INFORMATION SECURITY

DOI 10.20535/2411-1031.2022.10.1.261047
УДК 004(056.5+072)

СЕРГІЙ ВАСИЛЕНКО,
ІГОР САМОЙЛОВ,
СЕРГІЙ БУР'ЯН

МЕТОД УПРАВЛІННЯ СТАНОМ ЗАХИЩЕНОСТІ АВТОМАТИЗОВАНОЇ СИСТЕМИ УПРАВЛІННЯ ТЕХНОЛОГІЧНИМ ПРОЦЕСОМ ОБ'ЄКТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Постійні динамічні процеси інформатизації суспільства докорінно змінюють усі сфери його життєдіяльності, надаючи їм нових імпульсів розвитку та можливості реалізації в нових умовах. Одночасно ці процеси є причиною появи принципово нових викликів для безпекової сфери, що обумовлюється глибинним проникненням інформаційних технологій у всі елементи інфраструктури, у тому числі і критичної. Особливо небезпечними є кібератаки направлені на об'єкти критичної інформаційної інфраструктури об'єктів критичної інфраструктури, що можуть призвести до катастрофічних наслідків як для конкретного підприємства чи галузі, так і для екології та економіки країни в цілому. Велика частина кіберзагроз об'єктів критичної інформаційної інфраструктури об'єктів критичної інфраструктури пов'язана з масовою імплементацією таких технологій Індустрії 4.0 як: цифрові екосистеми, промисловий Інтернет речей, аналітика великих даних, використання цифрових платформ. Пов'язані з цим ризики вимагають нових рішень у методах управління станом захищеності об'єктів критичної інформаційної інфраструктури об'єктів критичної інфраструктури. У роботі в якості об'єктів критичної інформаційної інфраструктури об'єктів критичної інфраструктури розглядається автоматизована система управління технологічним процесом побудована з використання сенсорів промислового Інтернету речей, що значно полегшує процес розгортання персональних мереж для контролю та моніторингу промислових процесів та пришвидшує процес прийняття управлінських рішень. Представлено основні рівні типової автоматизованої системи управління технологічним процесом об'єктів критичної інфраструктури та наведено можливі шляхи проникнення шкідливого програмного забезпечення на кожному з них. Особливості побудови автоматизованої системи управління технологічним процесом об'єктів критичної інфраструктури та необхідність швидкого реагування на будь-які кіберінциденти вимагає автоматизації процесу прийняття управлінських рішень щодо застосування необхідних засобів захисту. Для управління станом захищеності від кібератак на автоматизовані системи управління технологічним процесом об'єктів критичної інфраструктури запропоновано використовувати метод прийняття управлінських рішень на основі динамічного програмування, що дозволить у залежності від типу кібератаки, здійснювати вибір та застосування відповідних засобів захисту, а також зменшити негативні наслідки реалізації кіберінцидентів.

Ключові слова: об'єкт критичної інфраструктури, автоматизована система управління технологічним процесом, промисловий Інтернет речей, управління станом захищеності, динамічне програмування.

Постановка проблеми. З метою пришвидшення процесу прийняття рішень, а також зниження негативного впливу операторів на процеси управління сучасні промислові підприємства все більше автоматизують процеси управління технологічним обладнанням. Керування здійснюється за допомогою автоматизованої системи управління технологічним процесом (АСУ ТП). Структура сучасних АСУ ТП відрізняється від звичайних корпоративних мереж наявністю спеціалізованих технічних та програмних засобів призначених для автоматизації процесу управління технологічним обладнанням підприємства.

У випадку якщо промислове підприємство за типом своїх основних послуг відноситься до об'єктів критичної інфраструктури автоматизована система управління технологічним процесом такого підприємства є об'єктом критичної інформаційної інфраструктури об'єкту критичної інфраструктури (ОКІІ ОКІ) та потребує вдосконалення системи захисту інформації.

У сучасних умовах розвитку та модифікації АСУ ТП кіберзагрози набувають організованих та цілеспрямованих рис та носять багатокроковий характер. Реалізація більшості кібератак здійснюється за допомогою використання високотехнологічних методів збору та обробки даних системи. Використання сучасних методів та засобів несанкціонованого доступу до ресурсів АСУ ТП може призвести не тільки до порушення функціонування ОКІ, а і стає інструментом зловмисника для створення цілого ряду загроз безпеці держави. Проблеми зростають при впровадженні у АСУ ТП технологій Індустрії 4.0 (І 4.0), особливо це стосується промислового Інтернету речей (ІІоТ), який передбачає використання ІІоТ-сенсорів та постійний зв'язок системи з глобальною мережею, в тому числі мережу Інтернет. У даних умовах система захисту ОКІІ має будуватися виходячи з необхідності реагування на комплекс загроз та їх узгоджену реалізацію і спрямовуватися на забезпечення стійкості функціонування ОКІ [1].

Складовою частиною системи управління інформаційною безпекою, у тому числі АСУ ТП об'єкту критичної інфраструктури, є підсистема оцінювання рівня захищеності інформаційної системи, що призначена для визначення ефективності застосованих засобів захисту і формування рекомендацій щодо підвищення її безпеки [2].

Аналіз останніх досліджень і публікацій. Аналіз світового досвіду останніх чотирьох років показав, що кількість кібератак на промисловий сегмент зросла на 110 %. При цьому, лише у другій половині 2021 року, кількість кібератак зросла щонайменше на 25 %. Проведені охоронною компанією Claroty дослідження показали, що майже 87 % уразливостей ОКІ були оцінені як атаки "невисокої складності". До них відносять вразливості пов'язані з відмовою в обслуговуванні, віддаленим виконанням коду, обходом механізмів захисту та можливістю зловмисникам отримувати доступ до даних програм. Причиною майже двох третин (63 %) зазначених атак є недостатній захист віддаленого мережевого доступу до обладнання. Більшість уразливостей (70%) можуть використовуватися без спеціальних привілеїв, а 64% взагалі не потребують взаємодії з користувачем [3].

Аналізуючи ситуацію в Україні починаючи з 2014 року основні вектори кібератак країни агресора направлені на спробу закріпитися у державних та банківських інформаційних системах та системах ОКІ, а також ряді приватних та державних секторів для подальших деструктивних дій шляхом використання шкідливого програмного забезпечення та DDoS-атак [4].

У звітах провідних організацій світу зазначено, що вразливості ОКІ в умовах розвитку І 4.0 виходять за межі операційних технологій та стосуються технологій ІІоТ та потребують створення єдиної системи управління інформаційною безпекою [3].

Розгортання ІІоТ-пристроїв у кіберфізичному середовищі полегшує розгортання персональних мереж для контролю та моніторингу промислових процесів. Але у зв'язку з недосконалістю системи захисту ІІоТ-сенсорів зазначені системи є привабливими для кіберзлочинців та потребують захисту [5] - [7].

Незважаючи на постійно зростаючу кількість публікацій, присвячених інформаційній безпеці, питання забезпечення кіберзахисту об'єктів критичної інфраструктури залишається актуальним та потребують вдосконалення процесів оцінювання та управління станом захищеності автоматизованих систем, а також впровадження сучасних методів виявлення кіберінцидентів і прийняття управлінських рішень щодо застосування засобів захисту в режимі реального часу.

Метою статті є визначення правила прийняття рішень щодо виявлення кіберінцидентів та вибору засобів захисту на АСУ ТП ОКІ в умовах розвитку Індустрії 4.0 від впливу кібератак.

Виклад основного матеріалу дослідження. Сучасні засоби забезпечення інформаційної безпеки здатні значно знизити ризики, які виходять від різного роду загроз (починаючи від

звичайних зловмисних програм і закінчуючи складними кібератаками). Особливості побудови та функціонування промислових інформаційних системах, а особливо фізично ізольованих, досить часто не передбачають застосування таких засобів.

Фізична ізоляція не здатна зупинити цільові атаки [8] - [10]. (як приклад – атаки на енергетичні об'єкти і критичні сектори України за допомогою програми BlackEnergy) і використання промислової кіберзброї (наприклад Stuxnet 11 та Irongate 12), а також стандартне зловмисне програмне забезпечення (ПЗ), яке регулярно виявляють на ізольованих об'єктах. Векторів атаки досить багато – починаючи від інженера, який приніс в ізольовану мережу заражений пристрій, і закінчуючи підрядником, що здійснює роботи на об'єкті. Окрім того атаки на промислові об'єкти тепер не тільки прерогатива кібертерористів і державних спецслужб інших країн, а й звичайних хакерів. З широким розповсюдженням IIoT кіберзлочинці активізуються ще сильніше. Крім зараження зловмисним ПЗ і цільових атак промислові організації стикаються з низкою інших кіберзагроз та ризиків, спрямованих проти всіх елементів інфраструктури: людей, процесів і технологій.

До основних ризиків, що можуть призвести до серйозних наслідків на ОКІ відносяться наступні інциденти:

- помилки та збої програмно-апаратних компонентів промислових систем;
- випадкові або навмисні помилкові дії співробітників або підрядників;
- шахрайські операції в АСУ ТП;
- необізнаність про правила розслідування кіберінцидентів та особливості збору достовірних даних про них [11].

Автоматизовані системи управління технологічним процесом вимагають зовсім іншого підходу до забезпечення кібербезпеки в порівнянні з класичною IT-інфраструктурою. У корпоративних середовищах основна увага приділяється збереженню конфіденційних даних, а безперебійна робота не настільки важлива, як для АСУ ТП, де ціна хвилини простою, як і будь-якої іншої помилки, дуже велика. Тому в забезпеченні безпеки технологічних процесів діє протилежний підхід, при якому основним завданням є підтримка їх безперервності і оперативне усунення будь-яких збоїв. Окрім того, промислова інфраструктура містить у собі вкрай спеціалізовані елементи, що не зустрічаються в корпоративних мережах: системи диспетчерського управління та збору даних, людино-машинні інтерфейси, програмовані логічні контролери та багато інших, що не підтримуються традиційними засобами забезпечення інформаційної безпеки.

Цикли оновлення програмного і апаратного забезпечення в промислових середовищах більш протяжні, оскільки часто на промислових об'єктах зустрічається ПЗ, яке вже давно не підтримується та містить безліч вразливостей. Такі умови також не дають змогу ефективно працювати традиційним засобам забезпечення інформаційної безпеки. Інструменти промислового кіберзахисту повинні відповідати вимогам державних і галузевих стандартів. Додатковою складністю є розмитість зони відповідальності за забезпечення промислової кібербезпеки: дуже часто промисловий рівень є доменом інженерів АСУ ТП, які відносяться до засобів забезпечення інформаційної безпеки як до перешкоди, здатної негативно впливати на технологічний процес. При цьому ринок інструментів забезпечення інформаційної безпеки, створених спеціально для захисту промислових об'єктів активно розвивається [11].

Важливою особливістю забезпечення промислової кібербезпеки є те, що кожен проєкт такого роду унікальний – так само, як і кожна промислова інфраструктура, в яку неможливо встановити стандартизовані продукти. Підбір оптимальної конфігурації захисних технологій і набору сервісів здійснюється після повного обстеження поточної системи безпеки промислового об'єкта, а імплементація обраних заходів відбувається тільки в спеціально відведене технологічне вікно, щоб не впливати на процес роботи системи. Незважаючи на трудомісткість подібного проєкту, результатом правильної інтеграції спеціалізованого рішення буде діюча концепція багаторівневого захисту: через поєднання різних методів превентивного захисту, моніторингу та інших сервісів оператор критичної інфраструктури отримує засіб, що

дає змогу реагувати на кіберінциденти на всіх можливих стадіях – від прогнозування потенційних атак і безпосереднього захисту від них до виявлення комплексних загроз і зниження шкоди.

У загальному вигляді АСУ ТП ОКІ представляє собою складну людино-машинну систему, що складається з великої кількості різнорідних елементів, що за допомогою інформаційних зв'язків об'єднані в підсистеми. До складу АСУ ТП ОКІ входять:

- технічні засоби (датчики, прилади, контролери) та програмне забезпечення (операційні системи (ОС), середовище розробки, ПЗ для контролера) АСУ ТП;
- комплекс інтелектуальних рішень, політик та правил, що описують архітектуру та функції.

Типова АСУ ТП ОКІ може бути представлена у вигляді трьох рівнів:

І рівень – мережа управління. Станції управління, що знаходяться в даній мережі, здійснюють управління контролерами, які отримують інформацію прийняту від датчиків ділянок ТП ОКІ.

ІІ рівень – виробнича мережа. У даному сегменті мережі знаходяться сервери даних на яких зберігаються дані, що циркулюють в системі.

ІІІ рівень – адміністративна мережа, що здійснює безпосереднє управління ТП ОКІ.

Варто також відмітити, що ІІІ рівень АСУ ТП ОКІ може мати вихід до мережі Internet, що значно підвищує ймовірність реалізації кібератак (рис. 1).

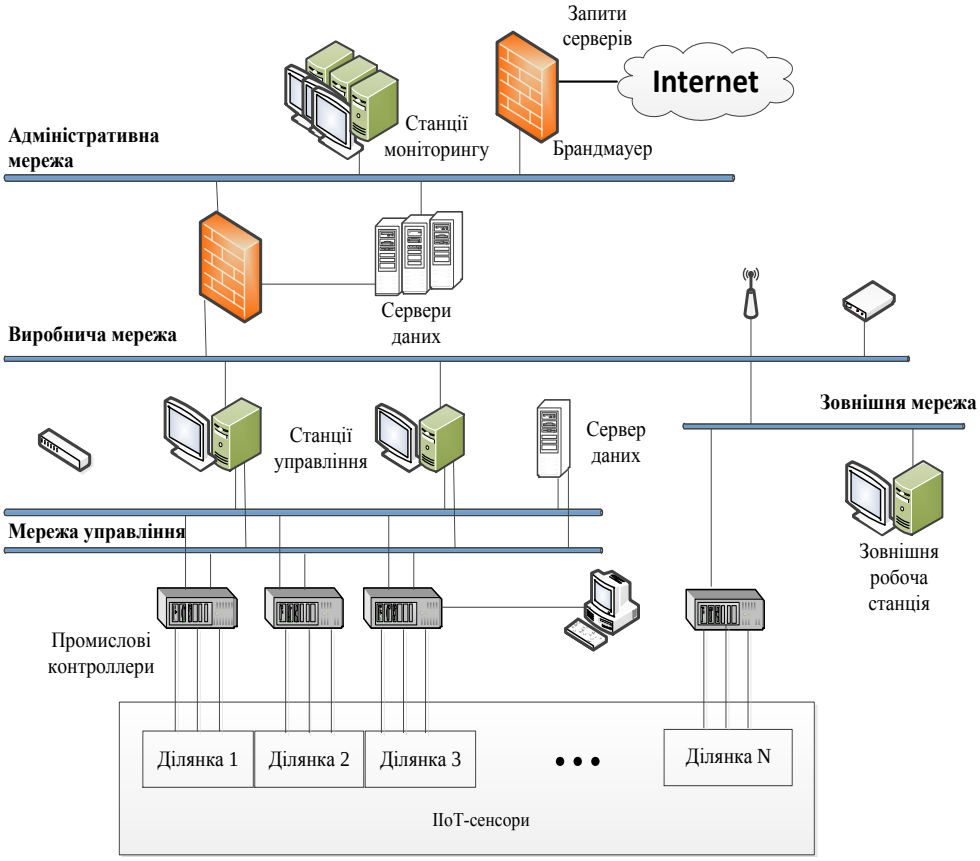

Рисунок 1 – Автоматизована система управління технологічним процесом ОКІ

На сьогодні у промислових системах управління спостерігається поступовий перехід засобів управління на стандарт Ethernet та протоколи TCP/IP [12], що впливає на пов'язаність процесів всередині систем управління в бік їх ускладнення. Побудова мереж АСУ ТП за принципом офісних мереж призводить до міграції вразливостей останніх в промисловий IT-сегмент, тобто системи стали відкриті до нових джерел загроз, на які їх розробники не розраховували. При цьому суттєво зросла кількість збоїв і простоїв обладнання через наслідки

дії зловмисного ПЗ та кібератак. Внаслідок цього виникають певні протиріччя. З одного боку, Ethernet-мережа дає змогу вивести процес автоматизації на новий рівень. З іншого – зловмисне ПЗ може вплинути на виробничий процес та нанести збитки [13].

На відміну від IT-безпеки, що фокусується на захисті даних від крадіжки (таких як дані кредитних карток, персональні дані та інші), головна мета заходів кіберзахисту ОКІІ ОКІ – це підтримувати виробництво у робочому та безпечному стані. Основні загрози для обох цілей – це проникнення зловмисника чи його ПЗ до системи.

Основними шляхами інфікування системи зловмисним ПЗ є:

- використання існуючих механізмів обміну для передачі файлів та віддаленого доступу до систем, наприклад надання загального доступу до файлів та протоколу передачі файлів;
- відкриття користувачем файлів, або запуск програм, що містять шкідливе ПЗ;
- використання уразливостей програмного забезпечення АСУ ТП ОКІ для виконання зловмисного коду в системі;
- автоматичне копіювання файлів з портативних носіїв даних, таких як USB-накопичувачі, CD, DVD та мобільних телефонів, до системи [12].

Наведені шляхи проникнення шкідливого ПЗ до АСУ ТП ОКІ представлені на рис. 2.

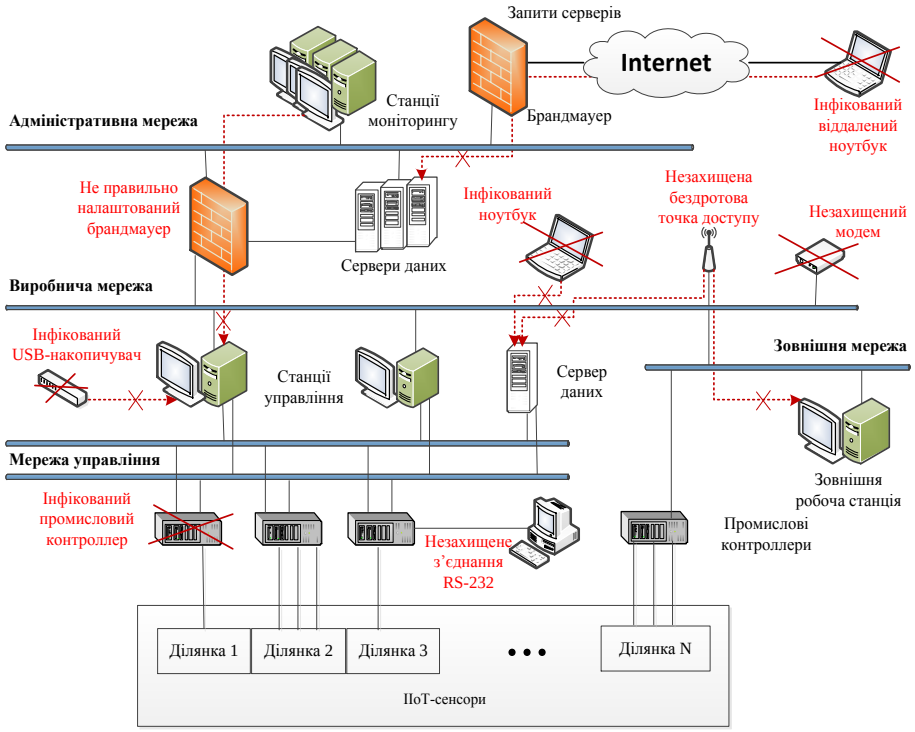

Рисунок 2 - Можливі шляхи проникнення зловмисного ПЗ до автоматизованої системи управління технологічним процесом ОКІ

Процес забезпечення кібербезпеки ОКІ передбачає протидію деструктивному впливу у цій сфері. Для цього необхідне створення та організація потужної підсистеми кіберзахисту із можливістю управління станом захищеності в режимі реального часу.

Оскільки кіберзагрози ОКІ реалізуються різнонаправленими кібератаками необхідно здійснювати управління станом захищеності. Існуючі системи управління станом захищеності передбачають прийняття рішень щодо виявлення кіберзагроз на основі обробки множини параметрів. Для цього може бути використаний метод управління станом захищеності від кібератак на основі динамічного програмування [14].

Для прикладу розглянемо можливість використання даного методу для АСУ ТП ОКІ. Для опису бази вхідних параметрів системи, що використовуються для виявлення атаки

застосовується механізм логічного виводу. На підставі співставлення вхідних параметрів системи з еталонними (отриманими на етапі введення в експлуатацію) здійснюється виявлення ознак зміни стану та приймається рішення щодо захищеності АСУ ТП ОКІ.

У відповідності до наведених вище шляхів проникнення зловмисного ПЗ в АСУ ТП ОКІ (рис. 2) можна виділити вісім типів атак на систему. Враховуючи той факт, що зазначені атаки можуть відбутися на кожному з мережевих рівнів вхідними параметрами системи є:

$$X = X1 \cup X2 \cup X3,$$

де $X1 = \{x_i(t), i = \overline{1,8}\}$ – множина параметрів на мережевому рівні;

$X2 = \{x_i(t), i = \overline{1,8}\}$ – множина параметрів на виробничому рівні;

$X3 = \{x_i(t), i = \overline{1,8}\}$ – множина параметрів на адміністративному рівні.

Вибір заходів захисту системи при повному описі АСУ ТП здійснюється на основі динамічного програмування з урахуванням стратегій впливу на неї.

Ймовірність здійснення j_z кібератак на множину об'єктів l може бути обчислена як:

$$P(j_z, l) = \prod_{v=1}^{l} P_v^{j_z}$$

Процес застосування засобів захисту (ЗЗ) реалізуються покроково: на кожному k-ому кроці виникає деяка сукупність даних про стан захищеності в певний фіксований момент часу $X(t) = \{x_1, ..., x_8\}$ та можливі порушення безпеки $\Lambda = \{\lambda_1, ..., \lambda_n\}$. Використовуючи отримані та наявні в БД відомості про стан захищеності приймається управлінське рішення щодо застосування конкретних ЗЗ $U_k = U(t) = \{u_1, ..., u_n\}$. На таке рішення впливають раніше прийняті рішення $U_{k-1}, U_{k-2}, ..., U_{k-l}$, а повна сукупність даних про стан захищеності системи $X(t)$, рішень про застосування ЗЗ U та реалізовані варіанти впливу на порушення безпеки Λ може бути описана як:

$$X(t) = \{x_1, ..., x_8\}, \quad U = \{U_1, ..., U_k\}, \quad \Lambda = \{\Lambda_1, ..., \Lambda_k\}, \quad k = 1, 2, ..., N.$$

Використані на будь-якому з кроків ЗЗ U_k впливають на можливі порушення безпеки $\Lambda_{k+1}, \Lambda_{k+2}, ...$ на наступних кроках, а отже і стан захищеності АСУ ТП $X(t)$. У загальному вигляді рішення про застосування ЗЗ U_k впливають на значення Λ_k на подальших кроках та повинні бути керованими [15].

Прийняття управлінських рішень про застосування необхідних ЗЗ U_k здійснюється на основі отриманих даних спостережень до k-ого кроку включно. У такому випадку правило прийняття рішення про застосування ЗЗ можна представити у вигляді ймовірнісної міри, яка залежить від стану захищеності системи та сукупності попередніх управлінських рішень щодо застосування ЗЗ до k-ого кроку включно:

$$p_k = p_k(U_k \mid X_k, U_{k-1}).$$

Для багатокрокової процедури знаходження оптимальної послідовності прийняття рішення щодо застосування ЗЗ може бути проведено методами динамічного програмування в загальній стохастичній формі. При цьому усереднена величина ризику виникнення порушень може бути визначена як:

$$R(t) = M\{g(U, \Lambda_k, X_k)\},$$

де $M\{\ \}$ – математичне очікування;

$g(U_k, \Lambda_k, X_k)$ – функція зміни стану захищеності.

Мінімальний середній ризик для оптимального правила прийняття рішення на k-ому кроці буде визначатися як:

$$R(A) = \min_{U_1, ..., U_k} M\{g(U, \Lambda_k, X_k)\} = \min_{U_1, ..., U_{k-1}} (\min_{U_k} M\{M\{g(U, \Lambda_k, X_k) \mid X_k, U\}\}),$$

де умовне математичне очікування представляє функцію апостеріорного ризику для сукупності рішень та даних спостережень:

$$R_k(U, X_k) = M\{g(U, \Lambda_k, X_k) \mid X_k, U\}.$$

У цьому випадку математичне очікування функції зміни стану захищеності визначається як:

$$M\{g(U, \Lambda_k, X_k)\} = M\{R_k(U, X_k)\} = M\{M\{R_k(U, X_k) \mid X_k, U_{k-1}, ..., U_1\}\}.$$

Звідки випливає, що

$$\min_{U_k} M\{M\{g(U, \Lambda_k, X_k) \mid X_k, U\}\} = M\{\min_{U_k} R_k(U, X_k)\}.$$

Таким чином, оптимальне Баєсове правило прийняття рішень на k-ому кроці визначає оптимальну послідовність застосування засобів протидії порушенням шляхом прийняття управлінських рішень та визначається як:

$$\min_{U_k} R_k(U, X_k) = \min_{U_k} M\{g(U_k, \Lambda_k, X_k)) \mid X_k, U_k\}.$$

Розглянутий метод управління станом захищеності від кібератак на АСУ ТП ОКІ, дозволяє приймати управлінські рішення щодо застосування ЗЗ для підвищення рівня стану захищеності інформаційних ресурсів, що циркулюють в системі, при множині вхідних параметрів кібератак на основі динамічного програмування.

Висновки. Оскільки сучасні автоматизовані системи управління технологічним процесом відрізняються від звичайних корпоративних мереж, перевірені та популярні технології кіберзахисту для них виявляються не такими ефективними та потребують комплексного рішення. У роботі з метою визначення правила прийняття рішень щодо виявлення кіберінцидентів та вибору засобів захисту на АСУ ТП ОКІ в умовах розвитку Індустрії 4.0 від впливу кібератак запропоновано використання оптимального Баєсового правила прийняття рішень. Використання запропонованого правила дозволяє на будь-якому k-ому кроці, на основі дослідження зміни параметрів системи, здійснити виявлення кіберінциденту та прийняти необхідні управлінські рішення щодо застосування конкретних засобів захисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] О. М. Суходоля “Захист критичної інфраструктури в умовах гібридної війни: проблеми та пріоритети державної політики України”, *Стратегічні пріоритети,* № 3, с. 62-76, 2016. [Електронний ресурс]. Доступно: http://nbuv.gov.ua/UJRN/ spa_2016_3_10. Дата звернення: Груд. 15, 2021.

[2] О. В. Потій, та А. В. Лєншин, “Дослідження методів оцінки ризиків безпеці інформації та розробка пропозицій з їх вдосконалення на основі системного підходу”, *Збірник наукових праць Харківського університету Повітряних Сил*, вип. 2 (24). с. 85-91, 2010.

[3] ICS vulnerability discoveries soar by 110% in four years. [Online]. Avaliable: https://drivesncontrols.com/news/fullstory.php/aid/6971/ICS_vulnerability_discoveries_soar_by_110_25_in_four_years.html. Accessed on: Oct. 17, 2021.

[4] Д. Дубов, “Кіберфронт. Як РФ атакує Україну та чи готові ми захищатися”. [Електронний ресурс]. Доступно: https://biz.nv.ua/ukr/experts/kiberataki-rosiji-na-ukrajinu-yak-prohodyat-ta-chim-zagrozhuyut-ostanni-novini-50236927.html. Дата звернення: Січ. 17, 2022.

[5] A. Djenna, S. Harous, and D. E. Saidouni, “Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure”, *Applied Scienses*, no. 11, 4580. pp. 1-30, 2021. [Online]. Avaliable: https://www.researchgate.net/publication/351652228_Internet_of_Things_Meet_Internet_of_Threats_New_Concern_Cyber_Security_Issues_of_Critical_Cyber_Infrastructure. Accessed on: Dec. 22, 2021.

[6] K. Kobara, “Cyber Physical Security for Industrial Control Systems and IoT” *790 IEICE TRANS. INF. & SYST.*, vol. E99–D, no. 4 pp. 787-795, April 2016. [Online]. Avaliable: https://www.researchgate.net/publication/299542268_Cyber_Physical_Security_ for_Industrial_Control_Systems_and_IoT. Accessed on: Nov. 22, 2021.

[7] Ionut Arghire Critical Vulnerabilities Found in Sealevel Device Used in ICS Environments. [Online]. Avaliable: https://www.securityweek.com/critical-vulnerabilities-found-sealevel-device-used-ics-environments. Accessed on: Jan. 12, 2022.

[8] При APT-атаках BlackEnergy на Украине применялся целевой фишинг с Word-документами, *Kaspersky Lab's Global Research & Analysis Team*. [Электронный ресурс]. Доступно: https://securelist.ru/blog/issledovaniya/27903/pri-apt-atakax-blackenergy-vukraine-primenyalsya-celevoj-fishings-ispolzovaniem-worddokumentov. Дата обращения: Февр. 01, 2022.

[9] Zero Days. The Internet Movie Database. [Online]. Avaliable: http://www.imdb.com/title/tt5446858. Accessed on: Jan. 9, 2022.

[10] А. Панасенко, "Хакеры нечаянно атаковали водоочистные сооружения", *Anti-Malware*, [Электронный ресурс]. Доступно: https://www.anti-malware.ru/news/2016-03-24/18450. Дата обращения: Янв. 27, 2022.

[11] T. Spring, "Зловред, заточенный под АСУ ТП, украл идеи у Stuxnet. Threatpost". [Электронный ресурс]. Доступно: https://threatpost.ru/irongate-ics-malware-steals-from-stuxnet-playbook/16544. Дата обращения: Февр. 02, 2022.

[12] Базові рекомендації з кібербезпеки промислових систем управління для відділів АСУ ТП (серпень 2017), *ТК 185 "Промислова автоматизація". Група "кібер-безпека в АСУ ТП"*.

[13] А. С. Римша, та К. С. Римша, "Анализ средств обеспечения информационной безопасности АСУ ТП газодобывающих предприятий", *CASPIAN JOURNAL: Control and High Technologies*, № 3 (47), с. 102-121, 2019.

[14] А. С. Сторчак, та С. В. Сальник, "Метод оцінювання рівня захищеності мережевої частини комунікаційної системи спеціального призначення від кіберзагроз", *Системи обробки інформації*, № 3 (158), с. 98-109, 2019, doi: https://doi.org/10.30748/soi.2019.158.12.

[15] А. С. Сторчак, "Метод оцінки захищеності інформації на основі багатокрокових процесів прийняття рішень", *Східно-Європейский журнал передових технологій. Фізико-технологічні проблеми радіотехнічних пристроїв, засобів телекомунікацій, нано- і мікроелектроніки*, № 2 (66), с. 82-85, 2013.

Стаття надійшла до редакції 22.02.2022.

REFERENCE

[1] O. M. Sukhodolia, "Zakhyst krytychnoi infrastruktury v umovakh hibrydnoi viiny: problemy ta priorytety derzhavnoi polityky Ukrainy", *Strategic priorities,* vol. 3, pp. 62-76, 2016. [Online]. Avaliable: http://nbuv.gov.ua/UJRN/spa_2016_3_10. Accessed on: Jan. 15, 2022.

[2] O. V. Potii, A. V. Lienshyn, "Doslidzhennia metodiv otsinky ryzykiv bezpetsi informatsii ta rozrobka propozytsii z yikh vdoskonalennia na osnovi systemnoho pidkhodu", *Collection of scientific works of Kharkiv University of Air Sy*, vol. 2 (24), pp. 85-91, 2010.

[3] ICS vulnerability discoveries soar by 110% in four years. [Online]. Avaliable: https://drivesncontrols.com/news/fullstory.php/aid/6971/ICS_vulnerability_discoveries_soar_by_110_25_in_four_years.html. Accessed on: Oct. 17, 2021.

[4] D. Dubov, "Kiberfront. Yak RF atakuie Ukrainu ta chy hotovi my zakhyshchatysia". [Online]. Avaliable: https://biz.nv.ua/ukr/experts/kiberataki-rosiji-na-ukrajinu-yak-prohodyat-ta-chim-zagrozhuyut-ostanni-novini-50236927.html. Accessed on: Jan. 17, 2022.

[5] A. Djenna, S. Harous, and D. E. Saidouni, "Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure", *Applied Scienses*, no. 11, 4580. pp. 1-30, 2021. [Online]. Avaliable: https://www.researchgate.net/publication/351652228_Internet_of_Things_Meet_Internet_of_Threats_New_Concern_Cyber_Security_Issues_of_Critical_Cyber_Infrastructure. Accessed on: Dec. 22, 2021.

[6] K. Kobara, "Cyber Physical Security for Industrial Control Systems and IoT" *790 IEICE TRANS. INF. & SYST.*, vol. E99–D, no. 4 pp. 787-795, April 2016. [Online]. Avaliable:

https://www.researchgate.net/publication/299542268_Cyber_Physical_Security_for_Industrial_Control_Systems_and_IoT. Accessed on: Nov. 22, 2021.
[7] Ionut Arghire Critical Vulnerabilities Found in Sealevel Device Used in ICS Environments. [Online]. Avaliable: https://www.securityweek.com/critical-vulnerabilities-found-sealevel-device-used-ics-environments. Accessed on: Jan. 12, 2022.
[8] Pry APT-atakakh BlackEnergy na Ukrayne prymenialsia tselevoi fyshynh s Word-dokumentamy, *Kaspersky Lab's Global Research & Analysis Team*. [Online]. Avaliable: https://securelist.ru/blog/issledovaniya/27903/pri-apt-atakax-blackenergy-v‑ukraine-primenyalsya-celevoj-fishings-ispolzovaniem-worddokumentov Accessed on: Febr. 01, 2022.
[9] Zero Days. The Internet Movie Database. [Online]. Avaliable: http://www.imdb.com/title/tt5446858. Accessed on: Jan. 9, 2022.
[10] A. Panasenko, "Khakery nechaianno atakovaly vodoochystnye sooruzhenyia", *Anti-Malware*. [Online]. Avaliable: https://www.anti-malware.ru/news/2016-03-24/18450. Accessed on: Jan. 27, 2022.
[11] T. Spring, "Zlovred, zatochenyi pod ASU TP, ukral idei u Stuxnet. Threatpost". [Online]. Avaliable: https://threatpost.ru/irongate-ics-malware-steals-from-stuxnet-playbook/16544. Accessed on: Febr. 02, 2022.
[12] Bazovi rekomendatsii z kiberbezpeky promyslovykh system upravlinnia dlia viddiliv ASU TP (August 2017), *TK 185 "Promyslova avtomatyzatsiia". Hrupa "kiber-bezpeka v ASU TP"*.
[13] A. S. Rymsha, and K. S. Rymsha, "Analyz sredstv obespechenyia ynformatsyonnoi bezopasnosty ASU TP hazodobuvaiushchykh predpryiatyi", *CASPIAN JOURNAL: Control and High Technologies*, no. 3 (47), pp. 102-121, 2019.
[14] A. S. Storchak, and S. V. Salnyk, "Metod otsiniuvannia rivnia zakhyshchenosti merezhevoi chastyny komunikatsiinoi systemy spetsialnoho pryznachennia vid kiberzahroz", *Information processing systems*, no. 3 (158), pp. 98-109, 2019. doi: https://doi.org/10.30748/soi.2019.158.12.
[15] A. S. Storchak, "Metod otsinky zakhyshchenosti informatsii na osnovi bahatokrokovykh protsesiv pryiniattia rishen", *Skhidno-Yevropeiskyi zhurnal peredovykh tekhnolohii. Fizyko-tekhnolohichni problemy radiotekhnichnykh prystroiv, zasobiv telekomunikatsii, nano- i mikroelektronik*, no. 2 (66), pp. 82-85, 2013.

SERHII VASYLENKO,
IHOR SAMOILOV,
SERHII BURIAN

METHOD OF CONTROL OF THE STATE OF PROTECTION OF THE AUTOMATED PROCESS CONTROL SYSTEM OF THE CRITICAL INFRASTRUCTURE FACILITY

Constant dynamic processes of society informatization drastically change all spheres of its life, giving them new impulses and opportunities for implementation in the new conditions. At the same time, these processes are the cause of fundamentally new challenges for the security sector, which cause the deep penetration of information technology into all elements of infrastructure, including critical ones. Cyberattacks on critical information infrastructure facility of critical infrastructure facility (CIIF CIF) are particularly dangerous. Much of the CIIF CIF cyberthreats are related to the massive implementation of Industry 4.0 (I 4.0) technologies such as digital ecosystems, the Industrial Internet of Things (IIoT), big data analytics, the use of digital platforms, etc. The risks associated with these require new solutions in the management of the CIIF CIF conservation status. In the work as CIIF CIF considered the automated process control system (APCS) CIF built with IIoT-sensors usage. The peculiarities of building such systems and the need for rapid response to any cyberincidents require automation of the management of decision-making process for the application of the necessary protection means. For the state of protection against cyberattacks on APCS CIF it is

proposed to use the method of making management decisions based on a dynamic programming, depending on the type of cyberattack control, selection and application of appropriate means of protection and to reduce the consequences of cyberincidents.

Keywords: critical infrastructure facility, automated process control system, industrial Internet of things, security management, dynamic programming.

Василенко Сергій Вікторович, кандидат технічних наук, начальник науково-дослідної лабораторії Науково-дослідного центру, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0001-6779-8246, vasylenko.phd@gmail.com.

Самойлов Ігор Володимирович, кандидат технічних наук, доцент, доцент кафедри безпеки державних інформаційних ресурсів, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0002-8251-9257, samoilov1966igor@gmail.com.

Бур'ян Сергій Костянтинович, старший викладач кафедри безпеки державних інформаційних ресурсів, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна, ORCID 0000-0001-7383-571X, burianserg15@gmail.com.

Vasylenko Serhii, candidate of technical sciences, head at the research laboratory of the scientific and research center, Institute of special communications and information protection of National technical university of Ukraine "Igor Sikorsky Kiev Polytechnic Institute", Kyiv, Ukraine.

Samoilov Igor, candidate of technical sciences, associate professor, associate professor at the state information resources security academic department, Institute of special communications and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.

Burian Serhii, senior lecturer at the state information resources security academic department, Institute of special communications and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.