УДК 004.056

Ю.Р. Гарасим

Національний університет «Львівська політехніка», Львів

АНАЛІЗ СИСТЕМ ЗАХИСТУ, ЯКІ МАЮТЬ ВЛАСТИВІСТЬ ЖИВУЧОСТІ

Стаття присвячена аналізу систем захисту інформації, які мають властивість живучості. За рахунок впровадження для систем захисту механізмів забезпечення живучості відбувається підвищення стійкості до атак, вторгнень, відмов і, відповідно, підвищується ефективність та результативність функціонування організації. Наведено основні властивості систем захисту, які мають властивість живучості. В статті пропонується метод аналізу живучості, який базується на таксономії загроз та деградації рівнів якості функціонування системи захисту інформації.

Ключові слова: *властивість живучості, системи захисту, рівні деградації якості функціонування.*

Вступ

Аналіз властивості живучості систем захисту інформації (СЗІ) [1] – прикладний процес. Метод аналізу живучості СЗІ є цілісним методом, невід'ємною частиною забезпечення захисту інформації від початкового етапу – планування СЗІ, до етапу її реалізації. Метод базується на оцінці безпеки, яка враховує одну загрозу і один захід захисту, шляхом інтегрального аналізу всіх загроз і заходів захисту, що необхідні для створення системи захисту, яка має властивість живучості [2]. Етапи методу аналізу живучості СЗІ містять цілі системи та визначення архітектури, визначення основних та додаткових завдань, що можуть бути скомпрометовані та аналіз живучості функціональних елементів, які водночас є необхідними для виконання й можуть бути скомпрометовані. Таксономія/модель загроз та вразливостей відіграють ключову роль в методі аналізу живучості СЗІ [3]. Результати аналізу живучості СЗІ в подальшому використовуються у визначенні необхідних заходів забезпечення живучості при забезпеченні стійкості системи захисту, усвідомленні атак і втручань, відновленні, а також до архітектури системи і вимог до неї.

Метод передбачає детальний огляд організаційних вимог до системи захисту, яка піддається аналізу. Аналізуються усі компоненти, процеси та архітектури, об'єднуються для пошуку вразливої ланки.

Незалежно від виявленої вразливої ланки, що впливає на роботу організації, аналізуються та вживаються заходи для забезпечення живучості системи захисту інформації. Вони надають інформацію про план для вдосконалення системи захисту в майбутньому, що робить його еволюційним процесом. Вважатимемо, що система захисту буде перебувати під впливом дестабілізуючих факторів (атаки, втручання, компрометація даних). Наведемо процес, який використовується для створення системи захисту, що матиме властивість живучості [2].

Аналіз останніх досліджень і публікацій. Хоча поняття живучості відоме в техніці давно і практично використовується при створенні технічних систем різного призначення, до сьогодні не було створено розвиненої теорії, яка містила б, як і теорія надійності, загальнотехнічні результати, що дозволяють досліджувати цю властивість, оцінювати її кількісно і розробляти практичні рекомендації проектувальнику СЗІ із забезпеченням властивості живучості.

На цей час теорія живучості знаходиться на такому етапі свого розвитку, коли ще не сформовані основні поняття і визначення, не існує єдиної думки і про те, що таке живучість, яка сфера її застосування. Практично немає апробованих тривалим практичним використанням моделей живучості. Велика різноманітність показників живучості, що пропонуються швидше свідчить про недостатню ясність у вирішенні цього питання, ніж про його пропрацьованість. Немає чітких методичних розробок оцінки живучості систем захисту інформації, яким чином нормувати і забезпечувати її живучість.

Значний внесок в розробку питань загальної теорії живучості систем внесли роботи докторів наук Рябинина І.А., Крапивина В.Ф., Парфенова Ю.М., Флейшмана Б.С., Котельникова В.А. Тематика живучості корпоративних та інформаційних мереж описується в роботах та наукових публікаціях вітчизняних дослідників: Додонов А.Г. [4, 5], Флейтман Д.В. [6-8], Харибін А.В [9, 10], Павлов І.М. [11, 12]. Варто зазначити, що кількість зарубіжних публікацій за

цією тематикою набагато більша, ніж вітчизняних. Серед зарубіжних авторів можна виділити переважно роботи науковців Росії: Громов Ю.Ю. [23], Черкесов Г.Н. [13, 14], Зиновьев П.А. [15]; США: Ellison R.J. [16, 17], Deepak R. [18], Китаю: Chenxi Wang [19], Yu Liu [20] та інші.

Постановка проблеми. Системи захисту інформації, які є основним механізмом забезпечення безпеки організації, повинні мати властивість живучості для того, щоб функціонувати в «агресивному» середовищі при дії зовнішніх та внутрішніх дестабілізуючих факторів (ДФ). Ця необхідність зумовлена тим, що припинення функціонування СЗІ внаслідок дії ДФ призводить до великих економічних втрат або катастрофічних наслідків через реалізацію загроз конфіденційності, доступності та цілісності інформації, яка в них функціонує.

Разом із проблемою захисту інформації в захищених корпоративних мережах зв'язку, які все частіше характеризують гетерогенністю структури, постає ще не до кінця досліджена проблема проектування та експлуатації СЗІ із заданими показниками живучості (survivability), для чого необхідно проводити її аналіз та оцінку. На цей час завдання аналізу та оцінки живучості СЗІ залишається невирішеним. Вирішення цього завдання дасть змогу проектувати СЗІ із заданими показниками живучості, експлуатувати їх в умовах ДФ із гіршими показниками якості функціонування, а також відновлювати їхню роботу.

Мета статті – розробити та дослідити метод аналізу живучості систем захисту інформації.

Живучість систем захисту

На цей час системи захисту інформації є розподіленими системами, підвищують ефективність і результативність функціонування організації, впроваджуючи нові рівні організаційної інтеграції. Проте така інтеграція супроводжується підвищеним ризиком вторгнень і компрометації інформації. Ці ризики можуть бути мінімізовані за рахунок включення заходів забезпечення живучості в системах захисту. Живучість як новостворена дисципліна ґрунтується на суміжних областях дослідження (наприклад, безпека, відмовостійкість, надійність, можливість повторного використання, продуктивність, перевірка та тестування) і вводить нові поняття й принципи. Основна увага властивості живучості приділяється збереженню основних послуг в системах захисту середовищ функціонування, навіть у тому випадку, коли системи в таких умовах піддаються впливу дестабілізуючих факторів [4].

Характеристики систем, що мають властивість живучості

Однією з ключових характеристик систем захисту інформації, які мають властивість живучості, є їх здатність надавати принаймні основні послуги в умовах здійснення атаки, відмови або аварійної ситуації [1, 4]. Основною при наданні необхідних послуг є здатність системи зберігати такі властивості, як, наприклад, задані рівні цілісності, конфіденційності, продуктивності та інші атрибути якості функціонування за наявності атак, відмов або аварійної ситуації. Таким чином, важливим завданням є визначення мінімального рівня якості атрибутів, які повинні бути пов'язані з основними послугами. Наприклад, запуск ракети системою захисту не буде ефективним, якщо продуктивність системи сповільнюється настільки, що ціль знаходитиметься за межею контрольованої зони, перш ніж система здійснить запуск.

Ці атрибути якості настільки важливі, що визначення живучості часто виражаються в розумінні підтримки балансу між декількома якісними атрибутами, такими як продуктивність, безпека, надійність, доступність, відмовостійкість, модифікованість і доступність. Атрибути якості представляють широкі категорії відповідних вимог, тому атрибути якості можуть містити інші атрибути якості. Наприклад, атрибут безпеки містить в собі три атрибути: конфіденційність, цілісність і доступність.

Можливість надання основних послуг (і підтримка суміжних властивостей) повинна бути гарантованою, навіть якщо значна частина системи виходить з ладу. Крім того ця здатність не повинна залежати від живучості конкретних інформаційних ресурсів, обчислень або каналу зв'язку. У військовому застосуванні основних послуг можуть бути ті, які необхідні для підтримки технічної переваги, а також основні властивості можуть включати цілісність, конфіденційність та рівень продуктивності, що буде достатнім для досягнення результатів за період менший, ніж один цикл рішення противника. У державному секторі, наприклад, живучість фінансової систем, яка підтримує цілісність, конфіденційність і доступність необхідної інформації та фінансові послуги, навіть якщо конкретний вузол або канал зв'язку втрачає працездатність внаслідок вторгнень або нещасного випадку і відновлює працездатність та своєчасне надання основних послуг внаслідок реалізації атаки. Живучість фінансової системи може бути оцінена за допомогою композитних мір порушення торгівлею акціями або банківських операцій (тобто оцінка внаслідок порушення основних послуг).

Ключові концепції живучості полягають у визначенні основних послуг (й суттєвих властивостей, які підтримують їх) в системі функціонування системи захисту інформації. Основні послуги визначаються як функції системи, яких слід дотримуватися у середовищі впливу дестабілізуючих факторів і/або нещасних випадках виявлення, які загрожують системі.

Існує велика кількість послуг, функціонування яких може бути тимчасово припинено, коли система має справу з атакою або іншими надзвичайними ситуаціями. Такий підхід може допомогти виокремити осередки, що постраждали від вторгнення, і вільні ресурси системи у зв'язку з його наслідками. Загальна функція системи повинна бути адаптована до збереження основних послуг.

Як було сказано вище, можливість системи, яка має властивість живучості для виконання своєї цілі, полягає у своєчасній здатності надавати основні послуги в умовах атаки, аварії чи збою. Якщо необхідна послуга втрачається або її виконання неможливе – вона може бути замінена іншою послугою, що підтримує виконання заданої цілі іншим, але еквівалентним чином. Проте визначення та захист основних послуг є важливою частиною практичного підходу до створення та аналізу систем захисту, які мають властивість живучості. В результаті основні послуги включають альтернативні набори основних послуг (можливо, взаємно виключних), які не повинні бути одночасно доступні. Для підтримки їх здатності надавати основні послуги системи захисту повинні володіти чотирма ключовими властивостями, які показані в табл. [21]:

Таблиця

Основні властивості систем захисту, які мають властивість живучості

Властивість	Опис	Приклад
Стійкість до атак	Методики виявлення та запобігання атак	Автентифікація користувачів; стохастична різноманітність програмного забезпечення
Виявлення наявності атаки та оцінка рівня пошкодження	Методики для виявлення атак (в тому числі й вторгнень) і визначення поточного стану системи, оцінка рівня пошкодження	Врахування моделей внутрішніх втручань; перевірка цілісності даних
Відновлення усіх або основних послуг після атаки	Методики відновлення скомпрометованої інформації або функціонування системи, обмеження масштабів збитку, підтримка або відновлення основних послуг в умовах обмеженого виконання функціональних елементів, відновлення повного спектра послуг	Реплікація й додаткова ініціалізація даних
Адаптація та вдосконалення з метою мінімізувати ефективність атак в майбутньому	Методики вдосконалення системи захисту на основі знань, які отримуються внаслідок виявлених атак	Впровадження нових моделей для виявлення втручань

Таксономія загроз

У класичній роботі з теоретичних проблем практичного використання системного аналізу в якості загальних принципів опису складних систем представлені наступні:

- принцип цілі;
- принцип багаторівневого опису;
- принцип класифікації.

Розглянемо, що дає застосування цих принципів до процедури побудови таксономії загроз систем захисту інформації. Провідним принципом опису систем виступає принцип мети. Для того, щоб конкретизувати цей принцип у відношенні досліджуваної проблеми, скористаємося формальною схемою моделі загроз безпеки, де для структурної моделі системи захисту виду

$$S = \{MC_i, i \in I\} \quad (1)$$

пропонується схема моделі загроз СЗІ виду

$$S^Y = \{MC_i^Y, i \in I\}, \quad (2)$$

де I – це безліч структурних представлень СЗІ, що дозволяють ідентифікувати всю множину загроз безпеки СЗІ;

MC_i – множина об'єктів, які представляють i-те структурне представлення СЗІ;

MC_i^Y – множина загроз, що ідентифікуються за об'єктами i-го структурного представлення СЗІ.

Очевидно, що в межах моделі можна представити ще декілька схем для завершення загальної схеми міркувань. А саме:

– схему профілю вимог щодо захисту (профілю захисту) СЗІ

$$S^{YR} = \{MC_i^{YR}, i \in I\}; \quad (3)$$

– схему множини заходів протидії, що задовольняють вимогам, які обрані для виключення загроз безпеці СЗІ

$$S^{YRM} = \left\{MC_i^{YRM}, i \in I\right\}; \quad (4)$$

– схему структурної моделі захищеної СЗІ, яка має властивість живучості

$$S^{YRMZ} = \left\{MC_i^{YRMZ}, i \in I\right\}. \quad (5)$$

Схема S^{YRMZ} описує новий «захищений» стан вихідної системи S, який може бути досягнутий після виконання певних процедур, що можна представити у вигляді операторів – побудови бази даних знань (БДЗ) (O^B), побудови моделі загроз (O^Y), побудови профілю захисту (O^R), розробки системи заходів захисту (O^M), розв'язання задач з оцінки створеної СЗІ при її реалізації (O^Z)

$$O^B : \left\{T^Y, DBI\right\} \to B^Y, \quad (6)$$

$$O^Y : \left\{S, B^Y\right\} \to S^Y, \quad (7)$$

$$O^R : \left\{S^Y, B^R\right\} \to S^{YR}, \quad (8)$$

$$O^M : \left\{S^Y, S^{YR}, B^M\right\} \to S^{YRM}, \quad (9)$$

$$O^Z : \left\{S^Y, S^{YR}, S^{YRM}, Z\right\} \to S^{YRM} Z, \quad (10)$$

де DBI – інструментарій розробки бази даних (БД) СЗІ. Основна вимога до DBI – він повинен дозволяти реалізувати БДЗ на основі заданої таксономії загроз T^Y;

Z – множина завдань, які повинні бути вирішені, для того щоб реалізувати заходи щодо захисту на заданих рівнях якості та гарантованості, що передбачені S^{YRM};

B^Y – БД загроз безпеки СЗІ;

B^R – БД вимог з безпеки СЗІ;

B^M – БД заходів протидії загрозам безпеки СЗІ.

Очевидно, що вирази (6) – (10) відображають не просто мету, а послідовність («дерево») цілей. Для їх досягнення завдання формування таксономії може бути сформульоване у вигляді оператора

$$O^T : \left\{S, B^R, B^M, Z\right\} \to T^Y. \quad (11)$$

Вираз (11) дозволяє конкретизувати принцип цілі для завдання побудови таксономії загроз СЗІ у вигляді наступних чотирьох принципів:

(I) Таксономія загроз безпеки повинна відповідати безлічі структурних представлень СЗІ (1).

Таксономія повинна передбачати наявність атрибутів загроз, які вказують на ті структурні представлення СЗІ, в яких вона може бути ідентифікована.

(II) Таксономія загроз безпеки повинна відповідати таксономії вимог з безпеки інформаційних технологій.

Цей принцип у додатку до розробки бази даних загроз може бути сформульований у вигляді вимоги ідентифікації щодо кожної загрози множини вимог її парування з бази даних вимог безпеки інформаційних технологій.

(III) Таксономія загроз безпеки повинна відповідати класифікації заходів протидії загрозам.

Цей принцип означає необхідність врахування в таксономії і, відповідно, в БДЗ класифікації заходів протидії і зокрема класифікацію за видами програмних і апаратних засобів. Наприклад, очевидно, що певна множина загроз існує тільки для інформаційних технологій (ІТ) на базі операційної системи (ОС) Unix і не існує для ІТ на базі ОС Windows NT, і навпаки. Такого роду відмінності добре відстежуються при класифікації заходів протидії, і це повинно враховуватися в таксономії загроз і при реалізації БДЗ.

(IV) Таксономія загроз безпеки повинна відповідати завданням з реалізації заходів протидії загрозам у СЗІ.

Роль таксономії загроз на етапі реалізації заходів щодо захисту СЗІ, яка має властивість живучості полягає в тому, що вона повинна дозволяти різним категоріям розробників, експертів і замовників системи оцінювати повноту захисту системи в різних аспектах: за структурними складовими системи, категоріями втрат, категоріями джерел загроз, інформаційними технологіями, що використовуються, тощо.

Наступним важливим принципом системного аналізу є принцип багаторівневого опису. Він говорить, що будь-який об'єкт при його системному поданні повинен бути описаний, по-перше, як елемент більш широкої системи, по-друге, як цілісне явище, по-третє, як деяка складна структура, внутрішню будову якої необхідно представити з достатньою для досягнення цілей дослідження рівнем деталізації.

У випадку таксономії загроз як об'єкта, що досліджується розглядається категорія загроз безпеки СЗІ.

Будь-яка загроза може бути реалізована певним чином. Спосіб реалізації загрози будемо називати атакою. Як правило, загроза може бути реалізована не одним, а кількома способами, тому можна говорити про множину атак, які пов'язані із загрозою безпеки СЗІ. Так, наприклад, загроза неявної компрометації секретних криптографічних

ключів у конкретному випадку може бути представлена у вигляді наступних атак, за допомогою яких вона може бути реалізована:

Атака 1 – приховане несанкціоноване копіювання інформації з машинних носіїв (дискет, смарт-карт, Touch-Memory), на яких записані криптоключі.

Атака 2 – «успішний» криптоаналіз, що дозволив «зламати» криптографічний алгоритм.

Атака 3 – копіювання за допомогою спеціальних програм («жучків», «закладок») криптографічних ключів під час їхнього перебування в оперативній пам'яті ЕОМ при виконанні криптографічних перетворень.

Таким чином, повертаючись до формальної схеми, будь-яка загроза може бути представлена вектором

$$Y = (IDO, A), \qquad (12)$$

де IDO – множина інформації, що ідентифікує і характеризує загрозу Y, як цілісний об'єкт в таксономії T^Y;

A – множина атак, за допомогою яких загроза Y може бути реалізована.

Атаку $A \in$ A можна представити у вигляді процедури, що ініціюється деяким джерелом атаки (SR), яке, використовуючи ті чи інші слабкі місця в СЗІ та умови їх використання (VL), через певні механізми атаки (MH), завдає шкоди (DG) СЗІ та інформаційним ресурсам СЗІ

$$A: \{SR, VL, MH\} \to DG. \qquad (13)$$

Інтерпретація атаки як процедури, дозволяє виділити класифікаційні ознаки, що задаються: 1) джерелами атаки; 2) вразливостями СЗІ, які використовуються в якості ресурсів атаки; 3) результатом атаки – шкода, яка наноситься СЗІ та її інформаційним ресурсам; 4) методами реалізації атаки – методами нанесення збитку СЗІ; 5) джерелом атаки шляхом використання вразливостей СЗІ. Очевидно, що таке подання загроз й атак дозволяє побудувати таксономію, яка буде задовольняти сформульованому вище принципу (IV), і закладає можливість при реалізації системи забезпечення безпеки СЗІ вирішувати такі завдання, як:

– контроль забезпечення безпеки СЗІ від основних джерел загроз;

– контроль усунення або послаблення можливостей використання слабких місць ІТ при атаках на СЗ;

– контроль можливостей системи захисту з протидії основним механізмам ата;

– контроль рівня можливого збитку при реалізації загроз.

Таким чином, додаток загального принципу багаторівневого опису до проблеми побудови таксономії загроз дозволяє конкретизувати його у вигляді принципу (V) – принципу обов'язковості відображення в таксономії загроз способів реалізації загроз – атак як процедур, здійснення яких призводить до збитку в СЗІ.

Нарешті, третій загальний принцип опису систем – принцип класифікації, встановлює необхідність класифікації значень параметрів (атрибутів) системи, які обираються.

Цей принцип при його додатку до проблеми побудови таксономії загроз може бути сформульований у вигляді принципу (VI) – обов'язковості класифікації значень параметрів (атрибутів) загроз, які обираються у межах таксономії загроз безпеки ІТ та СЗІ (VI).

Параметри (атрибути) загроз повинні включати:

Атрибут структурних складових СЗІ, в якому можуть бути ідентифіковані загрози безпеки ІТ і СЗІ. Необхідність наявності цього атрибуту випливає з принципу (I). Класифікація значень цього атрибута визначається множиною структурних представлень системи (1).

Атрибут вимог з протидії загрозам. Необхідність наявності цього атрибуту випливає з принципу (II). Класифікація його значень визначається ЗК.

Атрибут заходів протидії. Необхідність наявності цього атрибуту випливає з принципу (III). Класифікація його значень визначається класифікацією існуючих інформаційних технологій, які можуть використовуватися для захисту ІТ і СЗІ.

Далі йдуть атрибути, *які пов'язані із способами реалізації загроз* – атаками. Необхідність наявності цих атрибутів випливає з принципів (IV) і (V).

Атрибут категорії джерела атаки. Класифікацію джерел атак доцільно будувати на основі деяких об'єктивних параметрів – фізичної природи джерела (людина, програма або апаратні засоби), місця розташування джерела (локальне або віддалене), можливостей джерела з доступу до системи (користувач, адміністратор, сторонній). Такий підхід видається більш продуктивним, ніж використання популярних, але занадто широко трактованих понять типу «хакер».

Атрибут категорії втрат. Пропонується розглядати чотири категорії втрат. Втрати властивостей конфіденційності, цілісності, доступності, захисту безпеки інформації та ІТ в СЗІ.

Атрибут слабких місць (СМ) ІТ та СЗІ, які можуть використовуватися при реалізації атаки. Сюди включаються СМ, які зумовлені як природою інформаційних технологій (наприклад, побічне електромагнітне випромінювання), так і умовами їх

експлуатації (наприклад, людським фактором). Класифікація СМ визначається їх місцем розташування (для ІТ) або категорією осіб, які можуть негативно впливати на СЗІ (користувачі, адміністратори, розробники), і етапом життєвого циклу ІТ та СЗІ, коли ця особа може впливати на ІТ або СЗІ.

Атрибут ресурсів, яким завдається шкода, – атрибут збитку (втрат). Його значення класифікуються за місцем розташування і типом ресурсу.

Атрибут методів атаки. Його значення класифікують, насамперед, відповідно до категорій втрат, і далі згідно з класифікацією ресурсів, яким завдається шкода.

Таким чином, на основі загальних принципів системного аналізу нами запропонована система з шести принципів, яких слід дотримуватися при розробці таксономії загроз безпеки СЗІ, що має властивість живучості [22].

Застосування методу аналізу живучості

Метод є технологічним процесом, який забезпечує оцінку живучості сучасних систем захисту [2] і модифікацій існуючих систем захисту. Він складається з чотирьох етапів. *Крок 1*: визначаються цілі та використання вимог до системи захисту, її архітектура. *Крок 2*: на основі цілей і наслідків відмов визначаються основні послуги (які повинні мати властивість живучості) та основні засоби (ті активи, які повинні бути збережені під час атаки). Тоді визначаються моделі їх використання на основі визначених вище бізнес-функцій. Далі з наступним об'єднанням вищевказаних вимог вони пов'язуються з архітектурою системи захисту для того, щоб визначити основні компоненти (ті, які повинні бути в змозі надавати основні послуги та захист основних активів під час атаки). *Крок 3*: модель загроз (відповідно до таксономії загроз) вибирається так, щоб визначити вразливі компоненти (ті, які можуть бути піддані атакам). Останнім кроком є визначення вразливих компонентів архітектури (основні компоненти, які є вразливими). *Крок 4*: компоненти аналізують на три основні властивості живучості: стійкість до атак, виявлення атаки і відновлення функціонування. В результаті отримується «карта (модель, матриця) живучості», яка є відображенням залучення усіх моделей загроз із відповідними вразливостями, пов'язані поточні і рекомендовані архітектури стратегії опору, виявлення атак і відновлення функціонування системи захисту.

Описаний вище процес здійснюється двома підрозділами: підрозділом організації (ПО) і підрозділом забезпечення безпеки (ПЗБ). Дві групи взаємодіють через низку зустрічей. Підрозділ організації забезпечує визначення цілей, бізнес-процесів і системну архітектуру для ПЗБ. Підрозділ ЗБ використовує надану ПО інформацію для визначення основних компонентів і вимог до ПО. Підрозділ забезпечення безпеки аналізує атаки і звітує про вразливість компонентів ПО. Тоді ПЗБ визначає «карту живучості» і надають її ПО.

Описаний вище процес не завжди є лінійним. Вхідна інформація може змінюватися, переглядатися на будь-якому спільному засіданні, а також зміни використовуватися для оновлення результатів на будь-якому кроці. Цей процес отримав назву «спірального» – будь-який крок може бути повторений; навіть в кінці першого кроку можна було б повторити ще раз, якщо з'являється нова інформація.

Рівні деградації функціонування систем захисту

Система захисту інформації в залежності від своїх параметрів, стану системи управління, обладнання СЗІ та системи управління цим обладнанням може зазнавати різних рівнів деградації (рис. 1).

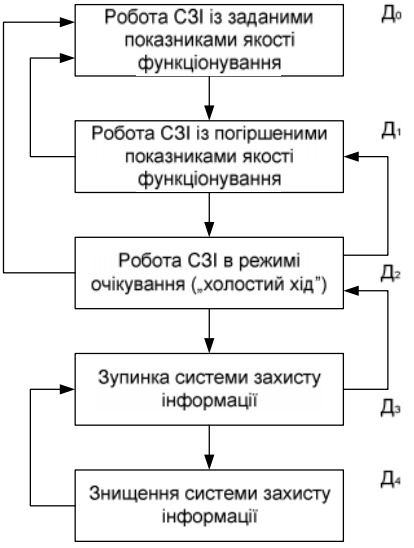

Рис. 1. **Рівні деградації системи захисту інформації, яка має властивість живучості**

Робота СЗІ із заданими показниками якості функціонування як в стаціонарних, так і в нестаціонарних (екстремальні умови) режимах відповідає вимогам, що застосовуються до неї, та є нульовим рівнем деградації ($Д_0$).

На першому рівні деградації ($Д_1$) СЗІ працює із погіршеними показниками якості функціонування та більш низькими, ніж номінальні, вихідними параметрами. Перехід на перший рівень деградації може бути спричинений відмовами в системі

управління СЗІ, в обладнанні СЗІ, в системі управління цим обладнанням, а також вимогами енергосистеми. Економічні втрати при цьому переході – невеликі. Період перебування СЗІ на цьому рівні деградації може бути недовготривалим, достатнім для відновлення обладнання, яке відмовило. Після цього СЗІ повертається на нульовий рівень деградації.

При певних умовах можливий перехід СЗІ на другий рівень деградації «холостий хід», ($Д_2$), тобто відбувається непланове від'єднання СЗІ від електромережі. На другий рівень деградації СЗІ може перейти як з нульового, так і з першого рівня. Економічні втрати при переході СЗІ в даний режим роботи збільшуються. З другого рівня деградації СЗІ може повернутися на перший або нульовий рівень деградації.

Третім рівнем деградації СЗІ є «зупинка» ($Д_3$). Вимушена зупинка СЗІ завдає великих економічних втрат. СЗІ на цей рівень деградації може перейти із будь-якого з раніше розглянутих рівнів деградації.

На нульовий або перший рівень деградації СЗІ може повернутися шляхом реалізації алгоритму запуску.

Останній, четвертий рівень деградації ($Д_4$), відповідає незворотному катастрофічному стану СЗІ «знищення». При цьому економічні втрати досягають значних розмірів, а також можливі й людські втрати (фізичне знищення елементів СЗІ, терористичні акти тощо).

Перехід СЗІ із режиму роботи із заданими показниками якості функціонування на наступні рівні деградації визначаються як змінами параметрів самої СЗІ, так і деградацією системи управління СЗІ, обладнання СЗІ та систем управління цим обладнанням, а також станом енергосистеми.

При дослідженні живучості СЗІ доцільно встановити зв'язок між рівнями деградації системи управління СЗІ та обладнанням СЗІ з рівнями деградації об'єкта управління – системою захисту інформації.

Алгоритм функціонування автоматизованої системи управління СЗІ при наявності в ній відмов наведемо на рис. 2.

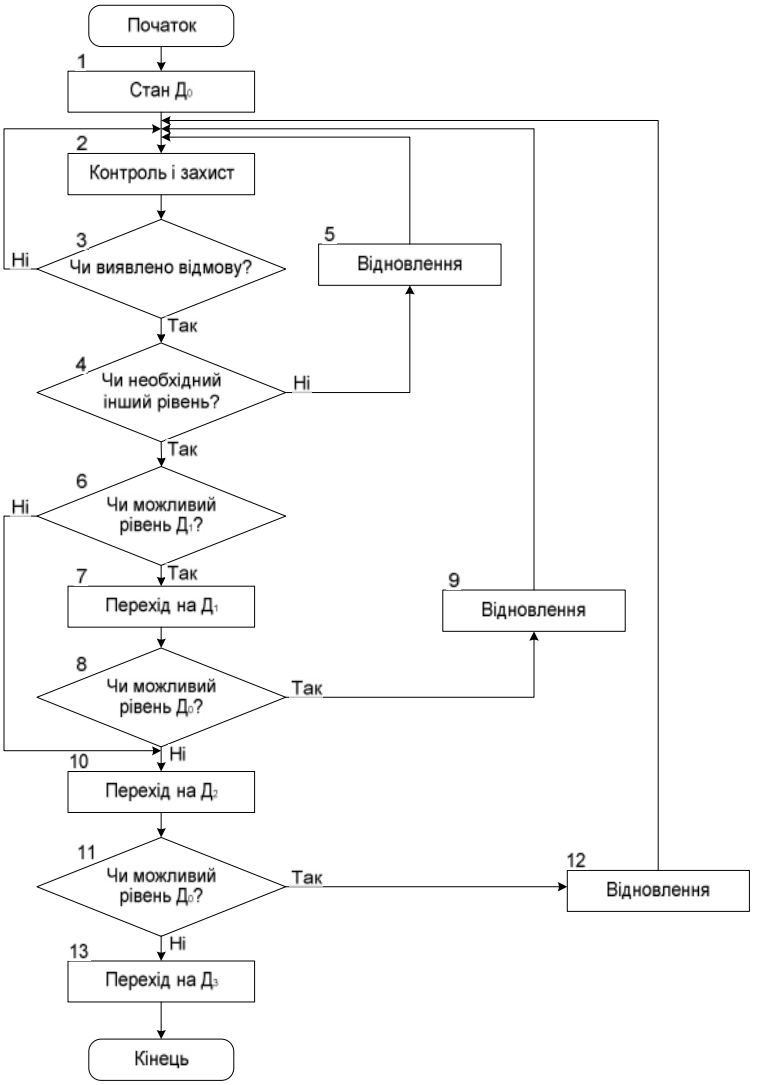

Рис. 2. **Алгоритм функціонування системи захисту інформації при наявності в ній відмов**

Висновки

У роботі пропонується метод аналізу живучості систем захисту інформації у вигляді 4-етапного процесу. У методі враховуються різні зовнішні та внутрішні дестабілізуючі фактори (зокрема, таксономії/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. Предметом подальших досліджень є створення нових і вдосконалення існуючих методів оцінки живучості систем захисту інформації для захищених корпоративних мереж зв'язку, що дозволить проектувати такі мережі із наперед заданими показниками живучості і, відповідно, стійкими до атак, відмов тощо.

Список літератури

1. Гарасим Ю. Р. Поняття живучості системи захисту інформації захищених корпоративних мереж зв'язку / Ю. Р. Гарасим, В. Б. Дудикевич // Тези доповідей ІІІ міжнародної науково-практичної конференції «Інформаційна та економічна безпека (INFECO-2010)». – Харків, 2010. – Випуск 3 (84). – С. 107-109.

2. Wutz Dale. Application of the Survivable Network Analysis Method to Secure My Office System / SANS Institute InfoSec Reading Room. – 2001. – P. 1-12.

3. Ellison R. J. A Case Study in Survivable Network System Analysis / R. J. Ellison, R. C. Linger, T. Longstaff, N. R. Mead // CMU/SEI-98-TR-014, ESC-TR-98-014. – 1998. – P. 1-37.

4. Додонов А. Г. Проблемы и тенденции создания живучих вычислительных систем / А. Г. Додонов, М. Г. Кузнецова. – К. : Наук. думка, 1981.

5. Додонов А. Г. Введение в теорию живучести вычислительных систем / А. Г. Додонов, М. Г. Кузнецова, Е. С. Горбачик. – К. : Наук. думка, 1990.

6. Флейтман Д. В. Подсистема обеспечения живучести корпоративной информационной системы / Д. В. Флейтман // Збірник наукових праць конференції «Інформаційні технології та безпека». – Київ, 2005. – Вип. 8. – С. 91-93.

7. Флейтман Д. В. Решение задачи обеспечения живучести корпоративных информационных систем при частичном разрушении каналов связи / Д. В. Флейтман // Реєстрація, зберігання і обробка даних. – 2005. – Том 7. – № 1. – С. 52-61.

8. Флейтман Д. В. Жизненный цикл и живучесть корпоративных информационных систем / Д. В. Флейтман // Реєстрація, зберігання і обробка даних. – 2004. – Т. 6. – № 3. – С. 74-84.

9. Харыбин А. В. Метод оценки живучести распределенных информационно-управляющих систем / А. В. Харыбин // Радіоелектронні і комп'ютерні системи. – 2007. – № 8. – С. 104-109.

10. Харыбин А. В. Программные средства оценки структурной надежности и живучести телекоммуникационных сетей критического применения / А. В. Харыбин // Радиоэлектроника и молодежь в XXI веке: 7-й Междунар. молодежный форум. – Харьков : ХНУРЭ, 2003. – С. 123.

11. Павлов І. М. Методики проектної оцінки надійності та живучості комплексної системи захисту інформації мобільних систем зв'язку і автоматизації : автореф. дис. на здобуття наукового ступеня канд. тех. наук: 05.13.21 / Павлов Ігор Миколайович; Держ. ун-т інформаційно-комунікаційних технологій. – К., 2008. – 19 с.

12. Павлов И. Н. Методика оценки количественных показателей живучести систем защиты информации / И. Н. Павлов // «Захист інформації». – Київ, 2005. – № 4 (27). – С. 5-14.

13. Черкесов, Г. Н. Методы и модели оценки живучести сложных систем / Г. Н. Черкесов. – М., 1987. – 38 с.

14. Астров В. В. Применение методов вероятностной логики и исследования операций к анализу живучести пространственно распределенных энергетических систем / В. В. Астров, И. П. Симаков, Г. Н. Черкесов // В кн.: Методические вопросы исследования надежности больших систем энергетики. – Вып. 20. – Иркутск : СЭИ СО АН СССР, 1980. – С. 32-42.

15. Зиновьев П. А. Анализ факторов и механизмов живучести в корпоративных информационных системах / П. А. Зиновьев // Исслед. по информ., Отечество. – Казань, 2007. – С. 3–30.

16. Ellison R. J. Survivable Network Systems: An Emerging Discipline / R. J. Ellison, D. A. Fisher, R. C. Linger, H. F. Lipson, T. Longstaff. – 1999. – 60 p.

17. Ellison R. J. Survivable Network System Analysis: A Case Study / R. J. Ellison, R. C. Linger, T. Longstaff, Mead N. M. – Carnegie Mellon University, 1998. – 20 p.

18. Deepak Rajan. Survivable network design: routing of flows and slacks / Rajan Deepak. – University of California, Berkeley, 2004. – P. 65-81.

19. Chenxi Wang. A security Architecture for Survivability Mechanisms / Wang Chenxi // A Dissertation Presented to the Faculty of the School of Engineering and Applied Science at the University of Virginia. – 2000. – 210 p.

20. Yu Liu. Spare capacity allocation: model, analyses and algorithm / Liu Yu. – Beijing, China, 1996. – 132 p.

21. Ellison R. J. Survivable Network Systems: An Emerging Discipline / R. J. Ellison, D. A. Fisher, R. C. Linger, H. F. Lipson, T. Longstaff, N. R. Mead // CMU/SEI-97-TR-013, ESC-TR-97-013. – 1999. – P. 1-51.

22. Черешкин Д. С. Принципы таксономии угроз безопасности информационных систем / Д. С. Черешкин, А. А. Кононов, Д. В. Тищенко [Електронний ресурс] режим доступу: http://www.rfbr.ru/default.asp?doc_id=5221

23. Громов Ю. Ю. Синтез и анализ живучести сетевых систем / Ю. Ю. Громов, В. О. Драчев, К. А. Набатов, О. Г. Иванова. – М.: «Издательство машиностроение – 1». – 2007. – 88 с.

Надійшла до редакції 25.10.2010 р.

Рецензент: доктор технічних наук, професор В.Б. Дудикевич, Національний університет «Львівська політехніка», Львів.

АНАЛИЗ СИСТЕМ ЗАЩИТЫ, ИМЕЮЩИХ СВОЙСТВО ЖИВУЧЕСТИ

Ю.Р. Гарасим

Статья посвящена анализу систем защиты информации, которые имеют свойство живучести. За счет внедрения для систем механизмов обеспечения живучести происходит повышение устойчивости к атакам, вторжений, отказов и, соответственно, повышается эффективность и результативность функционирования организации. Приведены основные свойства систем защиты, которые имеют свойство живучести. В статье предлагается метод анализа живучести, который базируется на таксономии угроз и деградации уровней качества функционирования системы защиты информации.

***Ключевые слова**: свойство живучести, системы защиты, уровни деградации качества функционирования.*

SURVIVABLE SECURITY SYSTEMS ANALYSIS

Y.R. Garasym

The paper is devoted to survivable security systems analysis. Resistance to attacks, intrusions, failures are increasing and, consequently, increases efficiency and effectiveness of enterprise functioning by implementing survivability mechanisms for security systems. The basic properties of survivable security systems are described. The paper proposes a survivability analysis method which is based on the security systems taxonomy of threats and functioning quality degradation levels.

***Keywords:** survivability, security systems, functioning quality degradation levels.*

УДК 629. 1113. 01

Л.В. Крайник, А.В. Волошанський

ВАТ "Український інститут автобусо – тролейбусобудування", Львів

ФОРМУВАННЯ ПЕРСПЕКТИВНОГО ТИПАЖУ АВТОТЕХНІКИ ДЛЯ ЗС УКРАЇНИ В СУЧАСНИХ УМОВАХ

В статті розглянуто існуючий типаж автомобільної техніки ЗС України та запропоновано новий, уніфікований модельний ряд військових автомобілів, що відповідають сучасним вимогам .

***Ключові слова:** типаж, повнопривідні вантажні автомобілі, технічні характеристики.*

Вступ

Впродовж останніх 30 років відбулись кардинальні зміни в формуванні типажу та перехід на нове покоління військових автомобілів, а з 2008-2010 рр. – практично появу нових промислових зразків наступного покоління (напр. MB Zetros). Разом з тим існуючий автопарк ЗС України є:

- практично на 90-95% з амортизованим і складається теж на 95% з тепер уже імпортних автомобілів явно застарілих моделей, розроблених понад 40-50 років тому (з 1956-1959 рр. – ГАЗ, ЗиЛ, УАЗ, з 1968-1970 рр. – КамАЗ);
- розуніфікованим за тактико-технічними характеристиками і параметрами прохідності (різна ширина колії – від 1780 мм в ГАЗ-66, 1453 мм в УАЗ-469, до 1820 мм для ЗиЛ-131, 2010 мм – КамАЗ-4310 і зрештою до 2160 мм в КрАЗ-260), аналогічно різні кліренс від 315 мм в ГАЗ-66 до 400 мм в Урал-375;
- різні допустимі осьові навантаження (від 3,9 т в ГАЗ-66 до 5 т в КамАЗ та 6,6 в КрАЗ), що ускладнює рух в одній колоні по бездоріжжю, в плані транспортних машин повністю роз уніфікована агрегатна база, 4 базові моделі (ЗиЛ, УАЗ, КамАЗ, КрАЗ) замість типового для сучасних армій уніфікованого за агрегатами і вузлами єдиного сімейства з 3 моделей (4х4,6х6,8х8) вантажністю відповідно 4,5-5 т, 7-8 т, 10-11 т.

Характерною особливістю зміні на нове покоління військових автомобілів в країнах Західної Європи і США (НАТО)з появою уніфікованих сімейств повно привідних вантажівок MAN (ФРН), важкого джипа M998 Hummer і його аналогів в 6 країнах Європи, Ізраїлі і з 2009 р. в КНР є перехід на сугубо утилітарні спеціальні автомобілі, максимально уніфіковані по параметрах прохідності (рух в єдиній колоні) та агрегатах і вузлах (типорозмірні ряди, мінімізація номенклатури запасних частин) з організацією спеціалізованих, відокремлених виробництв.