Restoration procedure as a mechanism for Information Security System Survivability Providing

Yuriy Garasym

Information Security Department,
Lviv Polytechnic National University,
UKRAINE, Lviv, 12, S. Bandery Street,
E-mail: garasym_yr@polynet.lviv.ua

The work is devoted to research aspects of the creation and use of special tools and subsystems to ensure survivability of information security systems (ISS). The main results will help professionals in the field of information security to apply the systems in ISS with the introduction in its structure of minimum redundancy. This, in its turn, will cause minimal reduction of the protection effectivity (for example, its quick-action).

The functioning recovery under conditions of uncertainty of influence of destabilizing factors (DF) - one of the most difficult for realization functions of ISS in ECN (enterprise communication networks), because when operating we can face unpredictable situations, and in the existing ISS in ECN the ability of software and hardware for detection, diagnosis, fault isolation, creation of operable structures, is limited.

Subsystems providing survival ISSa are maximum effective in unpredictable situations that are associated with loss of system hardware, power, performance, ISS productivity as a result of structural elements failures. E This contradiction can be partly eliminated as a result of the rational organization of the system processes of ISS on the means contained in the systems, in those time intervals when ISS part is not loaded with the main tasks.

Analysis of survivability properties leads to the need for using of reconfiguration mechanisms, ensuring of the gradual degradation, redistribution ISS resources in enterprise communication networks (ECN).

The work outlines methods of fault tolerance providing as a necessary subset of methods to ensure survivability, describes the nature restoration procedures for information security systems, which have survivability property, shows features of methods and mechanisms to increase survivability of information security systems for ECN.

Key words – information security systems, enterprise communication networks, survivability property, survivability providing, restoration procedure.

Переклад виконано Малиновською О. А., центр іноземних мов «Universal Talk», www.utalk.com.ua

Процедура відновлення як механізм забезпечення живучості систем захисту інформації

Юрій Гарасим

Кафедра захисту інформації,
Національний університет "Львівська політехніка",
УКРАЇНА, м.Львів, вул.С.Бандери, 12,
E-mail: garasym_yr@polynet.lviv.ua

В роботі окреслено методи забезпечення відмовостійкості як необхідної підмножини методів забезпечення живучості, описано характер процедур відновлення для систем захисту інформації, які мають властивість живучості, показано особливості застосування методів і механізмів підвищення живучості систем захисту інформації для корпоративних мереж зв'язку.

Ключові слова – системи захисту інформації, корпоративні мережі зв'язку, властивість живучості, забезпечення живучості, процедура відновлення.

I. Вступ

При створенні та використанні спеціальних механізмів і підсистем забезпечення живучості основна складність полягає в тому, що при включенні їх у системи захисту інформації (СЗІ) повинна вноситися мінімальна надлишковість, а функціонування їх повинно мінімально знижувати ефективність системи (наприклад, її швидкодію). Ці засоби повинні бути максимально ефективними в непередбачуваних ситуаціях, які пов'язані із втратою частини системного обладнання, потужності, продуктивності СЗІ внаслідок відмов її структурних елементів (СЕ). Ліквідувати це протиріччя частково вдається в результаті раціональної організації системних процесів СЗІ на тих засобах, які містяться в системах, в ті часові інтервали, коли частина СЗІ не завантажена основними завданнями [1].

Для організації функціонування СЗІ за умов відмов її СЕ [2] необхідно передбачити: контроль за станом ресурсів; діагностику відмов; механізм локалізації СЕ, які відмовили і їх ізоляції; перерозподіл ресурсів; інформаційну підсистему, що містить дані про ресурси і їх функціональні можливості, поточний розподіл, систему пріоритетів функцій тощо; процедури відновлення як набір механізмів відновлення функціонування та підготовки необхідної інформації відповідно до прийнятої стратегії відновлення; періодичне (в процесі нормального функціонування) збереження поточного стану [1].

В ідеальному випадку повинна існувати підсистема, яка здатна миттєво оцінити завдані збитки, прийняти рішення про нову структуру непошкодженої частини СЗІ, оновити інформацію (програми і дані) і вибрати новий рівень функціонування [3] (з попередньою або зниженою продуктивністю), відповідний тип цілі функціонування.

Усі механізми, що забезпечують функціонування СЗІ, наприклад, в корпоративних мережах зв'язку (КМЗ) закладаються на етапі проектування. У міру переходу до автоматизованого проектування, до самопроектування СЗІ на фоні подальшого вдосконалення КМЗ природним є розвиток цих механізмів і поява нових. Так, вимоги забезпечення надійності зумовили застосування розвинених механізмів дублювання та мажорирування, вимоги до відмовостійкості вимагали подальшого розроблення механізмів маскування помилок і відмов СЕ. Аналіз властивості живучості призводить до необхідності використання механізмів реконфігурування, забезпечення поступової деградації, перерозподілу ресурсів СЗІ в КМЗ [1].

II. Процедури відновлення систем захисту інформації

Відновлення функціонування за умов невизначеності впливу дестабілізуючих факторів (ДФ) – одна із найскладніших для реалізації функцій СЗІ в КМЗ, тому що при експлуатації можуть виникнути непередбачувані ситуації, а в існуючих СЗІ в КМЗ обмежена здатність програмних і апаратних засобів для виявлення, діагностики, локалізації несправностей, до створення роботоздатних структур [4].

Процедури відновлення розрізняють або щодо визначеного класу несправностей, або виходячи з методу забезпечення роботоздатного стану СЗІ після виникнення в ній відмови. Так, в [1] наведено декілька означень поняття відновлення: відновлення визначається як сукупність дій, які здійснюються системою після отримання сигналу про несправності або ж відновлення – це реконфігурування структури системи за відмов СЕ з метою перерозподілу завдань, які виконує система між работоздатними СЕ, або під відновленням мається на увазі заміна СЕ, що відмовив, його ремонт.

Розрізняють відновлення після трьох видів несправностей (помилок): фізичних; помилок програмного забезпечення; при управлінні обчислювальним процесом. Відповідно виділяють три принципово різних рівні відновлення: апаратний (фізичний), програмний та рівень управління. Процедури відновлення різних рівнів відрізняються, проте, обов'язковою є наявність таких етапів для процедур усіх рівнів: виявлення несправностей (діагностика); встановлення тимчасової затримки; відновлення роботоздатності.

В основі побудови процедур відновлення лежать такі принципи [1].

Принцип ядра, який розширюється. Суть цього принципу полягає у встановленні єдиного порядку відновлення системи захисту, що починається завжди з деякого ядра, відмовостійкість якого забезпечується статичним ресурсом. Оператори, що виконуються цим ядром, складають програмне ядро. Далі за допомогою ядра розширюється работоздатна частина СЗІ, а потім вже розширеним ядром відновлюються наступні засоби системи, які забезпечують подальше розширення ядра. Процес триває до найповнішого розширення системи.

Принцип поєднання централізованого та децентралізованого управління процесами відновлення у системі. Централізоване управління полегшує створення програмного забезпечення, але суттєво підвищує вимоги до надійності централізованого ядра, збільшує обсяги діагностичної та керуючої інформації, що циркулює по лініях зв'язку між СЕ. Децентралізоване управління знижує вимоги до надійності СЕ, які виконують функції ядра СЗІ, але суттєво ускладнює програмне забезпечення системи. Для кожної конкретної системи існує оптимальний рівень децентралізації управління, що мінімізує надлишковий ресурс СЗІ.

Принцип оптимального поєднання самовідновлення СЕ системи з відновленням, що використовують системні засоби. Підвищення рівня самовідновлення модулів дозволяє економніше витрачати резервний ресурс внаслідок гнучкішого виконання окремих СЕ СЗІ, але разом з тим збільшуються витрати на засоби діагностики. Існує оптимальний рівень самовідновлення СЕ, який визначається технологією їх виготовлення і структурою.

Залежно від стану СЗІ в КМЗ після відновлення розрізняють повне, часткове відновлення і безпечну зупинку. До функцій процедур відновлення відносимо: ідентифікацію і локалізацію несправностей; виправлення помилок у програмах і даних; перерозподіл ресурсів між процесами; заміну і вилучення несправних СЕ, ремонт, реєстрацію спостережень і прийнятих дій; відновлення роботи або завершення послідовності операцій зупинки.

Принциповою ознакою, за якою розрізняють алгоритми відновлення є наявність або відсутність людини-оператора як складової частини процедури відновлення.

Прийняття рішення про вибір процедури відновлення суттєво залежить від етапу, на якому перебуває розроблення СЗІ в КМЗ і декількох кількісних вимог до процесу відновлення. Апаратно-кероване відновлення є більш швидким, але вимагає введення в СЗІ спеціальних апаратних засобів, які повинні розроблятися на початковому етапі створення самої СЗІ в КМЗ. Програмно-кероване відновлення не вимагає змін в апаратурі, його можна «встановити» на наявні засоби, але це суттєво повільніший процес.

Процес відновлення на рівні управління передбачає взаємодію багатьох системних ресурсів і процесів, тому його слід розглядати як глобальну системну проблему. Головною вимогою до процедур цього рівня є мінімальне втручання в хід виконання прикладних процесів. На цьому рівні розрізняють два підходи до організації відновлення: припинення процесів (завдань) і перерозподіл ресурсів.

В основі вибору тієї чи іншої процедури відновлення, як правило, лежить моделювання станів системи. Серед моделей, які використовуються при розробленні процедур відновлення виділимо структурні, спеціалізовані моделі несправностей та імітаційні моделі. Перші використовують на ранніх етапах розроблення СЗІ в КМЗ. Їх параметрами є структурні елементи СЗІ в КМЗ, апаратні засоби. Параметри

якості, які досліджуються – продуктивність системи, готовність СЗІ в КМЗ, надійність, вартість. Метою використання цих моделей є отримання рекомендацій щодо архітектурних рішень [1].

Спеціалізовані моделі несправностей використовуються на етапі розроблення програмного забезпечення та випробувань СЗІ в КМЗ. Критерієм цінності цих моделей є прогнозуюча здатність, тобто модель є тим кращою, чим більше несправностей (помилок) з її допомогою вдається передбачити. Як параметри цих моделей виступають статистичні дані роботи апаратури, програмного забезпечення, специфікації вхідних даних і програм тощо. Параметри якості, які досліджуються – ймовірність появи несправностей, помилок, непередбачуваних ситуацій тощо. Мета моделювання – виявлення «найслабших» ділянок апаратної і програмної частин, отримання рекомендацій щодо використання захисного резервування, різних типів надлишковості, тієї чи іншої стратегії відновлення.

Імітаційні моделі [5] застосовують на етапі випробувань та експлуатації СЗІ в КМЗ. Параметрами цих моделей є параметри якості функціонування системи, характеристики стану системи тощо. Параметрами дослідження можуть бути надійність СЗІ в КМЗ, її відмовостійкість, живучість, відновлюваність тощо. Основна мета моделювання – виявлення слабких ланок в управлінні (етап випробувань) та організація процедур відновлення в процесі функціонування.

Процес відновлення характеризується такими кількісними показниками, як час відновлення $t_в$ і обсяг ресурсів СЗІ в КМЗ на реалізацію процедур відновлення v_p. Природним є прагнення мінімізувати обидва показники, проте, це досягається досить рідко.

На цей час не можна говорити про якийсь універсальний метод відновлення, хоча розроблено досить загальні способи. Так, для відновлення інформації використовуються резервування всієї інформації (або найважливішої її частини), коригування інформації за допомогою програм відновлення і відповідних вихідних даних (розроблені алгоритми, що дозволяють відтворити будь-який стан N-коректуючої структури даних, якщо вона перетворювалася не більше ніж N разів). Ці алгоритми вимагають і відповідної організації структури даних. Прикладом однокоректуючої структури даних може бути двозв'язний список. Широко розповсюдженим і досить простим методом відновлення є відновлення з поверненням.

Безсумнівно, цікавим, але ще недостатньо розробленим є метод відновлення з випередженням, що припускає можливість переходу в новий безпомилковий стан, який будується з частин (не зачеплених помилкою) поточного помилкового стану системи. Проте, зрозуміло, що алгоритми, які розробляються в рамках цього методу, мають приватний характер і застосовуються лише в системі, для якої вони і розроблялися [1].

На цей час в деяких системах програмного забезпечення використовують метод блоків відновлення, який використовує здатність програмного забезпечення (ПЗ) до реконфігурування. Метод блоків відновлення з'єднує три засоби: програми виявлення помилок, відновлення з поверненням і диверсійний метод відновлення. Цей метод розвинений до технології програмування.

При реконфігуруванні ПЗ мультипрограмних систем серйозною проблемою є структура міжпроцесних зв'язків. Наприклад, помилка, яка виявлена в деякому процесі і цей процес повернувся до останньої точки відновлення. Всі обміни інформацією між цим процесом та іншими, які відбулися в інтервалі між точкою відновлення і моментом виявлення помилки, повинні бути скасовані, а це вимагає повернення до точок відновлення інших процесів. Може виникнути лавиноподібний руйнівний процес повернень, що отримав назву ефекту доміно. Основною причиною цього є відсутність координації між точками відновлення різних процесів. Тому, при відновленні в мультипрограмних СЗІ в КМЗ доцільно використовувати альтернативні версії програм, що базуються на альтернативній структурі зв'язків.

При реалізації будь-якого з описаних методів в конкретній системі буде необхідним рішення цілого ряду серйозних завдань, як правило, приватного характеру, які пов'язані з конкретною метою функціонування конкретної СЗІ в КМЗ.

III. Системи захисту інформації, які відновлюються

Аналізуючи живучість та надійність, особливо при виборі показників живучості та надійності СЗІ, суттєве значення має рішення, яке повинно бути прийнято за умови відмови СЕ СЗІ в КМЗ. Під відновленням СЗІ розумітимемо не лише ремонт тієї чи іншої її частини, але в деяких випадках і повна її заміна або заміна її СЕ. Для користувача, який зацікавлений у виконанні заданих функцій, зовсім неважливо, відновлюється роботоздатність безпосередньо ремонтом об'єкта або заміною його на зовсім інший роботоздатний.

Для показників живучості і надійності можливими є дві форми подання: ймовірнісна і статистична. Ймовірнісна форма зазвичай буває зручнішою при апріорних аналітичних розрахунках живучості і надійності, статистична – при експериментальному дослідженні живучості і надійності СЗІ в КМЗ. Крім цього, виявляється, що одні показники краще інтерпретуються в ймовірнісних термінах, а інші – в статистичних.

Процес експлуатації СЗІ з відновленням представимо послідовністю інтервалів роботоздатності x_i, які чергуються з інтервалами простою h_i, тобто $x_1, h_1, x_2, h_2 \ldots$. Математичною моделлю процесу експлуатації об'єкта може бути відповідний випадковий процес.

Для СЗІ з відновленням характерний специфічний вид випадкового процесу, що описує функціонування її під час експлуатації. Основна особливість цього випадкового процесу полягає в тому, що в загальному випадку розподілу $F_1(t), F_2(t)...$, що відповідають випадковим величинам $x_1, x_2...$ можуть бути відмінні один від одного. Це пояснюється тим, що в черговий момент початку роботи після відновлення СЗІ характеризується цілком певним початковим станом. Далі розглядають в основному або характеристики об'єктів до першої відмови, або стаціонарні характеристики. Під стаціонарними характеристиками будемо розуміти характеристики відповідних стаціонарних випадкових процесів. У цьому випадку початкові стани виявляються однаковими у ймовірнісному розумінні, тобто випадкові величини x_k, x_{k+1} і т.д. мають для всіх k однакові розподіли $F_k(t) = F(t)$. Аналогічно і випадкові величини $h_1, h_2, ...$ можуть мати різні розподіли, проте, усюди будемо вважати їх еквівалентними випадковими величинами з розподілом $G(t)$ (через $g(t)$ будемо позначати щільність розподілу $G(t)$, якщо вона існує).

Практично у всіх випадках будемо вважати, що чергуючі величини x_i і h_i взаємно незалежні, а розподіл кожної з них не залежить від номера i, тобто будемо вивчати випадковий процес $\{x, h\}$, який у теорії відновлення носить назву альтернуючого.

Введемо позначення: $g(t)$ – щільність розподілу $G(t)$; $G(t) = P\{h \le t\}$ – розподіл часу відновлення; $h^{(i)}$ – i-та реалізація часу відновлення.

Середній час відновлення СЗІ в КМЗ

Ймовірнісне визначення

$$t = M\{h\} = \int_0^\infty t g(t)dt = \int_0^\infty t dG(t) = \int_0^\infty [1 - G(t)]dt,$$

де t – математичне сподівання (середнє значення) часу відновлення СЗІ в КМЗ.

Статистичне визначення

$$\hat{t} = \frac{1}{N(0)}\left(h^{(1)} + h^{(2)} + ... + h^{[N(0)]}\right) = \frac{1}{N(0)}\sum_{i=1}^{N(0)} h^{(i)},$$

де прийнято $h^{(1)} \le h^{(2)} \le ... \le h^{[N(0)]}$, причому $h^{(0)} = 0$; $\hat{t}$ – середнє арифметичне реалізації часу відновлення.

Інтенсивність відновлення СЗІ в момент часу t, який відраховується від моменту початку відновлення

Ймовірнісне визначення

$$m(t) = \frac{g(t)}{1 - G(t)},$$

де $m(t)$ – умовна щільність ймовірності відновлення СЗІ в момент часу t, який відраховується від моменту початку відновлення за умови, що до моменту часу t відновлення не відбулося.

Статистичне визначення

$$\hat{m}(t) = \frac{n_в(t + \Delta t) - n_в(t)}{N_в(t)\Delta t} = \frac{N_в(t + \Delta t) - N_в(t)}{N_в(t)\Delta t} = \frac{\Delta n_в(t, t + \Delta t)}{N_в(t)\Delta t},$$

де $\hat{m}(t)$ – відношення кількості відновлень в інтервалі часу $[t, t + \Delta t]$ до добутку кількості об'єктів, які ще не відновлені до моменту t, на тривалість інтервалу часу Δt [6].

Висновок

1. Запропоновано статистичне та ймовірнісне визначення середнього часу відновлення СЗІ в КМЗ.
2. Запропоновано статистичне та ймовірнісне визначення інтенсивності відновлення СЗІ в КМЗ в певний момент часу.

Література

[1] Додонов А. Г. Введение в теорию живучести вычеслительных систем / А. Г. Додонов, М. Г. Кузнецова, Е. С. Горбачик. – К. : Наук. думка, 1990. – 184 с.

[2] Дудикевич В. Б. Поведінка системи захисту інформації в умовах впливу дестабілізуючих факторів / В. Б. Дудикевич, Ю. Р. Гарасим // Системний аналіз. Інформатика. Управління (СІАУ-2011): тези доповідей ІІ Всеукраїнської науково-практичної конференції. – Запоріжжя : КПУ, 2011. – С. 76-78.

[3] Гарасим Ю. Р. Аналіз систем захисту, які мають властивість живучості / Ю. Р. Гарасим // Військово-технічний збірник. – № 1 (4). – 2010. – С. 87-95.

[4] Гарасим Ю. Р. Метод вибору варіанту системи захисту інформації за критерієм живучості в умовах невизначеності впливу дестабілізуючих факторів / Ю. Р. Гарасим // Збірник тез міжнародної наукової конференції студентів, аспірантів та молодих вчених «Теоретичні та прикладні аспекти кібернетики». – Київ, 2011. – С. 74-76.

[5] Гарасим Ю. Р. Математичні моделі оцінки живучості систем захисту інформації / Ю. Р. Гарасим // Тези доповіді ІХ Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики». – Київ, 2011. – С. 25-26.

[6] Черкесов Г. Н. Надежность аппаратно-програмных комплексов / Г. Н. Черкесов. – Спб. : Питер, 2005. – 479 с.