УДК 001.4

Ю.Р. Гарасим, В.Б. Дудикевич

Національний університет «Львівська політехніка», Львів

ПОНЯТТЯ ЖИВУЧОСТІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ЗАХИЩЕНИХ КОРПОРАТИВНИХ МЕРЕЖ ЗВ'ЯЗКУ

Впродовж останніх років зростає залежність суспільства від цифрових систем зв'язку (корпоративних мереж) та інформаційних систем (ІС). Оскільки корпоративні мережі зв'язку (КМЗ) все частіше стають розподіленими – зростають вимоги до забезпечення конфіденційності, цілісності, доступності та спостережуваності інформації, яка функціонує в цих мережах. Живучість таких мереж має вирішальне значення.

Живучість сучасних СЗІ захищених КМЗ (ЗКМЗ) є визначальною властивістю з точки зору забезпечення їхньої працездатності під впливом екстремальних (дестабілізуючих) факторів (ДФ) та умов експлуатації. Під живучістю системи розумі-

ється її властивість залишатися працездатною в умовах негативних зовнішніх впливів [1], властивість систем до збереження своїх основних функцій (хоча б із допустимою втратою якості їхнього виконання) при впливі факторів зовнішнього середовища катастрофічного характеру – неблагополучні умови експлуатації [2]. В [3] живучість визначена як властивість об'єкту, що полягає в його спроможності виконувати задане призначення в процесі дестабілізуючих впливів на весь об'єкт або окремі його компоненти, підтримуючи в допустимих межах свої експлуатаційні показники.

Постановка проблеми. Хоча поняття живучості відоме в техніці давно та практично використовується при створенні технічних систем різного призначення, до цього часу не створено розвинутої теорії, яка містила б, як і теорія надійності, загальнотехнічні результати, які дозволяють досліджувати цю властивість, оцінювати її кількісно та розробляти практичні рекомендації проектувальника складних систем (в тому числі й систем захисту інформації) із забезпечення живучості.

На даний момент теорія живучості знаходиться на такій стадії розвитку, коли ще не сформовані основні поняття, не існує єдиного науково обґрунтування того, що таке живучість, яка галузь застосування цього поняття. Практично відсутніми є апробовані довгим практичним використанням моделі живучості. Велика кількість пропонованих понять та показників живучості скоріше вказують про недостатню ясність у вирішенні цього питання, ніж про його пропрацьованість. Немає визначених методичних розробок у питанні, для яких систем необхідно оцінювати, нормувати та забезпечувати живучість.

Постановка завдання. Підсумовуючи усе вищесказане в роботі здійснюється систематизація та аналіз різних точок зору та основні методичні питання теорії живучості, пропонується авторська точка зору щодо поняття живучості системи захисту інформації захищених корпоративних мереж зв'язку з метою виключення неоднозначності трактування живучості СЗІ, основних її елементів для полегшення подальших досліджень якісних, та кількісних її атрибутів.

Поняття живучості системи захисту інформації

В роботі пропонується визначення поняття «живучість системи захисту інформації»:

Живучість системи захисту інформації = властивість системи захисту інформації, яка полягає у здатності зберігати та виконувати встановлений об'єм власних цільових функцій *(забезпечення конфіденційності, цілісності, доступності і спостережуваності інформації, яка в ній функціонує)* ***у відповідному середовищі з врахуванням різних зовнішніх та внутрішніх дестабілізуючих факторів*** *(зокрема, моделі загроз та порушника)****, що можуть призводити до відмов її функціональних елементів*** *(вузлів та/або каналів зв'язку)* ***за рахунок відповідної зміни структури і поведінки системи*** *(яка ґрунтується на результатах оцінки параметрів живучості)****, зберігаючи мінімально допустимий рівень якості функціонування відповідно до встановлених рівнів деградації із подальшим відновленням початкового ефективного функціонування протягом встановленого часу***.

Таким чином, технічне, програмне, інформаційне, методичне, лінгвістичне та організаційне забезпечення СЗІ повинне містити такі засоби, які дозволили б певним чином відреагувати на виникнення ситуацій, що призводять до погіршення функціонування та забезпечити збереження функціонування системи захисту інформації.

Зважаючи на складність задачі забезпечення живучості СЗІ її вирішення разовими конкретними заходами є неможливим. Необхідною є неперервна направлена система встановлених дій, які виконувалися б протягом усього життєвого циклу СЗІ. Складність надання властивості живучості СЗІ пояснюється й складністю бізнес-процесів, що протікають в корпоративних мережах зв'язку і, як наслідок, - складність сучасних інформаційних систем, що призначені для автоматизації цих бізнес-процесів.

Забезпечення живучості ускладнюється ще й тим, що в сьогоднішніх умовах сучасна система захисту інформації може самостійно породжувати нові функції, що не були закладені ні в технічному завданні, ні в проекті системи, не говорячи вже про неадекватну реакцію на виникнення різних непередбачуваних ситуацій.

Висновки

Аналіз проблеми забезпечення живучості в галузі інформаційної безпеки та запропоноване в роботі визначення поняття живучості системи захисту інформації має практичний інтерес для науковців, проектувальників та аудиторів систем захисту інформації та кінцевих користувачів.

Всі сучасні СЗІ володіють схожою структурою, складаються із схожих елементів, володіють схожим технологічним циклом та виконують схожі функції. Система забезпечення живучості (СЗЖ) для таких СЗІ також будуть володіти схожими рисами. Ця обставина дозволяє розробляти шаблонне рішення для СЗЖ, описати її типові задачі, структуру, методику побудови, а також визначити засоби, які входять в її склад.

Проте, кожна СЗІ є по-своєму унікальна для кожного об'єкту, на якому вона впроваджується, володіє специфічними рисами, якими вона наділяється відповідно до об'єкту та вимог замовника. Така унікальність вимагає побудови СЗЖ для кожної СЗІ індивідуально, що, в свою чергу, вимагає індивідуального підходу до розроблення СЗЖ для кожної конкретної СЗІ. СЗЖ повинна неперервно розроблятися паралельно з СЗІ та в повному обсязі враховувати її специфіку. Тільки в такому випадку можна досягнути максимально ефективного функціонування СЗЖ, СЗІ, КМЗ та організації в цілому.

Список літератури

1. Бачинський І.В. Термінологічний словник з інформаційної безпеки // І.В. Бачинський, В,Б. Дудикевич, В.С. Зачепило, Л.Т. Пархуць, В.В. Хома, О.В. Яструбецький. – Львів, 2005. – 140 с.

2. Глушкова В.М. Словарь по кибернетике // В.М. Глушкова. – К...: Гл. ред. Укр. сов. энциклопедии, 1979. – 880 с.

3. Волик Б.Г. Эффективность, надежность и живучесть управляющих систем // Б.Г. Волик, Й.А. Рябинин. – Автоматика и телемеханика. – 1984. – 340 с.

4. Тарасенко, Ф.П. Прикладной системный анализ (Наука и искусство решения проблем): учебник / Ф.П. Тарасенко. – Томск: Том. ун-т, 2004. – 186 с.

5. Мирзоев, Р.Г. Основные процедуры системных исследований: учеб. пособие / Р.Г. Мирзоев, А.Ф. Харченко. – СПб.: СПбГУАП, 2000. – 180 с.

6. Дж. ван Гиг. Прикладная общая теория систем: пер. с англ. / Дж. ван. Гиг. – М.: Мир, 1981. – 733 с.

7. Ellison R.J. Survivable Network Systems^ An Emerging Discipline / R.J. Ellison // Tech. Report CMU/SEI-97-TR-013. – Pittsburg, Penn, 1997. – P. 37-41.

8. IEEE Std 1061-1992, IEEE standard for a software quality metrics methodology.

9. Fisher D.A. Emergent algorithms - a new method for enhancing survivability in unbounded systems / D.A. Fisher, H.F. Lipson // Proceedings of the 32nd Annual Hawaii International Conference on Systems Sciences, IEEE. – 2002. – P. 351-357.

10. Robert P. Quality requirements for software acquisition / P. Robert // Software Engineering Standards Symposium and Forum, IEEE. – 1997. – P. 136-143.

11. Мордвинов, В. А. Онтология моделирования и проектирования семантических информационных систем и порталов / В.А. Мордвинов. – М., 2005. – 237 с.