовлена необхідністю контролю та усунення (зменшення) за необхідністю відхилення фактичного результату керуючого впливу (стану об’єкта управління) від очікуваного, що не може бути здійснено автоматично програмно-апаратним комплексом органу управління (рис. 1). Непридатність працездатного програмно-апаратного комплексу (об’єкта управління) своєчасно виробляти правильні керуючі впливи у контексті забезпечення виконання ітерацій циклів управління на всьому часовому інтервалі функціонування об’єкта критичної інфраструктури будемо розглядати як явище “кризова ситуація компрометації тракту управління”. Словосполучення “компрометація тракту управління” пропонується розглядати у контексті понятійного апарату словосполучення “компрометація системи” [17]. У такій інтерпретації “тракт управління” є системою послідовно зв’язаних програмно-апаратних засобів, призначених для передавання (перетворення) інформації у циклі управління, структура якої автоматично утворюється і залишається сталою протягом часового інтервалу мінімум однієї ітерації проходження циклу управління. За умови сталості (непошкодженості) об’єкта управління причинами кризової ситуації компрометації тракту управління може бути:

несвоєчасність надходження (тимчасове припинення, перевищення граничного часу очікування) інформації керуючого впливу від програмно-апаратного комплексу (органу управління) до пристрою зв’язку з об’єктом через непрацездатність і/або неправильну роботу програмно-апаратних засобів тракту каналу прямого зв’язку;

несвоєчасність надходження (тимчасове припинення, перевищення граничного часу очікування) інформації про стан об’єкта управління від пристрою зв’язку з об’єктом до програмно-апаратного комплексу (органу управління) через непрацездатність і/або неправильну роботу програмно-апаратних засобів тракту каналу зворотного зв’язку;

невиконання керуючого впливу і/або неодержання інформації про стан об’єкта управління через непрацездатність і/або неправильну роботу програмно-апаратного засобу пристрою зв’язку з об’єктом, приймача і/або ефектора, та, відповідно, рецептора і/або передавача у його складі.

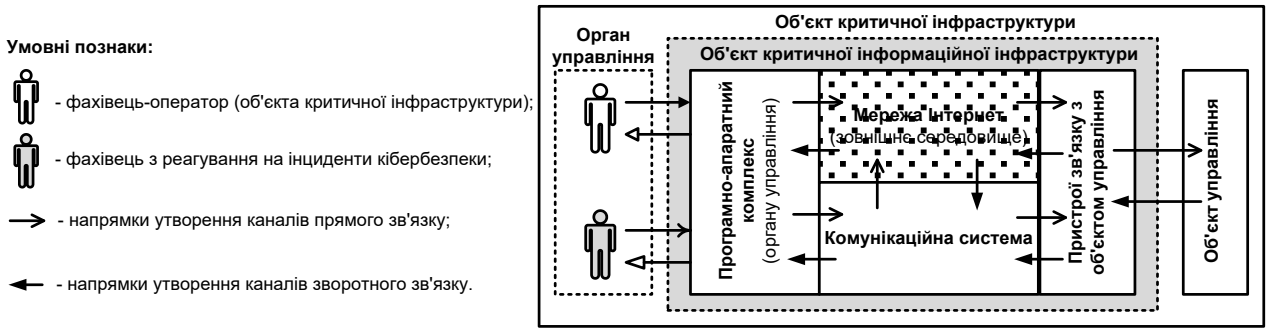

Рис. 1. Функціональна структура об’єкта критичної інфраструктури

Події, які призводять до непрацездатності і/або неправильної роботи програмно-апаратного засобу внаслідок зазвичай складної комбінації випадкових об’єктивних, суб’єктивних факторів (явищ) експлуатаційного, технологічного та організаційного характеру, прийнято асоціювати з поняттям “відмова” [6–9]. Прояв відмов як несприятливих

подій ненавмисного характеру уособлює першу складову поняття “інцидент безпеки критичної інфраструктури”. Друга складова поняття охоплює події несанкціонованого втручання (в функціонування об’єкта критичної інфраструктури). З’єднання комунікаційної системи з мережею Інтернет уособлює логічність розгляду для об’єкта критичної інформаційної інфраструктури (об’єкта критичної інфраструктури) множини форм несанкціонованого втручання у формі кібератаки, кіберпростору як середовища їх здійснення, роль та місце участі фахівця з реагування на інциденти кібербезпеки [12–16].

Сукупність програмно-апаратних засобів, які забезпечують функцію (функціональне призначення) передавання інформації незалежно від її типу або виду у вигляді електромагнітних сигналів, утворюють такі функціональні компоненти (рис. 2):

канал прямого зв’язку для інформації керуючого впливу від програмно-апаратного комплексу (органу управління) в пристрій зв’язку з об’єктом управління;

канал зворотного зв’язку для інформації про стан об’єкта управління від пристрою зв’язку з об’єктом управління у програмно-апаратний комплекс (органу управління).

Пристрій зв’язку з об’єктом управління є програмно-апаратним засобом, який здійснює для перетворення інформації керуючого впливу з каналу прямого зв’язку у форму значень фізичних величин ефекторів впливу на об’єкт управління та інформації про стан об’єкта управління від рецепторів об’єкта управління у форму для каналу зворотного зв’язку.

Множина каналів прямого (зворотного) зв’язку, пристроїв зв’язку з об’єктом управління об’єкта критичної інфраструктури визначається технічним завданням (умовами, проєктом) відповідно до проєктного цільового призначення. Тракт каналу прямого (зворотного) зв’язку є системою послідовно зв’язаних програмно-апаратних засобів, призначених для передавання інформації через канал прямого (зворотного) зв’язку у кіберпросторі об’єкта критичної інформаційної інфраструктури, структура якої автоматично утворюється і залишається сталою протягом часового інтервалу мінімум однієї ітерації проходження циклу управління. Під поняттям “ітерація циклу управління” розглядається неперервне виконання послідовності операцій передавання (перетворення) інформації керуючого впливу від органу управління в об’єкт управління через тракт каналу прямого зв’язку, одержання і доставка інформації про стан об’єкта управління в орган управління через тракт каналу зворотного зв’язку.

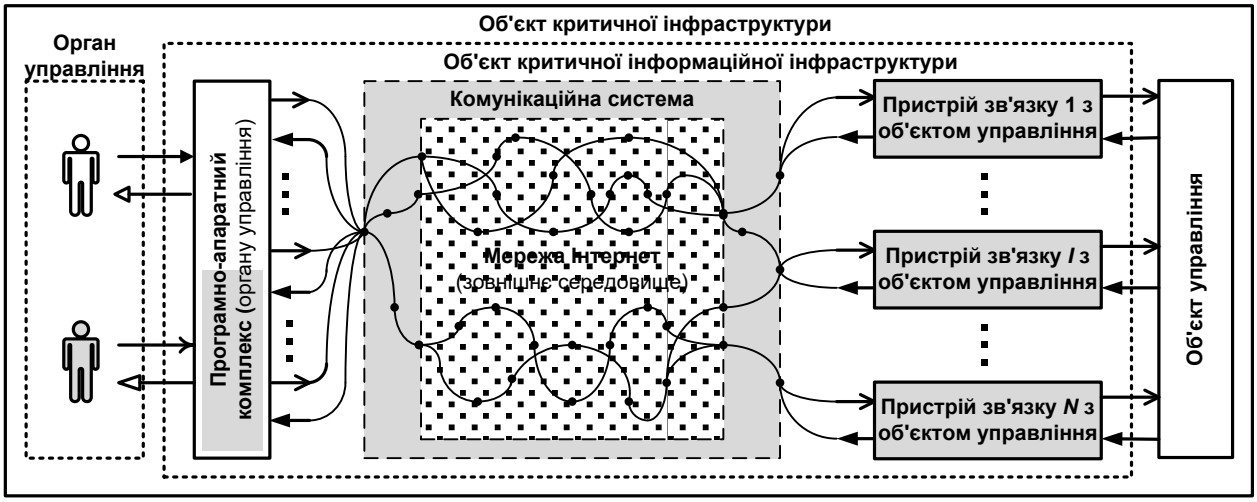

Рис. 2. Функціональні складові діяльності фахівця з реагування на інциденти кібербезпеки

Програмно-апаратний комплекс (органу управління) забезпечує виконання сукупності функцій для вироблення керуючих впливів в циклах управління об’єкта критичної інфраструктури на підставі інформації про стан об’єкта управління. Керуючий вплив є результатом його вибору з множини альтернативних варіантів (альтернатив). Порядок

створення множини альтернатив та вибору однієї з них визначається: методом управління (програмне, оптимальне, авторегулювання); особливостями цільової функції; характером функції оцінки корисності результату керуючого впливу (дослідження операцій, експертне оцінювання, імітаційне моделювання); невідповідністю одержуваної з каналу зворотного зв’язку інформації та реальним станом об’єкта управління. Мінімальна (допустима) невідповідність інформації дозволяє виробляти рішення автоматично на основі відповідних програмних алгоритмів керування, при перевищенні допустимого розходження – автоматизовано, за участю фахівця-оператора (об’єкта критичної інфраструктури).

За умови сталості (непошкодженості) об’єкта управління участь фахівця-оператора (об’єкта критичної інфраструктури) обумовлена явищем невизначеності (неповноти, недостовірності, неточності, обмеженості) та необхідністю його нівелювання (усунення, зменшення) при виборі керуючого впливу. Невизначеність є наслідком прояву одиничних, але, зазвичай, комплексних комбінацій обставин (причин, факторів) на етапах проєктування, розробки, впровадження та експлуатації системи управління технологічними процесами реального часу (об’єкта інформаційної інфраструктури), що передбачає обробку інформації в реальному масштабі часу або у темпі обслуговування технологічних процесів.

Можливість нівелювання (усунення, зменшення) впливу невизначеності базується на застосуванні апробованого науково-методичного апарату для адекватної оцінки, прогнозування та зменшення інтенсивності прояву відповідних обставин (причин, факторів). За характерною природою виникнення, приналежністю етапам життєвого циклу систем об’єкта критичної інформаційної інфраструктури та наявністю адекватного науково-методичного апарату можна відокремити когнітивно-помилкову, відмово-залежну та деструктивно-спрямовану підмножину обставин (причин, факторів) невизначеності.

Когнітивно-помилкова невизначеність. Когнітивна діяльність особи, яка приймає рішення (ОПР), розглядається як багаторівнева сукупність взаємозв’язаних процесів психофізичного, психологічного, гносеологічного та програмного характеру. Основні форми розумової діяльності: емпіричне, аксіоматичне, діалектичне. Емпіричне мислення базується на узагальненні попереднього досвіду, аксіоматичне – на застосуванні початкових знань про правила вирішення задачі. Діалектичне мислення є вищою формою психічних процесів людини, забезпечує позитивний прояв багатоваріантності, адаптації, самоорганізації, вибір рішення в умовах як повної, так і неповної інформації. Людина в ролі ОПР виступає складовим елементом ергатичної системи з функціями приймача, ретранслятора і перетворювача інформації, може здійснювати вибір рішення, контроль роботи об’єкта, вироблювати та виконувати команди.

Прямий чи опосередкований вплив на результат когнітивної діяльності ОПР мають психологічні властивості, які не є вродженими і з розвитком особистості змінюються (формуються) залежно від конкретних суспільно-історичних умов: світогляд (система поглядів на суспільство та природу явищ); інтереси (спрямованість на певні предмети та явища); здібності (індивідуальні особливості – умови успішного виконання якої-небудь однієї або кількох видів діяльності); темперамент; характер; увага (спрямованість свідомості на певний предмет або діяльність: стійкість, перемикання, кількість та розподіл інформаційних одиниць).

При виборі рішення ОПР керується міркуваннями передбачення, досвіду, інтуїції професійної підготовленості та кваліфікації, а також суб’єктивними уявленнями, судженнями, емоціями. Людина має багатоканальне сприйняття, раціональне використання інформації, здатність до навчання, але і може здійснювати помилкові дії через малу пропускну спроможність, обмежену швидкість, втомлюваність, недостатність кваліфікації та досвіду. Основним підходом до нівелювання (усунення, зменшення) прояву когнітивно-помилкової невизначеності при виборі керуючого впливу фахівцем-оператором (об’єкта критичної інфраструктури) є органічне впровадження в його діяльність функцій інформаційної

підтримки прийняття рішень на базі програмно-апаратного комплексу (органу управління). Науково-методичний апарат інформаційної підтримки рішень оперативного персоналу технічних систем у реальному масштабі часу був розроблений та апробований під керівництвом професора Герасимова Б. М. під час проведення багатьох дисертаційних досліджень представниками цієї наукової школи [2; 3; 18].

Відмово-залежна невизначеність. Відмова – випадкова подія, яка полягає у втраті технічним об’єктом (система, компонент, елемент, пристрій, засіб) як самостійної одиниці з погляду надійності, здатності виконувати потрібну функцію. Під поняттям “функція” розглядається властивість такого технічного об’єкта відповідно до вимог нормативної та (чи) конструкторської (проєктної) документації (на етапі розробки вимог, проєктування, виробництва, використання і ремонту об’єкта). Надійність – властивість об’єкта зберігати у часі в установлених межах значення всіх параметрів, які характеризують здатність виконувати потрібні функції в заданих режимах та умовах. В якості випадкових подій (обставин, причин), що можуть призвести до відмови, розглядаються:

недосконаліть, порушення встановлених правил, норм проєктування та конструювання (конструкційна відмова);

невідповідність виготовлення проєкту нормам виробництва (виробнича відмова);

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

відмова чи несправність іншого технічного об’єкта (залежна відмова);

проєкт, виробництво, правила експлуатації, документація (систематична відмова);

перевищення навантаження (відмова через перевантаження);

неправильне чи необережне поводження (відмова через неправильне поводження);

неміцність без перевищення навантаження (відмова через неміцність);

процеси деградації при дотриманні усіх встановлених правил, норм проєктування, виготовлення та експлуатації (деградовна відмова);

непередбачуване стихійне лихо (відмова внаслідок стихійного лиха).

Неповнота (недостовірність, неточність, обмеженість) інформації про закони розподілу ймовірності випадкових подій виникнення відмов розглядається як відмово-залежна невизначеність. Прояв відмово-залежної невизначеності при виборі керуючого впливу фахівцем-оператором (об’єкта критичної інфраструктури) полягає у його залежності від своєчасного і правильного передавання (перетворення) інформації у трактах управління від відмов програмно-апаратних засобів трактів прямого (зворотного) зв’язку, пристроїв зв’язку з об’єктом. Раніше було зазначено, що непрацездатність і/або неправильна робота через відмови програмно-апаратних засобів передавання (перетворення) інформації хоча в одному з множини трактів управління повинна розглядатися як кризова ситуація компрометації тракту управління (об’єкта критичної інфраструктури).

Основним підходом до нівелювання (усунення, зменшення) прояву відмово-залежної невизначеності полягає у застосуванні резервування, оптимального управління запасними елементами, термінами експлуатації, технічного діагностування та обслуговування на основі апріорного аналізу надійності системи управління технологічними процесами (об’єкта інформаційної інфраструктури). Апріорний аналіз надійності полягає в обґрунтуванні вибору одного з можливих варіантів проєктування (створення) технічного об’єкта за умови наявності повної інформації про закони розподілу ймовірності випадкових подій виникнення відмов, що на практиці, зазвичай, повністю невідома для всіх програмно-апаратних засобів технічного об’єкта. Науково-методичний апарат нівелювання (усунення, зменшення) “апріорної невизначеності” в задачах теорії надійності був розроблений та апробований під керівництвом професора Креденцера Б. П. під час проведення багатьох дисертаційних досліджень представниками цієї наукової школи [6–9].

Деструктивно-спрямована невизначеність. Зазвичай, об’єкт управління є різновидом штучної системи, яка складається з множини структурних елементів, які мають фізичне

розташування у межах окремих територіально-технологічних майданчиків об’єкта критичної інфраструктури. Створення та експлуатація власної комунікаційної системи (об’єкта критичної інфраструктури) для утворення трактів каналів прямого (зворотного) зв’язку має високу вартість при значній кількості територіально-технологічних майданчиків, їх розташування на значній географічній відстані, складності побудови ліній комунікації і т. д. Тому, використання мережі Інтернет як універсального комунікаційного середовища між територіально-технологічних майданчиками (об’єкта критичної інфраструктури) полягає у їх комунікації через програмно-апаратні засоби автономних систем локальних провайдерів послуг Інтернету (*Internet Service Providers*).

Така організація трактів каналів прямого (зворотного) зв’язку (об’єкта критичної інфраструктури) зазвичай є найкращим варіантом зменшення відповідних експлуатаційних витрат, але має негативний аспект, який полягає у необхідності врахування можливості несанкціонованого втручання у формі кібератак [19–22]. Кібератака на об’єкт критичної інфраструктури – спрямовані (навмисні) дії в кіберпросторі, які здійснюються суб’єктом кібератаки (на об’єкт критичної інфраструктури) за допомогою засобів електронних комунікацій з метою (ціль) примушення (нав’язування) до прояву кризової ситуації.

Взагалі, поняття “ціль” уособлює очікуваний (ідеалізований, уявний) результат психологічної діяльності людини на певному інтервалі часу. Формулювання цілі виникає як певний стимул змінити поточну ситуацію у потрібному напрямку з урахуванням набутого досвіду. Лінійно-впорядкована послідовність дій, спрямована на досягнення цілі з деякої фіксованої початкової ситуації, називається траєкторією діяльності. Траєкторія діяльності є сукупністю структурованих казуальних відношень (причинно-наслідкові зв’язки, ланцюги зв’язків) просування до головної цілі через проміжні (часткові, тактичні). Ланцюжок зі структурованої послідовності типових дій (процедур), в якому кожна чергова дія створює умови для здійснення наступної, називається казуальним сценарієм. Поняття “сценарій” означає формалізований опис стереотипних знань у формі стандартної послідовності взаємозв’язаних фактів типової ситуацій предметної області, послідовності дій або процедур досягнення цілей. Стереотипні знання – опис предметної області у формі послідовності фактів, який дозволяє передбачати та відновлювати пропущені факти.

Ціль кібератаки на об’єкт критичної інфраструктури уособлює очікуваний (ідеалізований, уявний) результат психологічної діяльності суб’єкта кібератаки (на об’єкт критичної інфраструктури) за визначений час для її досягнення (здійснення кібератаки). Введення поняття “суб’єкт кібератаки” здійснено для підкреслювання визначальної ролі антропогенної (людської) природи здійснення спрямованих (навмисних) дій у кіберпросторі з метою (ціль) примушення (нав’язування) до прояву кризової ситуації (об’єкта критичної інфраструктури) у формі проходження (виконання) відомої структурованої послідовності типових дій (процедур) казуального сценарію кібератаки. Отже, казуальний сценарій кібератаки визначає траєкторію діяльності суб’єкта кібератаки, яка спрямована на досягнення цілі кібератаки.

Примушення (нав’язування) до прояву кризової ситуації (ціль кібератаки на об’єкт критичної інфраструктури) може здійснюватися шляхом порушення штатного функціонування системи управління технологічними процесами (об’єкта критичної інформаційної інфраструктури), що полягає в одержанні хоча б одного успішного результату застосування технічних способів (*techniques*) на етапі досягнення тактичної цілі (*tactic*) *Impact* у такій формі (рис. 3):

відмова обслуговування (тимчасове припинення) пристрою зв’язку з об’єктом і/або ефектору в його складі (*Denial of Control*);

Рис. 3. Граф відношень між етапами досягнення тактичних цілей (*tactics*) казуального сценарію кібератаки на об’єкт критичної інфраструктури

відмова обслуговування (тимчасове припинення) пристрою зв’язку з об’єктом і/або рецептору в його складі (*Denial of View*);

недоступність пристрою зв’язку з об’єктом (*Loss of Availability*);

непрацездатність тракту каналу прямого зв’язку (*Loss of Control*);

непрацездатність тракту каналу зворотного зв’язку (*Loss of View*);

нав’язування хибної інформації керуючого впливу (*Manipulation of Control*);

нав’язування хибної інформації про стан об’єкта управління (*Manipulation of View*);

непрацездатність і/або неправильна робота функцій (процедур) безпеки технологічних процесів від несанкціонованого втручання (*Loss of Protection*);

непрацездатність і/або неправильна робота функцій (процедур) обробки аварійних ситуацій технологічних процесів (*Loss of Safety*);

порушення конфіденційності (витік) інформації керуючого впливу і/або про стан об’єкта управління (*Theft of Operation Information*);

довготривале та приховане нав’язування інформації керуючого впливу і/або про стан об’єкта управління для фізичного руйнування технологічних процесів (*Damage of Property*);

довготривале та приховане нав’язування інформації керуючого впливу і/або про стан об’єкта управління для зменшення продуктивності, якості, корисного ефекту технологічних процесів (*Loss of Productivity and Revenue*).

Досягнення цілі кібератаки на об’єкт критичної інфраструктури шляхом одержання хоча б одного успішного застосування технічних способів на етапі досягнення тактичної цілі *Impact* базується на якісному відпрацюванні етапів досягнення тактичних цілей та стадій:

Reconnaissance – збирання (узагальнення, аналіз) інформації про об’єкт критичної інформаційної інфраструктури (об’єкта критичної інфраструктури) для вироблення (уточнення) можливих казуальних сценаріїв для одержання успішного результату на етапі досягнення тактичної цілі *Gaining Access*;

Resource Development – підготовка (розробка) засобів для виконання казуальних сценаріїв одержання успішного результату на етапі досягнення тактичної цілі *Gaining Access*;

Gaining Access – стадія набуття повноважень авторизованого користувача в операційному середовищі хоча б одного з множини програмно-апаратних засобів функціональних компонентів системи управління технологічними процесами для виконання можливих казуальних сценаріїв для одержання успішного результату на етапі досягнення тактичної цілі *Action On Objects*;

Action On Objects – стадія багатоітераційного виконання казуальних сценаріїв для забезпечення можливості одержання успішного результату на етапі досягнення тактичної цілі *Impact*.

Орієнтовані дуги (див. рис. 3, *а–в*) ілюструють необхідність повернення до попередніх етапів (стадій) при неякісному результаті досягнення тактичних цілей відповідно до *Reconnaissance, Resource Development, Action On Objects*:

відсутність повної інформації для підготовки (розробки) засобів для виконання казуальних сценаріїв, у тому числі разом із виробленням іншого (більш перспективного) казуального сценарію одержання успішного результату на етапі досягнення тактичної цілі *Gaining Access* (див. рис. 3, *а*);

неможливість набуття повноважень авторизованого користувача в операційному середовищі хоча б одного з множини програмно-апаратних засобів функціональних

компонентів системи управління технологічними процесами, що обумовлює необхідність удосконалення (доробки) засобів для виконання казуальних сценаріїв одержання успішного результату стадії *Gaining Access* (див. рис. 3, *б*);

недостатність виконання дій *Action On Objects* для одержання хоча б одного успішного результату застосування технічних способів на етапі досягнення тактичної цілі *Impact*, у тому числі разом із виробленням іншого казуального сценарію одержання успішного результату стадії *Action On Objects* (див. рис. 3, *в*):

Persistence (забезпечення постійності повноважень *Initial Access*);

Privilege Escalation (розширення/зміна повноважень *Initial Access*);

Defense Evasion (запобігання виявлення несанкціонованого використання авторизованих повноважень *Initial Access* та *Privilege Escalation*);

Credential Access (одержання облікових та автентифікаційних даних для легітимного набуття повноважень поза контекстом тактичних цілей *Initial Access* та *Privilege Escalation*);

Discovery (одержання відомостей про внутрішню структуру та компоненти системи);

Lateral Movement (набуття авторизованих повноважень в операційному середовищі іншого програмно-апаратного засобу за результатами *Discovery*, але поза *Initial Access*);

Collection (акумулювання інформації системи для підготовки її подальшого витоку);

Command and Control (утворення прихованого каналу управління компонентом системи з повноваженнями авторизованого користувача);

Exfiltration (здійснення витоку інформації з циклів управління);

Inhibit Response Function (блокування процедур реагування на небезпечні стани технологічного процесу);

Impair Process Control (модифікація процедур реагування на небезпечні стани технологічного процесу та обробки інформації).

Прояв деструктивно-спрямованої невизначеності при виборі керуючого впливу фахівцем-оператором (об’єкта критичної інфраструктури) полягає у принциповій неповноті (недостовірності, неточності, обмеженості) інформації про успішний результат спрямованої (навмисної) реалізації суб’єктом кібератаки деструктивних технічних способів *Manipulation of Control, Manipulation of View, Loss of Protection, Loss of Safety, Damage of Property, Loss of Productivity and Revenue* на етапі досягнення тактичної цілі *Impact*, початок яких був раніше моменту спостереження та мав приховані ознаки акції *Advanced Persistent Threat*. Деструктивно-спрямована невизначеність уособлює складну комбінацію випадкових подій, обумовлених антропогенною (людською) сутністю суб’єкта кібератаки (на об’єкт критичної інфраструктури), для яких зазвичай невідома або принципово не може бути визначена функція розподілу ймовірностей, зокрема:

вибір певного варіанту з множини можливих казуальних сценаріїв траєкторії діяльності суб’єкта кібератаки (рис. 4) при застосуванні технічних способів (*techniques*) на етапах досягнення тактичних цілей:

− *Initial Access*, *Execution* стадії *Gaining Access*;

− *Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, Inhibit Response Function, Impair Process Control* багатоітераційного проходження стадії *Action On Objects*;

− *Execution* стадії *Action On Objects*;

комбінування мотивації, кваліфікації та ресурсних обмежень суб’єкта кібератаки;

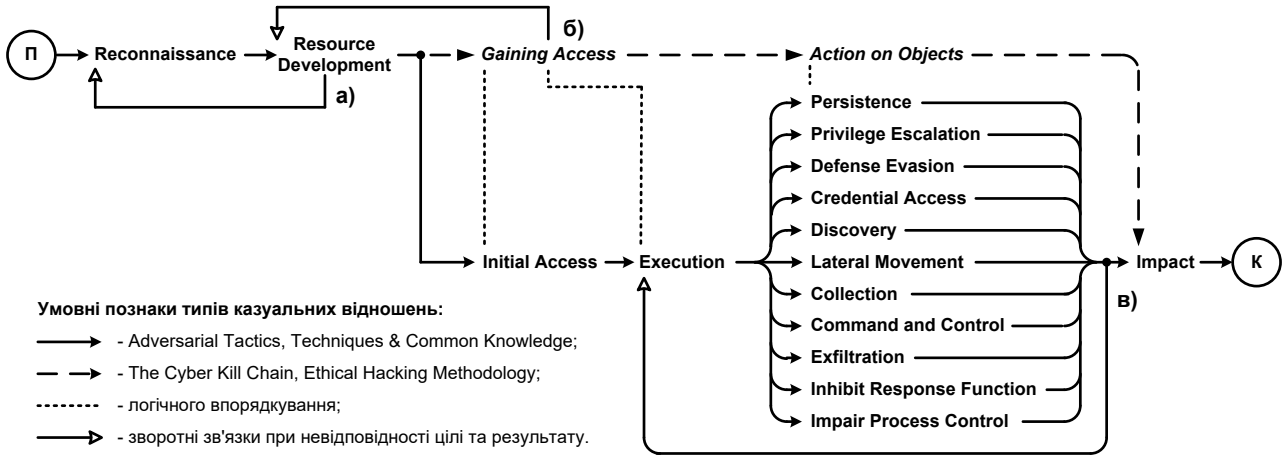

Рис. 4. Граф відношень формування можливих варіантів казуальних сценаріїв траєкторії діяльності суб’єкта кібератаки на об’єкт критичної інфраструктури

спроможність групового суб’єкта кібератаки забезпечити паралельність, координацію, обмін інформацією при виконанні незалежних операцій на множині можливих казуальних сценаріїв та технічних способів на етапах досягнення тактичних цілей та стадій;

наявність співпраці з інсайдером і/або інсайдерської інформації;

час початку суб’єктом кібератаки етапу досягнення тактичної цілі *Reconnaissance* та якість (повнота інформації) результатів його виконання;

час початку суб’єктом кібератаки стадії *Gaining Access*;

відрізок часу від початку суб’єктом кібератаки стадії *Gaining Access* до виявлення ознак її успішного результату;

відрізок часу від початку стадії *Gaining Access* до успішного результату етапу досягнення тактичної цілі *Impact*;

можливість розробки суб’єктом кібератаки на етапі досягнення тактичної цілі *Resource Development* новітніх засобів (з невідомими ознаками виявлення) для застосування технічних способів (*techniques*) на стадіях *Gaining Access* та *Action On Objects*.

Для з’ясування ролі орієнтованих дуг (див. рис. 4, *а–в*) необхідно звернутися до відповідних пояснень на граф відношень між етапами досягнення тактичних цілей (*tactics*) казуального сценарію кібератаки на об’єкт критичної інфраструктури (див. рис. 3, *а–в*). Успішний результат хоча б одного технічних способів на етапах досягнення тактичної цілі *Initial Access* та *Execution* утворюють комплекс умов для активації виконання шкідливого програмного засобу суб’єкта кібератаки в операційному середовищі деякого програмно-апаратного засобу системи управління технологічними процесами об’єкта критичної інфраструктури з повноваженнями авторизованого користувача.

Нівелювання (усунення, зменшення) прояву деструктивно-спрямованої невизначеності при виборі керуючого впливу фахівцем-оператором (об’єкта критичної інфраструктури) полягає у забезпеченні своєчасного та правильного оперативного (кризового) реагування на кіберінциденти. Реагування на кіберінциденти – структурована сукупність дій, спрямованих на підготовку до кіберінцидентів, їх виявлення та аналіз, мінімізацію шкоди від кіберінциденту та запобігання їх повторенню у майбутньому [5; 12; 17].

Раніше було доведено, що основна семантична відмінність поняття “кіберінцидент” від поняття “інцидент безпеки критичної інфраструктури” полягає в актуалізації розгляду для об’єктів критичної інфраструктури значної множини відомих казуальних сценаріїв здійснення несанкціонованого втручання у формі кібератак. За умови сталості (непошкодженості) об’єкта управління, програмно-апаратних засобів системи управління технологічними процесами в реальному масштабі часу (об’єкта критичної інформаційної інфраструктури) порушення

штатного функціонування об’єкта критичної інфраструктури здійснюється шляхом компрометації (хоча б одного, підмножини, всіх елементів) множини трактів управління технічними способами (*techniques*) досягнення тактичної цілі *Impact*. Своєчасне виявлення та аналіз фахівцем з реагування на інциденти кібербезпеки кіберінцидентів типу “кризова ситуація компрометації тракту управління”, вироблення множини автоматичних/ автоматизованих сценаріїв виконання завдань стримування, усунення та відновлення штатного функціонування уособлює сутність практичних потреб.

Висновки. Усунення протиріччя між потребами практики та відсутністю необхідного теоретичного базису (наукова проблема) полягає у розробці науково-методичного апарату інформаційної підтримки вибору рішень фахівцем із реагування на інциденти кібербезпеки при виявленні, усуненні, стримуванні кіберінцидентів типу “кризова ситуація компрометації тракту управління” систем управління технологічними процесами в реальному масштабі часу, а також відновленні штатного функціонування об’єкта критичної інфраструктури.

В якості *найближчої перспективи* оприлюднення результатів дослідження наукової проблеми планується модель оцінки тривалості виконання казуального сценарію кібератаки на систему управління технологічними процесами в реальному масштабі часу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

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

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

3. 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.

4. Хусаінов П. В., Штаненко С. С. Обґрунтування інформаційної підтримки фахівця з реагування на інциденти кібербезпеки об’єкта критичної інфраструктури // Системи і технології зв’язку, інформатизації та кібербезпеки: збірник наукових праць / за заг. ред. Г. Д. Радзівілова. К.: Військовий інститут телекомунікацій та інформатизації ім. Героїв Крут. 2025. № 8. С. 269–280. DOI: 10.58254/viti.8.2025.21.269.

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

6. ДСТУ 2860-94 Надійність техніки. Терміни та визначення. [Чинний від 1995-01-01]. URL: https://dbn.co.ua/load/normativy/dstu/dstu_2860_94/1-1-0-1099.

7. 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.

8. ДСТУ 2389-94 Технічне діагностування та контроль технічного стану. Терміни та визначення. [Чинний від 1995-01-01]. URL: https://dbn.co.ua/load/normativy/dstu/1-1-0-1094.

9. Фізичні основи теорії надійності: підруч. / М. К. Жердєв, С. В. Лєнков, Б. П. Креденцер та ін.; за ред. М. К. Жердєва. К.: Видавничо-поліграфічний центр “Київський університет”, 2008. 215 с.

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

11. Хусаінов П. В., Терещенко Т. П., Череушенко В. Б. Формування альтернативних стратегій тестування на проникнення Server-Side Web Application із врахуванням зменшення невизначеності // Системи і технології зв’язку, інформатизації та кібербезпеки: збірник наукових праць / за заг. ред. Г. Д. Радзівілова. К.: Військовий інститут телекомунікацій та інформатизації ім. Героїв Крут. 2025. № 8. С. 257–268. DOI: 10.58254/viti.8.2025.20.257.

12. Про затвердження Положення про організаційно-технічну модель кіберзахисту: постанова КМУ від 29.12.2021 № 426 // Офіційний вісник України. 2022. № 4. С. 247. Ст. 219.

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

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

16. 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.

17. 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.

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

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

20. The Unified Kill Chain. URL: https://www.unifiedkillchain.com.

21. Certified Ethical Hacker. URL: https://cert.eccouncil.org/certified-ethical-hacker.html.

22. Хусаінов П. В., Черниш Ю. О., Терещенко Т. П. Зменшення невизначеності оцінки часу компрометації Server-Side Web Application об’єкта критичної інфраструктури // Системи і технології зв’язку, інформатизації та кібербезпеки: збірник наукових праць / за заг. ред. Г. Д. Радзівілова. К.: Військовий інститут телекомунікацій та інформатизації ім. Героїв Крут. 2025. № 7. С. 232–242. DOI: 10.58254/viti.7.2025.21.232.

Надійшла до редколегії 08.04.2026.
Схвалена до друку 22.05.2026.
Дата публікації 29.05.2026.