1. *Зеликман М.И., Кручинин С.А.* Сравнительный анализ различных методов оценки эффективных доз при использовании рентгеновских - компьютерных томографов. – Мед. техника. – 2009, № 5. – С. 7-12.
2. *Євдокимов В.Ф., Огір О.С., Огір О.О.* Дослідження характеристик якості УЗ зображень та алгоритмів їх обробки // Моделювання та інформаційні технології: зб. наук. пр. – К.: ІПМЕ ім. Г.Є. Пухова НАНУ, 2017. – Вип. 80.
3. *Огир А.С., Душеба В.В., Огир Е.А.* Обработка и вывод изображений дефектов объектов и сред с помощью графических адаптеров // Моделювання та інформаційні технології: зб. наук. пр. – К.: ІПМЕ ім. Г.Є. Пухова НАНУ, 2017. – Вип. 81.
4. *Гонсалес Р., Вудс Р.* Цифровая обработка изображений. – М.: Техносфера, 2005. – 1072 стр.
5. *Стариков А.* Применение нейронных сетей для задач классификации и кластеризации. - http://www.basegroup.ru/.
6. *Уоссермен Ф.* Нейрокомпьютерная техника: теория и практика, пер. с анг. под ред. Ю.А. Зуев. – М.: Мир, 1992. – 184 с.
7. *Братко И.* Алгоритмы искусственного интеллекта на языке PROLOG. – М.: Вильямс, 2004. – 640 с.
8. *Осовский С.* Нейронные сети для обработки информации. – М.: Финансы и статистика, 2002. – 344 с.

Поступила 19.02.2018р.

УДК 004.056.52

А.М. Давиденко, Київ
О.А. Суліма, Київ

СТРУКТУРНІ ПІДХОДИ ДО МЕТОДІВ ОЦІНКИ РІВНЯ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ

Abstract. The analysis below illustrates the necessity of developing methods of assignment of access rights that would provide the necessary level of security of the information system. Structural methods based on the use of tree-like graphs representing a sequence of events that may occur in the system as a result of the action on the system of external negative factors are widely used to assess the security level. Beside this in the article is being analyzed tree faults, which reflect the processes of emergence and development of malfunctions that conditioned by the action on the system of negative factors.

Актуальність

Рівень безпеки інформаційної системі типу *IS* є важливим параметром, який повинен використовуватися не тільки у певні моменти часу функціонування *IS,* а у довільні моменти часу, що визначається функціональною необхідністю отримати значення оцінки поточного стану

системи. Завдяки цьому стає можливим активізувати деяку задачу в *IS* або перш ніж її активізувати, ініціювати засоби, що дозволяють підвищити поточне значення величини безпеки систем. Така необхідність може обумовлюватися не тільки потребою підвищення рівня безпеки. Вона також може обумовлюватися можливістю понижувати на певний період цей рівень. Необхідність пониження рівня безпеки в аспекті, наприклад, щодо полегшення доступу до системи може обумовлюватися задачами, для яких характерна висока інтенсивність звернень до системи, що не супроводжується необхідністю забезпечувати високий рівень захисту такого доступу. Така можливість для *IS* може забезпечуватися різними підходами в організації системи. Прикладом такого підходу може бути структуризація даних за ознаками, що характеризують їх конфіденційність та інші.

Постановка задачі

Доцільність не тільки підвищувати, а і понижувати рівень безпеки може обумовлюватися вартістю використання засобів захисту чи пониження рівня конфіденційності даних з метою полегшення доступу до їх використання або за рахунок опосередненого знецінення тієї чи іншої інформації. Прикладом останніх ситуацій можуть бути дані, що стосуються певних технологічних таємниць, а їх розсекречення може виявитися доцільним у зв'язку з необхідністю дискредитації неуповноваженої сторони, що використовує відповідну інформацію в корисних цілях і т.д. Це в свою чергу потребує розробку та дослідження механізмів керування рівнем безпеки. Актуальність цього для деяких випадків обґрунтовано в роботах [1–7]. Розглянемо структурні підходи оцінки рівня безпеки інформаційних систем яки використовують дерево подій та дерево несправностей.

Вирішення задачі

Приведені вище фактори ілюструють доцільність включати до інформаційних систем, у тому числі, і в системи типу *IS*, засоби оперативного управління рівнем безпеки, що в свою чергу обумовлює необхідність володіти засобами оперативної оцінки рівня безпеки. У рамках даного підходу рівень безпеки будемо розглядати в ракурсі засобів надання повноважень, які будемо приймати як засоби захисту інформації у системі. Важливими перевагами такого підходу до управління рівнем безпеки системи є наступне:

- в рамках такого підходу знижується рівень персоналізації процесів захисту, що утруднює можливість маніпуляції з даними окремими споживачами;
- вирішення задач захисту на рівні управління повноваженнями дозволяє більшою мірою акцентувати увагу на цілях, для яких передбачається використовувати ті чи інші дані;
- такий підхід дозволяє розв'язувати задачі захисту даних способом, який полягає у їх цільовій підміні, що в свою чергу дозволяє виявляти не

тільки самого інтруза, а і небезпеку, яка відповідного інтруза активізувала.

Один із таких підходів полягає у використанні графових структур, які відомі як дерева несправностей та дерева подій, які будемо позначати DN_i і DP, відповідно [8]. Використання уявлень про DN та DP ґрунтується на тому, що такі дерева відображають процес функціонування системи. При цьому не обов'язково очікувати завершення циклу процесу для виявлення несправності, а досить провести аналіз поточного стану DN_i, що дозволяє виявити несправність, яку прийнято називати первинною, оскільки вона, відповідно до логіки функціонування системи чи її фрагменту, дозволяє перейти по відповідному дереву до несправності кінцевої або вторинної, яка проявляється своїм впливом на кінцевий етап процесу функціонування системи. Тому немає необхідності чекати кінцевого прояву виникнення несправності, а достатньо на моделі DN_i промоделювати процес розвитку первинної несправності.

У більшості випадків, всі фрагменти певного процесу можуть бути апроксимованими логічними функціями. Це означає, що така модель оперує з подіями, які відбуваються в технічній або, у даному випадку, інформаційній системі таким чином, що модель відображає факт настання події. В основному, для інформаційних систем є характерною бінарна інтерпретація їх функціонування. Це ґрунтується на тому, що у довільній системі процеси, які реалізуються в окремих фрагментах, на інших етапах функціонування допускають інтерпретацію повстання або не повстання деякої події.

У рамках такого підходу можна визначити наступні положення, які визначають аналітичні можливості моделі DN і DP.

Положення 1. Окремі фрагменти функціонування системи представляються таким чином, що існує можливість детерміновано описувати функціонування на одному етапі такого процесу.

Наприклад, якщо фрагмент φ_i відображає адекватно процес функціонування, то існує логічна формула $\varphi_i(a_i) \to L_i(a_i^B)$, яка його описує. У багатьох випадках описи окремих фрагментів певного процесу не дозволяють однозначно стверджувати, що в результаті виконання фрагменту $\varphi(x_i)$ виникне деяка подія. У таких випадках використовуються ймовірнісні оцінки можливості виникнення деякого результату функціонування відповідного фрагменту. У цьому випадку виникнення події визначається деякою ймовірною величиною, яку будемо описувати у загально прийнятому вигляді $P_i(x_i)$, де $P_i(x_i)$ означає деяку ймовірність виникнення події x_i в результаті функціонування фрагменту процесу φ_i. У рамках таких моделей для їх формального опису використовується логічні функції & та V, як основні компоненти та цілий ряд різновидностей функцій логічного типу, які допускають свою інтерпретацію в бінарній множині. Наприклад, у логічному операторі виключаючої диз'юнкції вихід такої функції може приймати одне з бінарних значень, наприклад «1», лише у тому випадку, коли тільки на

одному з входів появилася подія, яка інтерпретується значенням «1». На відміну від класичної диз'юнкції V, яка допускає появу "1" на виході, коли на двох її входах є одиниці, тому, будемо використовувати для позначення виключаючої диз'юнкції символ "U". Залежно від потреб, що визначаються особливостями системи та особливостями задач, які реалізуються, можна вводити цілий ряд інших операторів, що допускають бінарну інтерпретацію.

Оскільки дерево подій на початковому етапі будується на основі інтерпретації інформаційної системи та на основі інтерпретації окремих задач, що розв'язуються в рамках системи, то відповідне дерево подій може виявлятися надмірним. У цьому випадку розв'язується задача оптимізації такого дерева, що дозволить скоротити час його аналізу. Один з таких методів полягає у визначенні найменшого перерізу дерева подій (рис. 1).

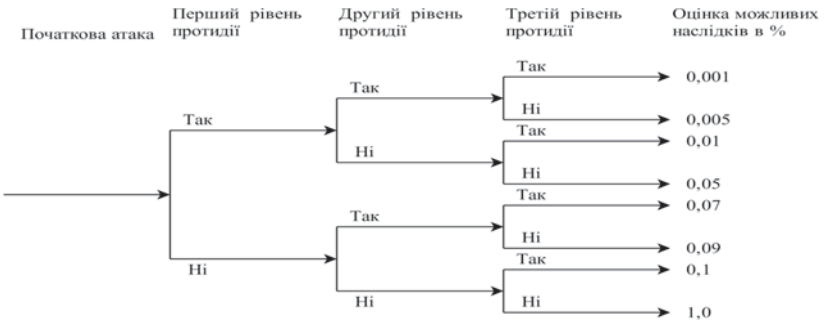

Рис. 1. Дерево подій

У межах булевої алгебри визначення найменшого перерізу ґрунтується на мінімізації булевої формули, що описує відповідне дерево. Для ілюстрації цього методу пошуку найменшого перерізу DP приймемо, що кінцева подія описується булевою формулою $f(x_1, x_2, x_3, x_4)$. Відповідно до вибраної для прикладу структури розв'язання задачі виявлення $f(x_1x_2, x_3, x_4)$ таку структуру можна описати логічною формулою:

$$f(x_1, x_2, x_3, x_4) = (x_1 + x_2)(x_1 + x_3) + (x_1 + x_4) \cdot x_1 + x_1 \cdot x_3 \qquad (1.2).$$

За допомогою відомих правил перетворень:

1) $z \cdot (x + y) = x \cdot z + y \cdot z$;

2) $x + x = x$;

3) $x \cdot x = x$,

приведену формулу для $f(x_1, x_2, x_3, x_4)$ можна перетворити у вираз:

$$f(x_1, x_2, x_3, x_4) = x_1 + x_2 \cdot x_3 + x_2 \cdot x_4$$

Цей вираз описує мінімальну логічну залежність, яка відображає залежність вихідної події $f(x_1, x_2, x_3, x_4)$ від вхідних події x_1, x_2, x_3x_4. Відповідно до отриманого опису мінімального перетину дерева DP, кінцева подія може виникнути в наступних випадках:

– при появі події x_1,

– при появі подій x_2 і x_3,
– при появі подій x_2 і x_4.

У результаті визначення мінімального перерізу дерева подій, в рамках конкретної задачі, можна перейти, до структури дерева, яке не має надмірності. Слід зауважити, що при переході до іншої задачі, необхідно повернутися до початкового дерева, оскільки в цьому випадку можуть появитися нові вхідні величини та може змінитися основна вхідна подія.

Використання дерев типу DN і DP дозволяє проводити аналіз безпеки системи не тільки у випадку детермінованих подій у процесах, що описуються деревами, а і у випадку, коли події, які описуються, носять ймовірнісний характер. В багатьох випадках буває досить складно привести систему до ситуації, коли її можна було б описувати детермінованими співвідношеннями. Для можливості проведення ймовірнісного аналізу процесів на основі використання дерев несправностей та дерев подій, необхідно пов'язати ймовірності з логічними елементами, що використовуються для побудови DN і DP. Розглянемо таку інтерпретацію на прикладі операції кон'юнкції та диз'юнкції. Для випадку операцій кон'юнкції ймовірність виникнення події на виході, при відомих ймовірностях виникнення вхідних даних, описується наступним співвідношенням:

$$\rho(a, b, \ldots, c) = \rho(a) \cdot \rho(b) \cdot, \ldots, \cdot \rho(c)$$

Приведена інтерпретація є досить простою і очевидною. Для випадку операції диз'юнкції, коли вхідні події є не залежними, ймовірність появи вихідної події описується співвідношенням:

$$\rho(a, b, \ldots, c) = \rho(a) + \rho(b) + \ldots + \rho(c) \quad (1)$$

З точки зору принципів оцінки ймовірнісних подій, для диз'юнкцій з двома входами, ймовірність вихідної події описується співвідношенням:

$$\rho(a, b) = \rho(a) + \rho(b) - \rho(a \cdot b)$$

У випадку, коли a і b статистично незалежні і добуток $\rho(a) \cdot \rho(b)$ досить малий, то $\rho(a, b) \approx \rho(a) + \rho(b)$, що обумовлює коректність використання співвідношення (1).

На основі використання моделей, що грунтуються на уявленнях про дерева несправностей та дерева подій, можна розв'язувати цілий ряд задач, які в тій чи іншій мірі, допускають інтерпретацію забезпечення того чи іншого рівня безпеки. До таких задач відносяться:

– задача оцінки інтенсивності успішності атак;
– задача оцінки безпеки при відновленні елементів, що були дискредитовані успішними атаками;
– задача оцінки безпеки при дії масових атак та інші.

На основі розв'язання приведених вище задач можна проводити узагальнені оцінки рівнів безпеки, які мають власні та досить специфічні інтерпретації. Першою з таких є оцінка по Бірнбауму. Важливість події x по Бірнбауму визначається відношенням зміни частоти успішних атак до зміни ймовірності реалізації події x, що формально описується наступним

співвідношенням:

$$B(x) = \frac{d}{dx}[P(x)]; B(x) = F(1) - F(0).$$

Величина оцінки по Бірнбауму представляє собою різницю між частотою успішних атак при виникненні події x і частотою успішних атак у випадку, коли подія x не виникла. Коефіцієнт збільшення величини ризику (RIR) показує як збільшується мінімальна верхня границя мінімальних перетинів коли ймовірність головної події збільшується і прямує до одиниці:

$$RIR = F(\lambda)/F(x).$$

Значимість по Фуселу-Веселу події x визначається як відносний вклад події в частоту успішних атак:

$$Fv = [F(x) - F(0)]/F(x),$$

де $F(x)$ – частота успішних атак при номінальному значенні ймовірності основного значення x; $F(0)$ – те ж саме, але при припущенні, що подія x не виникла.

Алгоритм обчислення величини ризику системи може полягати у наступній послідовності дій.

Ризик буде обчислюватися для окремих задач, оскільки користувача цікавить безпека співпраці з мережею в аспекті задачі, яку користувач використовує.

Кожна задача описується у вигляді дерева подій DP, множина яких описує відповідну роботу користувача.

Для всіх відомих несправностей (по відношенню до всіх станів в DP) будується дерево несправностей або відмов (DN) (рис 2).

На основі емпіричних даних обчислюється ймовірність переходу з одного стану до іншого при виникненні відповідних подій.

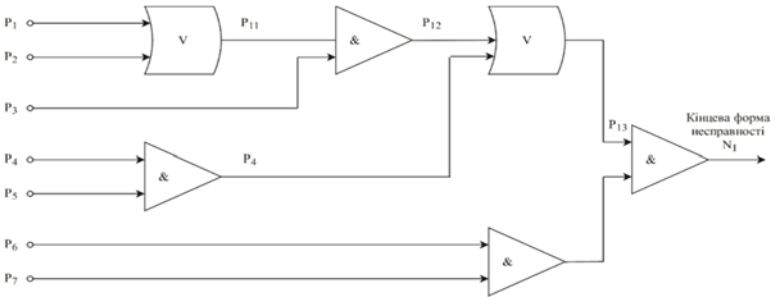

Рис. 2. Дерево несправностей

Базовим співвідношення для оцінки інтенсивності потоку несправностей або відмов є співвідношення Пуассона:

$$P(x,t) = \left(\lambda^x \cdot e^{-\lambda}\right)/x!,$$

де λ – інтенсивність відмов. Середнє значення частоти рівне $\lambda = x/t$, де x – кількість відмов за час спостереження t. Для рідких подій, в якості середнього

значення приймається оцінка $\lambda = 0{,}693/t$. Довірена границя у випадку Пуассоновських відмов визначається у відповідності із співвідношенням:

$\lambda_\alpha = -\ln(1-\alpha)/t$, де α – довірена границя ймовірностей.

Поточна у часі величина ризику локальної мережі по Бірнбауму обчислюється співвідношенням:

$$R(S) = \sum_{j=1}^{n}\sum_{i=1}^{k} RIR_j(x_i)$$

У процесі функціонування мережі, змінюється значення ймовірності $P_i(x_i)$ подій, які виникають в мережі і відображаються в DP. Залежно від виникнення атак різних типів, змінюються значення x_i в DN. Тому змінюються характеристики ризику по Бірнбауму в локальній мережі.

Для визначення рівнів безпеки можна використовувати методи, що будуються на основі Марківських моделей. Марківський процес – це процес, у якого кожний наступний стан системи залежить тільки від стану системи в момент часу t_{i-1}. Введемо наступні позначення:

- "0" – "l" - безпечні стани мережі;
- "1.1" – "$n.1$" - небезпечні стани мережі;
- $\lambda_{1.0} - \lambda_{n.1}$ - інтенсивності переходів у відповідні стани;
- $\mu_1 - \mu_l$ - інтенсивності переходів з безпечних станів в інші безпечні стани.

Інтенсивність переходів в стан "$i.0$" описуються співвідношенням $\lambda_{i.0}(i) = \lambda_i(t) \cdot Q_i(t, t_p)$, де λ – інтенсивність переходу з і-го початкового стану, $Q_i(t, t_p)$ – ймовірність виконання всіх функцій захисту в і-тому початковому стані. Інтенсивність переходу стану "$i.1$" з порушенням безпеки при і-тому початковому стані описується наступним чином: $\lambda_{i,1}(t) = \lambda_i(t)Q(t, t_p)$, де $Q(t, t_p)$ – ймовірність не виконання функції забезпечення безпеки.

Для можливості використання зазначеного підходу до моделювання рівня безпеки, з метою оперативного визначення цього рівня, необхідно представити задачі, що розв'язуються в цій системі у вигляді окремих станів систем і переходів системи з одного стану в інший стан.

Оскільки в рамках даної статті розглядаються інформаційні системи і в першу чергу, програмні засоби, які реалізують такі системи, тому доцільно розглядати параметри, що пов'язані з надійністю системи, оскільки остання, як і безпека, визначається як параметр, що характеризує здатність системи розв'язувати задачі, що передбачені технічними умовами на відповідну систему. Якщо розглядати надійність IS на зальному рівні, то можна стверджувати, що безпеку системи можна, в певній мірі, пов'язати з надійністю. Атаки, що скеровуються зовнішніми небезпеками на систему, можуть мати вищу успішність, якщо система містить в програмному середовищі похибки, які не вдалося виявити на етапах проектування та

випробування системи. Одним з базових підходів до підвищення надійності системи є перевірка її відповідності встановленим вимогам. Одним з основних підходів до реалізації таких перевірок є тестування системи програмних засобів. Атаки, що активізуються зовнішніми небезпеками, в більшості випадків, ґрунтуються на даних про систему. Тому такі данні про небезпеку, якою найчастіше виступає деяка зовнішня інформаційна система, проводить дослідження IS. У результаті використання таких даних небезпека може сформувати більш ефективну атаку. Таке дослідження може представляти собою тестування потенціального об'єкту атаки з метою виявлення слабких місць і по можливості дефектів, які могли залишитися після розробки та випробування IS [9]. У цьому випадку функції захисту в системі понині бути розширені засобами, що виявляють відповідні спроби несанкціонованого дослідження системи. Функції дослідження системи IS можуть реалізовуватися на рівні доступу до системи надання повноважень. Тому доцільно розглянути модель надійності системи програм, яка вносить свою частку в рівень безпеки відповідної системи. У зв'язку з цим розглянемо деякі моделі надійності, а також можливість їх інтерпретації з точки зору забезпечення та оцінки рівня безпеки інформаційної системи.

Одним з підходів до визначення рівня надійності інформаційної системи є підхід, що ґрунтується на оцінці можливих помилок, які могли залишитися в програмному середовищі. Тоді показником надійності програмного забезпечення служить ймовірність відсутності програмних помилок протягом певного інтервалу часу експлуатації відповідної програми. Одна з таких моделей ґрунтується на наступних припущеннях:

– загальна кількість операторів в програмі є постійна;

– в процесі відладки інформаційної системи певна кількість помилок виявляється та усувається, при цьому до системи не вносяться нові похибки;

– за сумарною кількістю виявлених помилок можна проводити оцінку кількості помилок, що залишилися;

– інтенсивність відмов системи пропорційна числу помилок, що залишилися.

В даному випадку надійність системи визначається величиною середнього періоду часу безвідмовності роботи системи, який визначається співвідношенням наступного типу:

$$T_0 = 1\big(K_s\big[E_0\big(1 - e_c(x)\big)\big]\big),$$

де K_s і E_0 – параметри моделі надійності; $e_c(x)$ – сумарна кількість помилок, що виправлені до моменту t; I – загальна кількість операторів у системі на момент часу t_0. Параметр E_0 визначається співвідношенням:

$E_0 = \{I[\gamma e_c(x_1) - e_c(x_2)]\}/(\gamma - 1)$, де $\gamma = (T_1/T_2) * (n_2/n_1) = T_{01}/T_{02}$,

де T_{01} - середній час безвідмовної роботи, який відповідає періоду відладки системи і позначається x_i. Тоді $T_{0i} = T_i/n_i$, де n_i – поточне число помилок у системі, що були виявлені у процесі відладки за період x_i. Параметр K_s

обчислюється за наступною формулою:

$$K_s = n_1/\{[(E_0/I) - e_c(x_1)]T_1\},$$

де T_1 і T_2 - час роботи системи, який відповідає інтервалам часу x_1 і x_2.

Наступна модель надійності програмної системи, як і попередня, ґрунтується на припущенні про експоненціальний розподіл часу безпомилкової роботи програмної системи. Приймається, що частота появи помилок пропорційна числу помилок, що залишилися [10]. Тоді середній час безпомилкової роботи системи визначається наступним співвідношенням:

$$T_0 = 1/\{K_{JM}[E_0 - i + 1]\},$$

де K_{JM} – коефіцієнт пропорційності; i – номер поточного інтервалу, що визначає період, через який була виявлена поточна помилка; E_0 – число помилок, що існують в програмі на початковому моменті x_0.

Наступна модель надійності програми відрізняється від попередніх тим, що припускається наступне. Частота появи помилок пропорційна не тільки кількості помилок, що залишилися, а і часу відладки програми. Така модель описується наступним співвідношенням:

$$T_0 = \left\{[\pi/2K_{SW}(E_0 - i + 1)]^{1/2} = \sqrt{\pi/2|K_{SW}(E_0 - i + 1)}\right\},$$

де T_0 – час роботи або інтервал часу роботи, який програма буде працювати без помилок; K_{SW} – коефіцієнт пропорційності.

На рівень безпеки інформаційної моделі впливає цілий ряд факторів. До них відносяться:

– модульність інформаційної системи;
– модифікація програмних засобів в процесі експлуатації інформаційної системи;
– періоди експлуатації системи та інші.

Це призвело до того, що вводяться уявлення про нескінченні моделі надійності, оскільки кількість помилок у програмі може бути нескінченна. Це пов'язано з тим, що при усуненні одних помилок можуть виникати нові. Систематична модифікація програми також призводить до можливості появи нових помилок і т.д. Тому крім загально прийнятих початкових умов, вводиться положення про те, що накопичена кількість помилок в програмі у поточний момент t описується процесом Пуассона з середнім значенням його величини, яка описується співвідношенням: $\mu(t) = \alpha t^{\beta}$, де оцінки α і β визначаються наступними співвідношеннями:

$$n/t^{\beta}; \beta = n/[\sum_{i=1}^{n-1} \ln(t_n/t_1)].$$

Приведена модель є більш близька до моделі визначення рівня безпеки, яка повинна враховувати вторгнення до системи атак.

Припущення про те, що нові помилки можуть вводитися до системи, досить добре підходить для випадків, коли атака, реалізація якої представляє собою програмний продукт, вторгається в систему. Цей факт допускає інтерпретацію, що полягає в наступному. Будь-яке вторгнення програмного інтруза до системи приводить до ефектів, які відповідають наслідкам

активізації фрагментів програм, що містить помилки.

При цьому у випадку атак, які полягають у внесенні змін до програм, можуть виявлятися не відразу, що не відповідає у більшості випадків прояву звичайних помилок в інформаційній системі.

Приведені моделі надійності можуть використовуватися певною мірою, як доповнення реалізації моделей безпеки інформаційної системи. При цьому, можна приймати положення, що допускають інтерпретації ситуацій, які виникають, при появі атаки, що здійснила вторгнення в середовище програмної системи.

Висновок

Один з поширених методів оцінки рівня безпеки інформаційних систем ґрунтується на використанні матричних моделей. У рамках такої матриці існує можливість зіставляти кожному з користувачів певні об'єкти, якими є дані, програми чи процеси, до яких цей користувач може мати відповідні повноваження. Прикладом таких повноважень можуть бути повноваження на виконання операцій читання, запису, заміни інформації та інші. Відомими є моделі надання повноважень, які використовують уявлення про класи безпеки та уявлення про категорії об'єктів.

Однією з поширених оцінок є оцінка, яка використовує уявлення про ризик зниження рівня безпеки системи. Також широко використовуються методи, що ґрунтуються на використанні експертних оцінок. У більшості з них, в якості експертів використовуються фахівці, які можуть оцінити рівень вразливості окремих засобів, можливість виникнення загрози та інші фактори. Всі ці оцінки представляються у вигляді певної таблиці, до якої впроваджуються правила її використання, що використовуються при визначенні рівня ризику.

Для оцінки рівня безпеки досить широко використовуються структурні методи, які ґрунтуються на використанні деревоподібних графів, що відображають послідовність подій, які можуть виникати в системі внаслідок дії на систему зовнішніх негативних факторів. Крім цього, використовуються дерева несправностей, які відображають процеси виникнення та розвитку несправностей, що обумовлюються дією на систему негативних факторів.

Приведений аналіз ілюструє необхідність розвитку методів надання повноважень, які забезпечували б необхідний рівень безпеки інформаційної системи.

1. *Аверченков В. И.* Системы защиты информации в ведущих зарубежных странах / В. И. Аверченков, М. Ю. Рытов, Г. В. Кондрашин, М. В. Рудановский. — Брянск : БГТУ, 2007. — 223 с.

2. *Суліма О. А.* Аналіз методів оцінок рівня безпеки доступу до даних / О. А. Суліма // Моделювання та інформаційні технології: Зб. наук. праць ІПМЕ НАН України. — 2017. — С. 80–87.

3. *Павлов І. М.* Проектування комплексних систем захисту інформації / І. М. Павлов, В. О. Хорошко. — Вінниця : ВНТУ, 2011. — 245 с.

4. *Архипов А. Е.* Практические аспекты оценивания рисков реализации угроз в информационных системах / А. Е. Архипов, А. В. Скиба // Захист інформації. — 2014. — Т. 16, № 3. — С. 215–222.
5. *Андрєєв В. І.* Основи інформаційної безпеки / В. І. Андрєєв, В. О. Хорошко, В. С. Чередніченко, М. Є. Шелест. — К. : ДУІКТ, 2009. — 292 с.
6. *Бояринова Ю. Є.* Технології захисту комп'ютерних систем і мереж / Ю. Є. Бояринова, А. Г. Корченко, И. А. Терейковский // Інформаційні технології в економіці та природокористуванні. — 2017. — Т. 1, № 1.
7. *Борботько Т. В.* Защита информации в банковских технологиях / Т. В. Борботько. — Мн. : БГУИР, 2006. — 125 с.
8. *Диллон Б.* Инженерные методы обеспечения надежности систем / Б. Диллон, Ч. Сингх. — М. : Мир, 1984. — 318 с.
9. *Барлоу Р.* Статистическая теория надежности и испытания на безотказность / Р. Барлоу, Ф. Прошан. — М. : Наука, 1984.
10. *Архипов О. Є.* Інформаційні ризики: методи та способи дослідження, моделі ризиків і методи їх ідентифікації / О. Є. Архипов, А. В. Скиба // Захист інформації. — 2013. — Т. 15, № 4. — С. 366–375.

Поступила 12.02.2018р.

УДК 004.054

С.В. Медушевський, Черкаси

ПРИКЛАД ВАЛІДАЦІЇ АВТОМАТИЗОВАНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ СЕРІЙНОЇ РЕЄСТРАЦІЇ

Abstract. The article examines the example of validation of the automated information system (AIS) serial registration. The architecture and features of the system are analyzed. A step-by-step description of the strategy and validation approach is presented. A list of standardized operational procedures for ensuring the life cycle of the AIS has been developed.

Актуальність

Фармацевтична промисловість зобов'язана ретельно документувати кожен крок в процесі виробництва лікарських засобів [1; 2]. Це одна з обов'язкових заходів, що забезпечують безпеку препарату для використання. Такі правила, як GMP в Європейському союзі (EC GMP) або Кодекс федеральних правил (CFR) органів охорони здоров'я США, вимагають реєстрації специфічної для серії інформації на всіх етапах виробництва (EC GMP і 21 CFR 11) [3].

Електронна система серійної реєстрації (EBRS) – це автоматизована інформаційна система (AIC), яка створює електронні записи серії. Проте, дана система, має більш ширший функціонал. Її можна вважати Системою