3. Першин И. М. Анализ и синтез систем с распределенными параметрами : Монография / И. М. Першин - Пятигорск, 2007. — 245 с.
4. Рапопорт Э. Я. Структурное моделирование объектов и систем управления с распределенными параметрами : учеб. пособие / Э. Я. Рапопорт. — М. : Высш. шк., 2003. — 299 с: ил.
5. Modicon Premium PLPs TSX 37/PPX 37 Implementation Manual Volume 1-4 / Руководство пользователя по ПЛК Modicon Premium. Тома 1-4. http://www.schneider-electric.ru/sites/russia/ru/support/automation-and-control-library/download/download-documents.page

УДК 681.518.25:004.056

В. М. Дубовой, Г. Ю. Дерман, О. М. Миколайчук

ПІДХІД ДО АНАЛІЗУ БЕЗПЕКИ ІЄРАРХІЧНИХ ІНФОРМАЦІЙНИХ СИСТЕМ, ЩО РОЗВИВАЮТЬСЯ

Метою роботи є розробка удосконаленої моделі безпеки ієрархічних інформаційних системах (ІІС), що розвиваються, в цілому, що враховує рівень безпеки складових елементів ІС. Забезпечення безпеки ІІС є важливою науково-технічною проблемою. У статті запропонований підхід, що ґрунтується на особливостях обробки інформації в ІІС. Для аналізу впливу порушень безпеки на виконання функцій ІІС розглянуто елементи ІІС як агенти мультиагентної системи, кожен з яких характеризується певним набором параметрів. Порушення безпеки розглядається як нездатність агентом виконувати деякі або усі функції. Розроблено алгоритм, що дозволяє прогнозувати ймовірність виконання функцій системи з урахуванням невизначеності факторів розвитку.
Ключові слова: порушення безпеки, ієрархічна інформаційна система, процес розвитку, невизначеність.

Постановка проблеми. Інформаційні системи (ІС) забезпечують постійно зростаючі потреби суспільства у отриманні, обробці, збереженні, пошуку та поданні інформації та знаходяться у стані постійного розвитку. Однією з найпоширеніших структур ІС є ієрархічна [1, 2].

Ієрархічна ІС (ІІС) складається з великої кількості компонентів: програмних та апаратних. Будь-які зміни цих складових ІІС можуть приводити до погіршення рівня її безпеки. Забезпечення безпеки ІІС є важливою науково-технічною **проблемою**. Небезпеку для ІІС несуть не тільки атаки [3, 4], але й неузгодженість окремих аспектів розвитку, що призводить до порушення здатності ІС протистояти атакам і виконувати свої функції. Деякі фактори і характеристики небезпеки неузгодженого розвитку наведені у [5].

Аналіз наукових досліджень та публікацій. Більшість робіт з інформаційної безпеки присвячено криптографічному і технічному захисту інформації [6, 7], контролю доступу [8], мережевій безпеці [9], забезпеченню надійності системи та її компонентів, відмовостійкості [10, 11] та ін. У [12] розглянуто методи оцінювання інформаційної безпеки і підходи до дослідження отриманих оцінок інформаційної безпеки. У [13] розглянуто ряд питань, пов'язаних із забезпеченням безпеки інформаційних технологій, розглянуто шляхи створення систем захисту інформації. Розроблена модель впливу

розвитку на безпеку окремого елементу розгалуженої ІС [5]. Проте питання зміни характеристик і рівня безпеки елементів ІІС, що розвивається, на загальний рівень безпеки досліджено недостатньо. **Метою** роботи є розробка удосконаленої моделі безпеки ІІС, що розвивається, в цілому, що враховує рівень безпеки складових елементів ІС.

Основні матеріали дослідження. Процес розвитку може бути поданий послідовними фрагментами логістичної кривої. Зокрема, статистичні дані щодо розвитку Інтернету свідчать, що розвиток відбувається циклічно. Таким чином, Враховуючи особливість розвитку ІС, яка полягає у постійному пришвидшенні процесів розвитку, процес розвитку ІС подамо системою рівнянь

$$\begin{cases} n(t) = \mathrm{int}\left[\dfrac{t}{T}\right]; \\ \tau(t) = t - n(t)\cdot\dfrac{T_0}{\left[n(t)\right]^{v}}; \\ S'(\tau) = \dfrac{K\cdot S_0 e^{r\tau}}{K + S_0\left(e^{r\tau}-1\right)}; \\ x(t) = S'(T)\cdot n(t) + S'(\tau), \end{cases} \qquad (1)$$

де T - інтервал дії одної ділянки логістичної кривої; $\mathrm{int}[\bullet]$ - функція виділення цілої частини аргументу; $n(t)$ - номер ділянки логістичного типу; $\tau(t)$ - інтервал часу від початку чергової ділянки логістичного типу; $S'(\tau)$ - окрема ділянка логістичного типу; $x(t)$ - крива розвитку параметра x; v - показник темпу прискорення. Параметри K, S_0, T, r підлягають ідентифікації для процесу розвитку окремого параметра ІІС.

Вектор параметрів $\bar{x}$ складається з двох підмножин: підмножини $\bar{x}_1$ параметрів, які менші за оптимальне значення $\bar{x}_{10}$, і підмножини $\bar{x}_2$ тих, які більші за оптимальне значення $\bar{x}_{20}$. Відповідно, збільшення значень $\bar{x}_1$ буде зменшувати ймовірність небезпеки, а збільшення $\bar{x}_2$ буде її збільшувати.

Для оцінювання ризику порушення безпеки необхідно отримати оцінки ймовірностей P варіантів порушення безпеки в результаті неузгодженого розвитку окремих параметрів ІС та масштаби впливу результатів цих порушень на роботу ІІС вцілому.

$$P = e^{-k\frac{\bar{x}_1}{\bar{x}_2}},\ \bar{x}_1 < \bar{x}_{10},\ \bar{x}_2 > \bar{x}_{20}. \qquad (2)$$

Зазначену ймовірність апроксимуємо функцією, яка задовольняє умови належності імовірнісному простору і має додаткові переваги диференційованості на усій області визначення. Коефіцієнт k підлягає ідентифікації для кожної ІС і пари підмножин її параметрів $\{\bar{x}_1, \bar{x}_2\}$.

Загальна ймовірність порушення безпеки деякої функції

$$P_{ij} = 1 - \prod_{\forall (x_u, x_v)} \left(1 - P_{ijx_u x_v}\right), \quad (3)$$

де x_u, x_v - параметри розвитку і-го агента, які впливають на виконання j-ої функції.

Для аналізу впливу порушень безпеки на виконання функцій ІІС будемо розглядати елементи ІІС як агенти мультиагентної системи, кожен з яких характеризується набором параметрів: множина функцій $\{F_i\}$, обсяг пам'яті M_i, продуктивність P_i, кількість комунікаційних каналів C_i, рівень розвитку засобів безпеки D_i, де i – індекс агента, тощо.

Порушення безпеки розглядається як нездатність агентом виконувати деякі або усі функції з множини $\{F_i\}$. Оскільки взаємодія агентів приводить до того, що виконання функцій одним агентом вимагає певних ресурсів, які надаються йому іншими агентами, то для побудови моделі безпеки скористаємось діаграмою логічних відношень між функціями - use-case diagram. При цьому для кожного агента всі інші виступають акторами, і одночасно мають внутрішню функціональну структуру. Use-case diagram представлені на рис. 1 та рис. 2. (відповідно, use-case diagram на рівні агента та use-case diagram на рівні ІС).

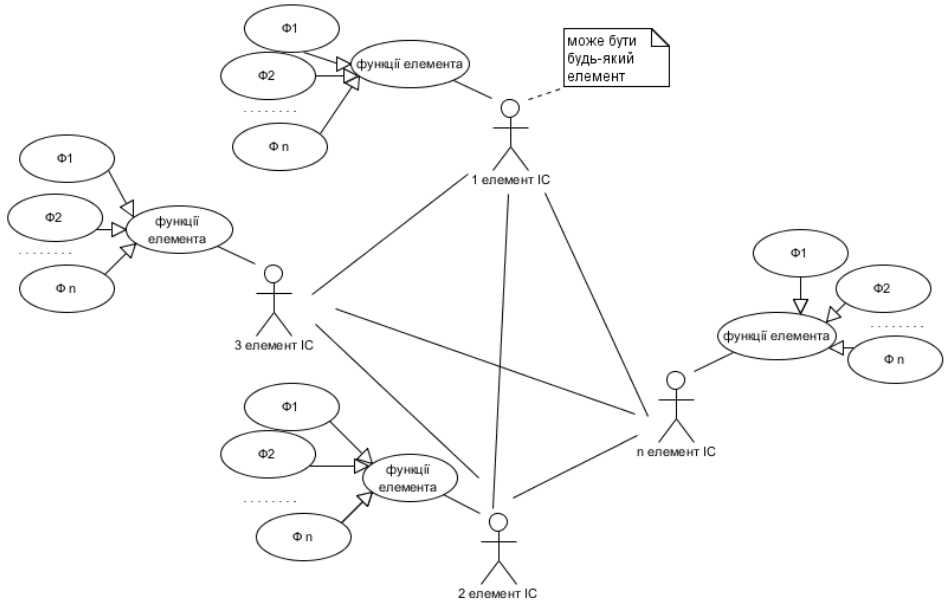

Рис. 1 - Use-case diagram на рівні агентів

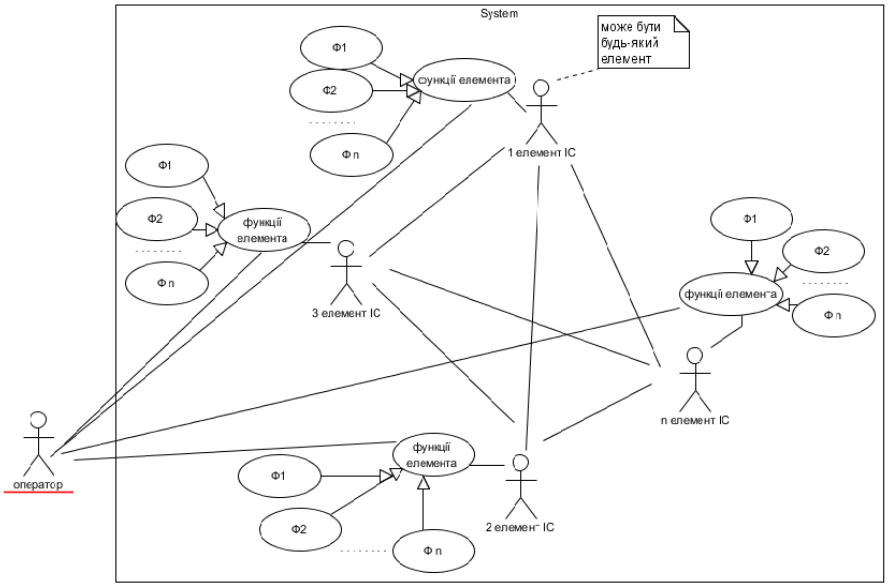

Рис. 2 - Use-case diagram на рівні інформаційної системи

Отримана таким способом use-case діаграма є орієнтованим графом, у якому від кожної функції як від кореня можна побудувати дерево Т використання ресурсів як того агента, що розглядається, так і агентів, що функціонально з ним пов'язані.

Звичайна діяльність агентів ієрархічної ІС передбачає обробку верхніми рівнями даних, що надходять з нижніх рівнів. З діаграми видно, що внаслідок ієрархічної структури ІС відмова функції, що забезпечує постачання інформації верхнім рівням, призводить до відмов відповідних функцій на усіх рівнях догори по дереву.

Для розв'язання задачі аналізу безпеки ієрархічних систем визначимо функції на графі, що зображує use-case diagram. Оскільки граф зазвичай подається матрицею суміжності, то функції будемо визначати над матрицею суміжності А:

1. Функція $UpLevel(A, a_{ij})$ – пошук вершини верхнього рівня по відношенню до вершини a_{ij}, де i - індекс агента; j - індекс функції у множині $\{F_i\}$.
2. Функція $Root(A, a_{ij})$ – визначення, чи є вершина a_{ij} коренем дерева.
3. Функція $DownLevel(A, a_{ij})$ – пошук вершини нижнього рівня по відношенню до вершини a_{ij}.
4. Функція $Leaf(A, a_{ij})$ – визначення, чи є вершина a_{ij} «листком» дерева.

Будемо вважати, що функція у вершині a_{ij} не буде виконана, якщо через порушення безпеки не буде виконана хоча б одна з функцій, які є для неї допоміжними, тобто є результатами функції $DownLevel$.

Твердження: для того, щоб виконувалася функція a_{ij}, необхідно, щоб виконувалися функції, що утворюють піддерево графа системи з коренем a_{ij}.

Доведення цього твердження легко здійснити методом індукції, починаючи з «листків» зазначеного піддерева.

Основні кроки алгоритму оцінювання ризику порушення безпеки ієрархічної ІС передбачають:

1. Опис use-case діаграми ІС у вигляді матриці суміжності;
2. Вибір інтервалу прогнозу;
3. Розрахунок прогнозних значень параметрів агентів на основі моделі (1);
4. Розрахунок ймовірності порушень безпеки за формулами (2) – (3);
5. Розрахунок ймовірності невиконання кожної функції дерева функцій, починаючи від «листків»

$$P_{ij\ \text{заг}} = 1 - \left[P_{ij0} + \left(1 - P_{ij0}\right) \cdot \sum_{\forall L_{ij}} P_{ijL_{ij}} \right], \qquad (4)$$

де L_{ij} – гілки дерева, які починаються від кореня a_{ij}; P_{ij0} – ймовірність порушення безпеки функції a_{ij}; $P_{ijL_{ij}}$ – ймовірність невиконання допоміжних функцій по гілці L_{ij}.

Не всі ресурси ІС однаково важливі для реалізації функцій системи, і дана модель не повністю описує реальну роботу системи. Для підвищення достовірності моделювання ІС, модель підлягає удосконаленню. Крім того, для складних ІІС реальні характеристики агентів часто невідомі, причому ступінь невизначеності зростає із зростанням відстані між агентами (у логічному розумінні, тобто як кількість дуг між функціями різних агентів на графі системи).

Запропонований підхід до аналізу безпеки ІІС застосований при проектуванні інформаційної системи освітніх закладів області (ІС ОЗО), яка призначена для підтримки процесу розподілу фінансових ресурсів.

На рис. 3 представлено ієрархічну структуру системи. Оскільки система розподілена та передбачає віддалений доступ користувачів з різними правами доступу, важливо забезпечити цілісність даних, їх високу захищеність та відмовостійкість. Також важливим аспектом є подальший розвиток системи (розширення функцій системи, введення нових навчальних закладів, відповідальних осіб тощо).

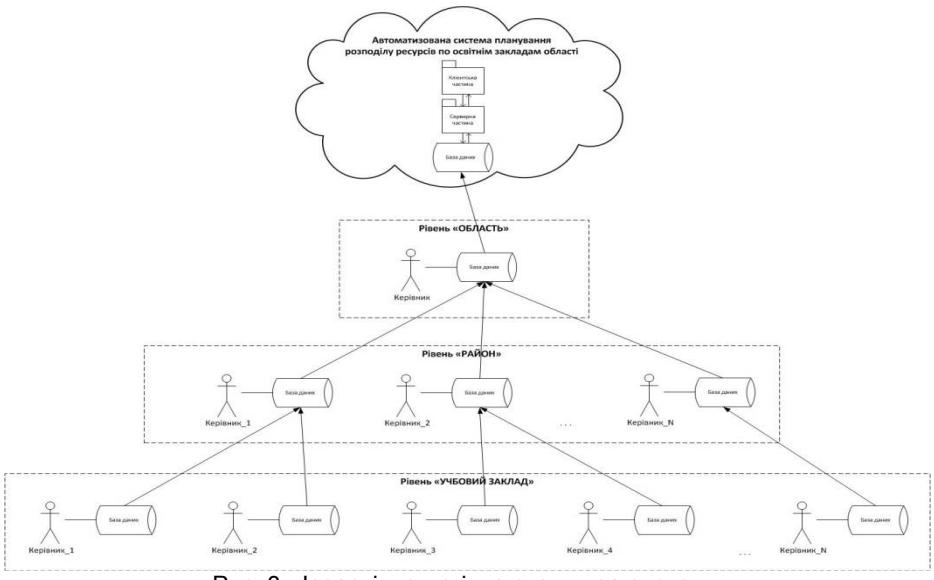

Рис. 3 - Ієрархічно-логічна структура системи

Для досягнення мети, запропоновано надавати кожному користувачеві доступ лише до тих даних, які він контролює відповідно свого службового становища. Після завершення роботи, дані оновлюються на усіх рівнях за принципом «знизу-догори». Так, якщо керівник освітнього закладу зробив певні зміни, оновлюються дані на рівні «РАЙОН», а це, в свою чергу, слугуватиме приводом для оновлення даних на рівні «ОБЛАСТЬ» та оновлення резервної бази даних. Через такий принцип оновлення даних при виході з ладу одного з вузлів на рівні N виникнуть проблеми на усіх вищих рівнях.

Розвиток ІС ОЗО призводить до змін у попередньо визначеному рівні безпеки системи. Прогноз розвитку ІС ОЗО здійснюється на основі плану інвестицій в інформатизацію освіти, програми удосконалення мережі освітніх закладів, статистичних даних щодо розвитку параметрів основних компонентів ІС, експертних оцінок тенденцій розвитку ІС, статистики порушень безпеки. На основі прогнозу розвитку і оцінювання рівня безпеки формуються рекомендації щодо розподілу ресурсів по окремим аспектам інформатизації.

Висновки. Запропонований підхід ґрунтується на особливостях обробки інформації в ієрархічних ІС. Розвиток таких систем суттєво впливає на рівень їх безпеки. Розроблений алгоритм дозволяє прогнозувати ймовірність виконання функцій системи з урахуванням невизначеності факторів розвитку.

Спсиок літератури

1. Воронин А. А. Оптимальные иерархические структуры / Воронин А. А., Мишин С. П. - М. : ИПУ РАН, 2003. - 214 с.
2. Михайлов К. М. Методологические аспекты построения информационной струкруры АСУ / К. М. Михайлов, В. С. Кокошко // Вестник ХНТУ. – 2002. – №1(14). – С. 216–221.
3. Томашевський О. М. Інформаційні технології та моделювання бізнес-процесів : навч. посіб. / О. М. Томашевський, Г. Г. Цигелик, М. Б.Вітер, В. І. Дудук. – К. : Центр учбової літератури, 2012. – 296 с.

4. Лукацкий А. В. Обнаружение атак / Лукацкий А. В. – СПб : БХВ-Петербург. – 2003. – 624 с.
5. Дубовой В. М. Підхід до визначення рівня безпеки системи, що розвивається / В. М. Дубовой, Г. Ю. Дерман // Інформаційні технології та комп'ютерна інженерія. – 2012. – №3.
6. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. - М. : ДМК Пресс, 2008. — 544 с.
7. Яковлев А. В. Криптографическая защита информации : учеб. пособие / А. В. Яковлев, А. А. Безбогов, В. В. Родин, В. Н. Шамкин. – Тамбов : Изд-во Тамб. гос. техн. ун-та, 2006. – 140 с.
8. Ворона В. А. Системы контроля и управления доступом / В. А. Ворона, В. А. Тихонов. – [Б. м.] : Горячая линия-Телеком, 2010. – 272 с.
9. Защита информации в компьютерных сетях : Практический курс : учеб. пособие / А. Н. Андрончик, В. В. Богданов, Н. А. Домуховский, А. С. Коллеров, Н. И. Синадский, Д. А. Хорьков, М. Ю. Щербаков; под ред. Н. И. Синадского. – Екатеринбург : УГТУ-УПИ. – 2008. – 248 с.
10. Додонов А. Г. Обеспечение безопасности на основе средств и механизмов повышения живучести информационных систем / Додонов А. Г., Горбачик Е. С. // Информационная безопасность. — К., 2005. — Вып.2. : Информационная политика и технологии. - С. 98–103.
11. Павский В. А. Вычисление показателей живучести распределенных вычислительных систем и осуществимости решения задач / Павский В. А., Павский К. В., Хорошевский В. Г. // Искусственный интеллект.— 2006. — № 4. — С. 28–34.
12. Курило А. П. Аудит информационной безопасности / Курило А. П., Зефиров С. Л. , Голованов В. Б. – [Б. м.] : БДЦ-пресс. – 2006. – 304 с.
13. Домарев В. В. Безопасность информационных технологий : Методология создания систем защиты. – К.: ТИД "ДС", 2002 – 688 с.

УДК 517.958.536.72

О. Г. Архипов, О. В. Любимова-Зінченко, В. А. Борисенко,
Д. Т. Близнюк

ДОСЛІДЖЕННЯ ЗМІН МЕХАНІЧНИХ ХАРАКТЕРИСТИК СТАЛІ ASTM A333 Grade 6 ПІСЛЯ ТРИВАЛОЇ ЕКСПЛУАТАЦІЇ В УМОВАХ ТРАНСПОРТУВАННЯ РІДКОГО АМІАКУ

У статті приведений результат металографічних досліджень а також аналіз впливу терміну експлуатації на ступінь зміни характеристик міцності сталі ASTM A333 Grade 6. Установлені функціональні залежності змін в часі умовної границі текучості $\sigma_{0,2}$ і комплексного показника $\sigma_{0,2}/\sigma_в$. Дж. 8.

Вступ. Старіння і деградація сталей є небезпечний і незворотній процес, що триває безперервно з початку експлуатації обладнання і апаратури. Особливо цим негативним процесам піддані частини обладнання, що працюють за значних механічних навантажень в агресивному середовищі. На поточний момент дискусійним є питання вибору характеристик і показників, що спроможні