УДК 004.056.52

Петро ПІДЛИСЬКИЙ, Марія ЛИСИК

Західноукраїнський національний університет

МОДЕЛЬ ФУНКЦІОНАЛЬНОЇ СТІЙКОСТІ ЦЕНТРУ ІНТЕЛЕКТУАЛЬНОГО УПРАВЛІННЯ МЕРЕЖЕВОЮ БЕЗПЕКОЮ

Вступ. Від центру інтелектуального управління мережевою безпекою (ЦІУМБ) потрібна не просто його стійкість як системи, а стійкість, яка визначається як у штатному режимі, так і в умовах загроз інформаційній безпеці (ІБ) (в умовах спрямованих на нього комп'ютерних атак, при збоях підвищеного ступеня серйозності та в умовах надзвичайних ситуацій) [1].

Тобто це є здатність ЦІУМБ регулювати своє функціонування в єдиному інформаційному просторі з метою підтримки виконання його бізнес-процесів за очікуваних вимог і в умовах посилення цих вимог, порушень та інцидентів, загроз ІБ та непередбачених обставин. Це активна форма стійкості для динамічної системи і побудова її моделі є актуальною задачею.

Мета: розробити модель функціональної стійкості ЦІУМБ.

1. Модель функціональної стійкості ЦІУМБ

Забезпечення функціональної стійкості типового ЦІУМБ має підтримуватись збереженням безперервності його бізнес-процесів та їх частин у вигляді окремих бізнес-процесів операцій та доступності ІТ-послуг та ресурсів користувачам навіть в умовах передбачуваної заздалегідь деградації інфраструктури та функціональних процесів, у тому числі при впливі різних дестабілізуючих впливів та відмов усередині самого ЦІУМБ. Його функціональну стійкість можна розглядати як таку його здатність, при якій рівень ризику порушення функціонування та доступності ІТ-послуг і ресурсів передбачувані і прийнятні як для їх користувача, так і для власника. Причому ця здатність має бути спочатку вбудована в проект типового ЦІУМБ, а всі порушення та інциденти ІБ мають бути контрольованими.

Функціональна стійкість типового ЦІУМБ після припинення дії деструкції має проявлятися у двох режимах:

1) у малому, коли з часом досить мале відхилення режиму роботи від вихідного (установленого) зменшується і функціонування ЦІУМБ повертається у вихідний стан;

2) у великому, коли після припинення дії збурення при досить великому початковому відхиленні функціонування ЦІУМБ повертається у вихідний стан.

Управління функціональною стійкістю типового ЦІУМБ має враховувати, що для досягнення поставленої мети його функціонування під час та після впливу інциденту ІБ може знадобитися зміна значень параметрів, що стосуються всіх його бізнес-процесів (на відміну від окремого випадку управління - регулювання, яке полягає лише у підтримці певних параметрів системи у заданих межах).

В загальному випадку управління функціональною стійкістю (її модель представлена на рисунку 1) типового ЦІУМБ базується на управлінні ІТ-операціями та наданні ІТ-послуг, управлінні безперервністю функціонування,

управлінні власною ІБ ЦІУМБ та інших складових цього процесу, наприклад, управлінні фінансами, персоналом, комунікаціями та обізнаністю.

Рисунок 1 - Модель управління функціональною стійкістю типового ЦІУМБ

Управління ІТ-операціями, безперервністю функціонування та ІБ - це доповнюючі і взаємодіючі між собою процеси, орієнтовані на управління операційними ризиками ЦІУМБ, які мають одну спільну мету - покращувати та підтримувати функціональну стійкість типового ЦІУМБ. При цьому ризик порушення функціонування ЦІУМБ або операційний ризик (англ. operational risk), це ризик збитку установи внаслідок неадекватних чи помилкових внутрішніх процесів ЦІУМБ, дій його робітників та систем або зовнішніх подій.

Отже, значна частина операційних ризиків типового ЦІУМБ, включаючи ризик переривання його діяльності, пов'язана з інформацією, а рівень та умови прояву цих ризиків багато в чому визначаються якістю ІТ-послуг (з підготовки, обробки, передачі, зберігання та відображення інформації).

Безперервність функціонування ЦІУМБ - це його стратегічна та тактична здатність планувати свою роботу у випадку інцидентів ІБ та порушень його функціонування, спрямована на забезпечення безперервності бізнес-процесів на встановленому прийнятному рівні. Тоді можна вважати, що забезпечення безперервності функціонування ЦІУМБ буде забезпеченням такої стратегічної та тактичної здатності цієї системи, що передбачає довгострокове існування ЦІУМБ. У свою чергу, управління безперервністю функціонування ЦІУМБ є цілісним системним процесом, що передбачає ідентифікацію потенціальних порушень та інцидентів ІБ та їх впливу на функціонування ЦІУМБ для прийняття обґрунтованих рішень щодо збереження його бізнес-процесів. Такий вид управління створює основу для підвищення функціональної стійкості центру і направлений на реалізацію таких типових заходів у відповідь проти інцидентів ІБ, які забезпечують захист функціонування ЦІУМБ. Тоді безперервність функціонування типового ЦІУМБ також можна визначити як здатність ЦІУМБ зберігати надійність його ресурсів, що забезпечують безперервність бізнес-процесів та доступність ІТ-послуг і самої інформації користувачам.

З рисунка 1 видно, що ефективність та результативність управління функціональною стійкістю типового ЦІУМБ безпосередньо залежить від процесів управління безперервністю його функціонування та управління ІБ. На рисунку 1 ці два процеси показані як незалежні, хоча насправді вони можуть перетинатися, оскільки деякі загрози та ризики управління неперервністю функціонування та

управління ІБ можуть бути одними і тими ж. На основі проведеного аналізу однакових ризиків можуть бути вироблені схожі вимоги щодо забезпечення безперервності функціонування та ІБ, а надалі обрані однакові процеси та заходи забезпечення ІБ для подібних ризиків.

Загалом процес управління безперервністю функціонування типового ЦІУМБ можна розділити на два генеральні напрями його реалізації:

1) забезпечення функціональної стійкості ЦІУМБ та його бізнес-процесів, в результаті чого відбувається зниження ймовірності настання ризикових подій (інцидентів, порушень, відмов тощо) на основі розробки та впровадження превентивних антикризових заходів;

2) відновлення (продовження) функціонування ЦІУМБ, включаючи бізнес-процеси, окремі операції та ресурси, після ризикових подій з наступною мінімізацією та коригуванням їх негативного впливу, якщо вони вже сталися.

Наочно процес відновлення функціональної стійкості ЦІУМБ після інциденту ІБ представлено на рисунку 2. Важливо зауважити, що після інциденту ІБ не завжди відразу відбувається різке припинення здійснення бізнес-процесів (як на рисунку 2), оскільки він може породжувати як прямі, так і непрямі збитки.

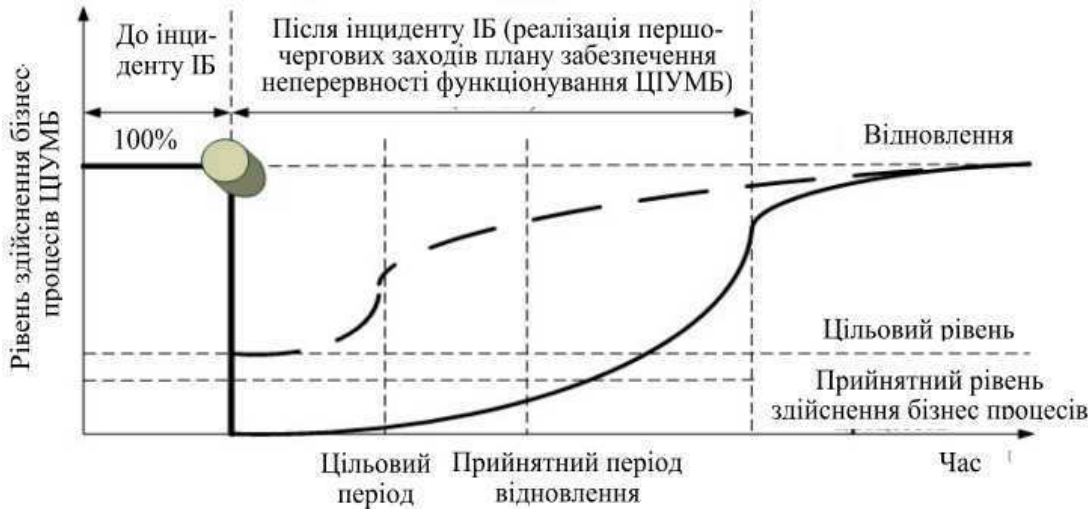

Рисунок 2 - Процес відновлення функціональної стійкості типового ЦІУМБ після інциденту ІБ

Найпростішими заходами забезпечення функціональної стійкості типового ЦІУМБ є розробка плану забезпечення безперервності функціонування, застосування генераторів для резервного живлення, використання більш довговічних будівельних матеріалів тощо.

Висновок. Розроблено модель функціональної стійкості ЦІУМБ.

Перелік використаних джерел.

1. Reviews for Security Threat Intelligence Products and Services Market: Веб-сайт / GARTNER. - Gartner, 2020. [Електронний ресурс] - Режим доступу: https://www.gartner.com/ reviews/market/securitythreat-intelligence-services#:~:text=%22Threat%20intelligence%22%20(TI),to%20that%20menace%20or%20hazard.