УДК 004.41:004.056

Коваленко О.В.
Центральноукраїнський національний технічний університет

АНАЛІЗ І ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

У роботі проведено аналіз основних тенденцій розвитку інформаційних технологій розробки програмного забезпечення та вимог до програмних засобів, показників і критеріїв оптимізації, а також підходів математичної формалізації відповідних інформаційних процесів та інформаційних технологій. Аналіз і дослідження, використання методів просторово-матричного представлення систем, а також єдиний підхід до конвергенції показників функціональної й інформаційної безпеки дали змогу розробити ієрархічний комплексний показник безпеки програмного забезпечення комп'ютерних систем критичного застосування, який ураховує як параметри функціональної та інформаційної безпеки, так і фактор зовнішніх впливів. У результаті формується загальна схема характеристик і показників, що стосуються якості програмного забезпечення.

Проводяться порівняльні дослідження основних підходів математичної формалізації інформаційних технологій розробки програмного забезпечення, що дають можливість сформулювати оптимізаційні задачі синтезу інформаційної технології розробки програмного забезпечення для підвищення безпеки даних. Основним завданням синтезу інформаційної технології розробки програмного забезпечення є розробка, вдосконалення та вибір моделей, методів і засобів, що забезпечують максимальні показники безпеки програмного забезпечення.

Ключові слова: *інформаційні технології, розробка програмного забезпечення, безпека програмного забезпечення.*

Постановка проблеми. Сучасний період розвитку засобів автоматизації й інформатизації суспільства загалом та окремих організацій і підприємств зокрема можна охарактеризувати як час масового переходу від стихійної комп'ютеризації окремих елементів діяльності організацій до єдиних інтегрованих рішень, що охоплює всі аспекти їх існування. Це не могло не відобразитися на складі й обсязі ІТ-проектів, які частіше за все виконуються на методах їх виконання.

Особливостями сучасних ІТ-проектів є замовлення (розробка) й експлуатація уніфікованих програмних додатків та ERP-систем; перехід до поділу праці в проектах щодо розробки ПЗ; підвищення вимог до якості ПЗ; залучення замовника в процес розробки тощо.

Динамічний розвиток цифрових технологій, зростання кількості пристроїв, підключених до Інтернету речей, прийняття закону Сарбейнса-Оксли, зміна нормативно-правового середовища, часті фінансові кризи, відмови в роботі критично важливого обладнання, терористичні атаки і зростання кіберзлочинності – лише деякі з причин, які змушують суспільство вдосконалювати свої інформаційні системи й засоби захисту програмного забезпечення. Особливо гострою ця проблематика виглядає в умовах використання комп'ютерних систем критичного застосування, вимоги до безпеки програмних засобів у яких надзвичайно високі.

Аналіз останніх досліджень і публікацій. Натепер Українське законодавство регламентує питання безпеки програмного забезпечення на підставі Закону України «Про авторське право і суміжні права» в редакції від 11 червня 2001 р. [1], а також підзаконних актів, прийнятих урядом України (ДСТУ ISO/IEC 25010 до: 2016, ДСТУ ISO/IEC 25012 до: 2016, ДСТУ ISO/IEC 25021: 2016 та ін.) [2], у яких під якістю програмного забезпечення розуміється набір ознак і властивостей програмних засобів, які характеризують здатність задовольняти встановлені й передбачені потреби. Однак, відповідно до зазначених документів, вибір метрик оцінювання якості та, відповідно, безпеки виконується суб'єктивно. Це значною мірою ускладнює процес об'єктивної оцінки якості програмного забезпечення загалом і безпеки зокрема, що, у свою чергу, знижує цінності процедур сертифікації програмного забезпечення (далі – ПЗ).

Якість ПЗ можна уявити як функцію восьми складників: підфункцій придатності (Fa), ефективності (Fe), сумісності (Fc), зручності використання (Fu), супровідності (Fes), можливості перенесення й установки (Ft), функціональної безпеки (Fr), інформаційної безпеки (Fs). При цьому

характеристика придатності є функцією показників функціональної повноти (Ffc), функціональної коректності (Ffcr), функціональної доцільності (Ffe). Показники, що характеризують ефективність, можна подати у вигляді вектора, складовими елементами якого є функції поведінки в часі (Fbt), поведінки ресурсів (Fbr), ємність (Ffca). Сумісність ПЗ – це функція, показниками якої є співіснування (Ffco) і взаємодія (Ffi). У свою чергу, характеристику «зручність використання» можна уявити як сукупність показників доцільності (Ffre), керованості (Fcon), захисту від помилок користувачів (Fum), естетичності інтерфейсу (Ffai), доступності користувачів (Ffa). Супровідність є функцією показників модульності (Ffmod), можливості повторного використання (Ffrei), можливості аналізу (Ffan), можливості модифікації (Ffmod), можливості тестування (Fftes). Можливість перенесення й установки як ще одна важлива характеристика може описуватися за допомогою показників адаптованості (Ffadp), можливості інсталяції (Ffins), можливості заміни (Ffrep).

Дослідження показали, що групу характеристик безпеки ПЗ (функціональної безпеки (Fr), інформаційної безпеки (Fs)) доцільно розглядати з погляду єдиної мети – забезпечення безпеки комп'ютерних систем критичного застосування, наявної можливості взаємовпливу один в одного. При цьому показниками функціональної безпеки є зрілість (Fmat), відмовостійкість (Ffft), відновлюваність (Frec), а показниками інформаційної безпеки є конфіденційність (Fconf), цілісність (Fint), автентичність (Fauth), доступність (Favb), причетність (Ffir) .

У роботах [3; 4] проводилися дослідження й розроблені комплексні показники якості функціонування комп'ютерних систем критичного застосування (далі – КСКЗ). Скористаємося системними підходами, представленими в цих роботах, і розробимо комплексний показник безпеки ПЗ КСКЗ.

Постановка завдання. Метою роботи є дослідження інформаційних технологій розробки програмного забезпечення, що забезпечують максимальні показники безпеки.

Виклад основного матеріалу дослідження. Проведені дослідження й аналіз показників якості ПЗ у вигляді ієрархічної векторної системи, а також показників безпеки ПЗ зокрема дали змогу представити комплексний показник безпеки ПЗ КСКЗ $Y_i^{(ПЗ)}$ у вигляді твору матриць:

$$Y_i^{(ПЗ)} = (X_{ik} \cdot Y_k) \cdot A, \qquad (1)$$

де $X_{ik} = \left[x_\psi^{(\xi)}\right]$ – матриця усереднених коефіцієнтів впливу зовнішніх процесів і факторів впливу на окремі показники безпеки ПЗ, i – кількість зовнішніх факторів, що впливають на функціонування системи, k – кількість програмних засобів ПЗ КСКЗ, $x_\xi^{(\psi)} = \frac{1}{N}\sum_{i=1}^{N} x_\ell^i$ – усереднений коефіцієнт впливу зовнішніх процесів (ψ) на показники безпеки окремих програмних засобів КСКЗ (ξ), ℓ – найменування окремого показника безпеки ПЗ, A – матриця усереднених коефіцієнтів взаємовпливу різних характеристик якості ПЗ, $Y_k = \left[\overline{Y_{mat}^{(ПЗ)}}, \overline{Y_{fft}^{(ПЗ)}}, \overline{Y_{rec}^{(ПЗ)}}, \overline{Y_{conft}^{(ПЗ)}}, \overline{Y_{intt}^{(ПЗ)}}, \overline{Y_{autht}^{(ПЗ)}}, \overline{Y_{avb}^{(ПЗ)}}, \overline{Y_{fir}^{(ПЗ)}}\right]$ – матриця показників безпеки ПЗ, $\overline{Y_{mat}^{(ПЗ)}}, \overline{Y_{fft}^{(ПЗ)}}, \overline{Y_{rec}^{(ПЗ)}}, \overline{Y_{conft}^{(ПЗ)}}, \overline{Y_{intt}^{(ПЗ)}}, \overline{Y_{autht}^{(ПЗ)}}, \overline{Y_{avb}^{(ПЗ)}}, \overline{Y_{fir}^{(ПЗ)}}$ – векторні показники безпеки ПЗ.

У результаті перемноження (вираз 1) буде сформована матриця, що являє собою комплексний показник безпеки $Y_i^{(ПО)}$ ПЗ КСКЗ.

Надалі в процесі моделювання й розробки інформаційної технології підвищення безпеки ПЗ, застосування та аналізу її структурних елементів для вирішення приватних оптимізаційних задач доцільно виставляти прапор пріоритетності на окремі елементи матриць X_{ik}, Y_k та A.

Використання методів просторово-матричного представлення систем, а також єдиний підхід до конвергенції показників функціональної й інформаційної безпеки дали можливість розробити ієрархічний комплексний показник безпеки ПЗ КСКЗ, який ураховує як параметри функціональної та інформаційної безпеки, так і фактор зовнішніх впливів.

Аналіз вимог безпеки в законодавчих і регламентуючих актах, дослідження моделі якості ПЗ, а також досвід розробки, специфіки впровадження та супроводу ПЗ дав змогу зробити висновок про значне підвищення вимог до безпеки, особливо в КСКЗ.

Натепер існує низка способів забезпечення безпеки програмного забезпечення. Серед них можна виділити способи, які стосуються обґрунтованої розробки та ефективного виконання політики безпеки, оперативного реагування на події, пов'язані з безпекою ПО, безпечного програмування тощо [5].

Усі ці способи тією чи іншою мірою повинні виконуватися відповідно до методології, що призводить до фізичного змісту інтегрального рівня безпеки (SIL – Safety Integrity Level) [6; 7]. Відповідно до цієї методології, дії, пов'язані із забезпеченням безпеки програмного забезпечення, починаються найбільш ранніх стадіях роботи над проектом і тривають протягом усього циклу розробки, причому багато дій виконуються пара-

лельно. На рисунку 1 показано, як дії, пов'язані із забезпеченням безпеки програмного забезпечення, накладаються на різні інші дії, що виконуються в процесі його розробки.

Варто зауважити, що під час розробці ПЗ дуже важливим кроком є обґрунтований вибір методології реалізації цього завдання, що дає змогу підвищити ефективність і якість програмного продукту. При цьому необхідно враховувати, що сукупність процесів розробки ПЗ є складною багатофакторною системою проходжень етапів у рамках обраної методології. Аналіз літератури [8; 9] показав, що сучасні методології розробки ПЗ можна розділити на три основні групи: послідовні (прогнозовані), циклічні (напівпрогнозовані), гнучкі (абстрактні).

Рис. 1. Діаграма операцій забезпечення безпеки в циклі розробки програмного забезпечення

Основні відмінності між гнучкими й послідовними методологіями розробки ПЗ представлені на рисунку 2. При цьому варто зауважити, що філософія Agile включає в себе різні принципи та правила, об'єднані між собою в один документ (маніфест Agile). На рисунку 2 виділені тільки основні правила.

Сьогодні існує безліч підходів математичного моделювання процесу розробки програмного забезпечення. Їх основою є положення теорії системного аналізу, масового обслуговування, нейронних мереж, нечіткої логіки, графових моделей і комбінаторних методів розрахунку тощо [8; 10]. Крім того, набули свого розвитку засоби рішення оптимізаційних задач, що формалізуються на основі даних моделей. Це передусім аналітичні методи, методи математичного програмування, евристичні методи тощо [8]. Проаналізуємо найбільш часто використовувані на практиці моделі розробки ПЗ, які різною мірою адаптовані до сучасних вимог до безпеки під час формалізації процесів управління розробкою.

На початку виділимо, що нині в теорії системного аналізу виділяють низку напрямів, серед яких виділимо напрями якісного й кількісного аналізу різних технічних систем і процесів. При цьому якісний аналіз характеризується простотою та високою швидкістю реалізації, а кількісний аналіз – точністю.

Для опису поведінки керованих процесів (у тому числі й процесу розробки ПО) з дискретною безліччю станів і безперервним часом широко використовується теорія марковських процесів. Якщо при цьому закони розподілу тривалості перебування в кожному зі станів до відходу в інший можливий стан не є експонентними, то адекватною моделлю поведінки системи є напівмарковський процес [11].

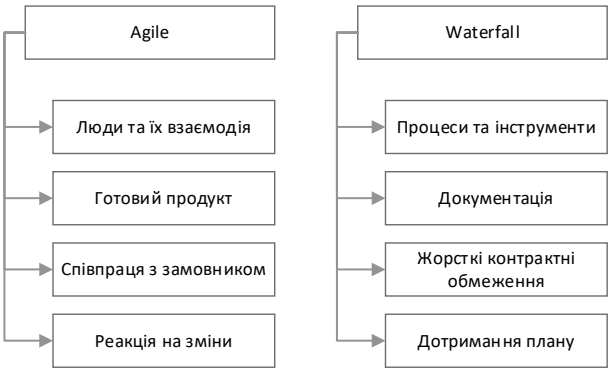

Рис. 2. Основні відмінності між гнучкими та послідовними методологіями

Традиційні технології аналізу напівмарковських систем обмежуються розрахунком фінального розподілу ймовірностей станів системи за формулами:

$$P_i = \frac{\pi_j \overline{T}_j}{\sum_{j=1}^{n} \pi_j \overline{T}_j}, \quad i = 1,2,..,n,$$

де n – число можливих станів системи,

$$\bar{T}_j = \int_0^\infty (1 - F_i(t))dt = \int_0^\infty (1 - \sum_{j=1}^{n} P_{ij}F_{ij}(t))dt$$

– середній час перебування в стані i до відходу, ${}^c\pi_i$ – стаціонарна ймовірність перебування в стані i, i=1,2,...,n, набір яких знаходиться шляхом вирішення векторно-матричного рівняння

$$(\pi_1, \pi_2, .., \pi_n) = (\pi_1, \pi_2, .., \pi_n)\begin{pmatrix} P_{11} & P_{12} & .. & P_{1n} \\ P_{21} & P_{22} & .. & P_{2n} \\ .. & .. & .. & .. \\ P_{n1} & P_{n2} & .. & P_{nn} \end{pmatrix}.$$

Якщо, крім фінальних імовірностей для дослідження системи, необхідне знання будь-яких тимчасових характеристик її поведінки (наприклад, закон розподілу тимчасового інтервалу до потрапляння в який-небудь стан системи), то для вирішення відповідних завдань використовується апарат інтервально-перехідних імовірностей [10; 11]. Напівмарковський процес, як відомо, відрізняється від марковского тим, що закон розподілу часу перебування в кожному зі станів не є обов'язково експоненціальним, а може бути довільним. Ці фактори доцільно використовувати при кількісній оцінці ризиків розробки ПЗ для розробки оптимізаційної стратегії прийняття рішень.

Одним із сучасних напрямів математичного моделювання є біологічний напрям з допомогою нейронних мереж [12]. Багато в чому це пов'язано зі специфікою функціонування комп'ютерних систем, які є людино-машинними системами. Крім того, останнім часом усе більшу увагу розробники та проектувальники стали приділяти питанням захисту даних від програмних загроз. А в цьому випадку результати дослідження систем, проведені за допомогою біологічного підходу, показують найбільш адекватні результати.

Однак проведені дослідження моделей комп'ютерних систем, представлених у вигляді нейронних мереж [12–14], поряд з їх достоїнствами показали й недоліки, пов'язані з істотними (до 100 спостережень) тимчасовими витратами на процес навчання під час побудови моделі, як наслідок, «консерватизмом» щодо динамічних змін у процесі управління розробкою системного ПЗ. Тому ці моделі доцільно використовувати під час моделювання окремих компонентів або структурних елементів інтелектуальних систем прийняття рішень або використовувати в основі процесу вироблення практичних рекомендацій менеджерам.

Однією з поширених технологій математичної формалізації процесів, що протікають у технічних системах, є технологія автоматного моделювання. В автоматизованій моделі управління технологія розробки системного ПЗ представляється детермінованим автоматом, на вхід якого надходить послідовність команд користувачів. Основними елементами автоматизованої моделі може бути безліч станів системи $\{V\}$, безліч користувачів $\{U\}$, безліч матриць доступів $\{M\}$, безліч команд користувачів, що змінюють матрицю доступів $\{CC\}$, безліч команд користувачів, що змінюють стан $\{VC\}$, безліч вихідних значень $\{Out\}$ [8; 13].

Перевагою цієї технології є можливість відображення різних підходів управління, що визначають не тільки архітектуру системи, а й конфігурацію, порядок взаємодії між об'єктами та суб'єктами процесу розробки ПЗ.

Серед недоліків автоматних моделей можна відзначити складність їх практичної реалізації в разі збільшення використовуваних підходів і методологій розробки системного ПЗ.

Як зазначено в низці джерел [10; 11; 15], домінуючим під час вирішення широкого кола завдань аналізу й синтезу систем управління різного призначення тривалий час залишався графокомбінаторний підхід. У цьому випадку процес розробки ПЗ представляється у вигляді функції: $G(N, C)$ або $G(\mathrm{x})$, де N – безліч станів в управлінні, C – безліч зв'язків між станами, x – характеристика якості управління (ефективність, безпеку, вартість тощо), обрана як критерій оптимізації. Тоді приватна задача розробки системного програмного забезпечення може трансформуватися в оптимізаційну задачу виду: $G(x) \to opt$.

Рішення мережевих завдань управління в рамках цього підходу ґрунтувалося на моделюванні процесу у вигляді графа й пов'язане з направленим перебором можливих варіантів з метою досягнення деякого оптимуму щодо аналізованого властивості.

Одним із можливих методів математичного графового уявлення процесу розробки ПЗ є метод, заснований на GERT-мережах. Цей метод дає змогу моделювати процеси із заздалегідь невідомою функцією розподілу випадкових величин, успішно випробуваний під час математичної формалізації низки процесів, пов'язаних із проектуванням і тестуванням програмного забезпечення, що висвітлено в роботах [16; 17].

Результати, отримані під час моделювання таких процесів, показали можливість використання цього підходу з урахуванням можливих

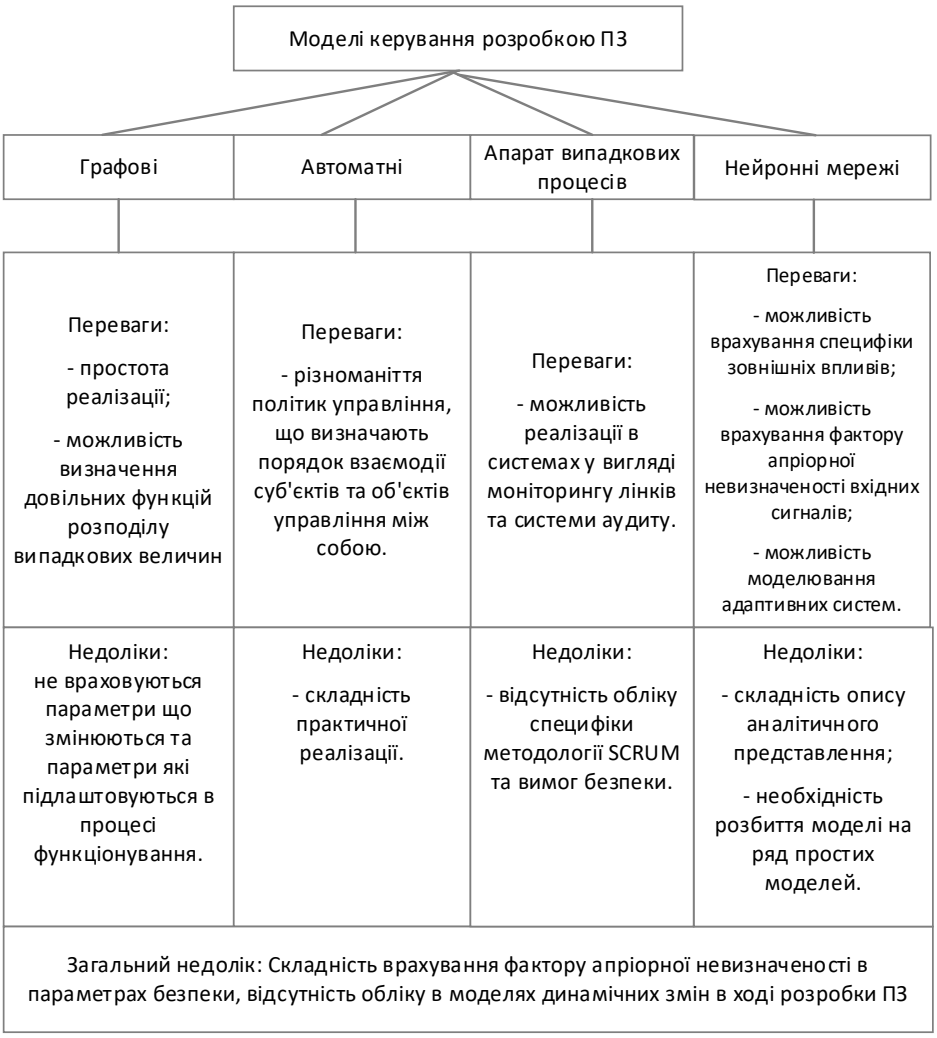

Рис. 3. Порівняльна характеристика найбільш відомих підходів математичної формалізації процесу управління розробкою системного ПЗ

негативних ситуацій і наслідків. Зокрема, аналіз GERT-моделей показав доцільність еквівалентних спрощують перетворень складних процесів, розбиття складних етапів на низку підетапів, використання відомого математичного апарату (наприклад, формули Мейссоньє, леми Жордана) тощо.

На рисунку 3 представлено порівняльну характеристику найбільш відомих підходів математичної формалізації процесів управління розробкою із зазначенням їх достоїнств і недоліків.

Отже, в результаті аналізу й порівняльних досліджень наявних моделей процесу розробки ПЗ виявлено низку характерних особливостей, переваг і недоліків наявних напрямів аналізу та синтезу цих систем.

Проведені дослідження наявних інформаційних технологій і методологічного забезпечення процесу розробки ПЗ, методів і засобів управління цим процесом, а також технологій математичної формалізації дали змогу виявити низку недоліків та обмежень їх використання в умовах підвищеного інтересу до ПЗ у зловмисників і високих вимог безпеки. Ці результати характеризують об’єктивно існуюче протиріччя розвитку інформаційних технологій розробки програмного забезпечення в умовах наявної філософії Agile та гнучких методологій розробки ПЗ.

Це дало змогу зробити висновок про необхідність урахування низки негативних факторів, що впливають на безпеку інформації, під час розробки та реалізації інформаційної технології розробки ПЗ.

Проведені дослідження показали, що існує широкий спектр варіантів розробки й використання інформаційних технологій управління розробкою ПЗ. Ці варіанти можуть відрізнятися способами впровадженнями, вартісними й іншими

тактико-технічними показниками, характеристиками її окремих елементів тощо [4].

Безліч можливих варіантів побудови інформаційної технології розробки ПЗ Θ може бути представлено у вигляді об'єднання підмножин $\tilde{\Theta}$ і Θ, що забезпечують безпеку на всіх етапах життєвого циклу розробки ПЗ й не забезпечують заданий показник якості відповідно.

Основним завданням для вирішення науково-технічної проблеми, яка полягає в синтезі інформаційних технологій розробки ПЗ КСКЗ для підвищення безпеки даних, є розробка, вдосконалення та вибір інформаційних технологій, методів і моделей, що належать до підмножини й забезпечують максимальні показники безпеки ПЗ.

Під час розробки інформаційної технології якісного аналізу необхідно зазначити, що основою для розробки є методика структурної ідентифікації ризиків розробки ПО, що відрізняється від відомих побудов оцінювання ризиків, розробки ПЗ «зверху» у вигляді безлічі за наявності довільного несуперечливого кінцевого набору «квантів інформації».

Під час розробки комплексу математичних моделей технології тестування Web-додатків необхідно виділити такі окремі наукові завдання: розробка та дослідження математичних моделей технології тестування DOM XSS уразливості й технології тестування уразливості до SQL ін'єкцій, оцінювання ефективності та адекватності розробленого комплексу математичних моделей.

Висновки. У статті проведено аналіз сучасних тенденцій розвитку інформаційних технологій розробки програмного забезпечення та вимог до програмних засобів, показників і критеріїв оптимізації, а також підходів математичної формалізації відповідних інформаційних процесів та інформаційних технологій.

Проведені аналіз і дослідження дали змогу сформувати ієрархічний показник вимог до якості ПЗ КСКЗ, виділити в ньому вимоги до безпеки. У результаті сформована загальна схема характеристик і показників, що стосуються якості програмного забезпечення.

Аналіз інформаційних технологій і методологій розробки програмного забезпечення, а також факторів, що впливають на безпеку, дав можливість виділити протиріччя між підвищеними вимогами до безпеки ПЗ (з урахуванням усіх ризиків безпеки) і необхідністю адаптації до наявних об'єктивно-суб'єктивних факторів, властивих сучасному світу ІТ-індустрії.

Проведені порівняльні дослідження основних підходів математичної формалізації інформаційних технологій розробки ПЗ дали змогу сформулювати оптимізаційну задачу синтезу інформаційної технології розробки ПЗ для підвищення безпеки даних. Основним завданням синтезу є розробка, вдосконалення та вибір моделей, методів і засобів, що забезпечують максимальні показники безпеки ПЗ.

Список літератури:

1. Про авторське право і суміжні права: Закон України від 11.06.2001 № 2627-III. Дата оновлення: 22.07.2018. URL: http://zakon.rada.gov.ua/laws/show/3792-12.
2. Каталог на Україні: URL: http://csm.kiev.ua/.
3. Яковина В.С., Федасюк Д.В., Мамроха Н.М. Аналіз використання аспектно-орієнтованого програмування як засобу підвищення надійності програмного забезпечення. Інженерія програмного забезпечення. 2010. № 2. С. 24–29.
4. Wang Y. Software engineering foundations. A software science perspective. Auerbach Publications, 2008. 1419 p.
5. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. Киев: Свифт, 2001. 680 с.
6. Mitchell K., Longendelpher T., Kuhn M. Safety Instrumented Systems Engineering Handbook. USA, 2010. 562 p.
7. Marszal E. Safety Integrity Level Selection – Systematic Methods Including Layer of Protection Analysis. The Instrumentation, Systems, and Automation Society. Research Triangle Park. USA, 2002. 136 p.
8. Говорущенко Т.О., Красій А.В. Математичне моделювання специфікації вимог та характеристик програмного забезпечення. Радіоелектронні і комп'ютерні системи. 2014. № 5. С. 34–39.
9. Ambler W. Agile Model Driven Development (AMDD): The Key to Scaling Agile Software Development. 2007. URL: http://www.agilemodeling.com/essays/amdd.htm.
10. Мхитарян В.С., Шишов В.Ф., Козлов А.Ю. Теория вероятностей и математическая статистика: учебное пособие для студ. учреждений высш. проф. образования. Москва: Академия, 2012. 416 с.
11. Praba B., Sujatha R., Srikrishna S. A study on homogeneous fuzzy semi-Markov model. Applied Mathematical Sciences. 2009. № 3 (50). P. 2453–2467.

12. Хайкин С. Нейронные сети. Москва: Вильямс, 2006. 1103 с.

13. Головко В.Л. Нейронные сети: обучение, организация и применение. Москва: ИПРЖР, 2001. Кн. 4 / под ред. А.И. Галушкина. 645 с.

14. Пильгун В.М. Глубинное обучение нейронных сетей и достижения в их применении. Киев, 2015. 589 с.

15. Смірнов О.А., Коваленко О.В., Мелешко Є.В. Інженерія програмного забезпечення: навчальний посібник. Київ: РВЛ КНТУ, 2013. С. 409

16. Коваленко А.В. Технология тестирования DOM XSS уязвимости. Безпека інформації. 2017. № 2 (23). С. 73–79.

17. The mathematical model of the testing technology for DOM XSS vulnerabilities / O. Kovalenko, O. Smirnov, A. Kovalenko, S. Smirnov, V. Vialkova. Scientific & practical cyber security journal (SPCSJ). Georgia. Tbilisi: SCSA, 2018. № 2 (1). P. 22–28. URL: https://journal.scsa.ge/issues/2018/03/997.

АНАЛИЗ И ИССЛЕДОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

В работе анализируются основные тенденции развития информационных технологий разработки программного обеспечения и требования к программным средствам, показателям и критериям оптимизации, а также подходов математической формализации соответствующих информационных процессов и информационных технологий. Анализ и исследования использования методов пространственно-матричного представления систем, а также единый подход к конвергенции показателей функциональной и информационной безопасности позволили разработать иерархический комплексный показатель безопасности программного обеспечения компьютерных систем критического применения, который учитывает как параметры функциональной и информационной безопасности, так и фактор внешних воздействий. В итоге формируется общая схема характеристик и показателей, относящихся к качеству программного обеспечения.

Проводятся сравнительные исследования основных подходов математической формализации информационных технологий разработки программного обеспечения, что позволяют сформулировать оптимизационную задачу синтеза информационной технологии разработки программного обеспечения для повышения безопасности данных. Основной задачей синтеза информационной технологии разработки программного обеспечения является разработка, совершенствование и выбор моделей, методов и средств, обеспечивающих максимальные показатели безопасности программного обеспечения.

Ключевые слова: *информационные технологии, разработка программного обеспечения, безопасность программного обеспечения.*

ANALYSIS AND RESEARCH OF INFORMATION TECHNOLOGIES FOR SOFTWARE DEVELOPMENT

This paper analyzes the main trends of development of software development information technology and software requirements, indicators and criteria of optimization and approaches of mathematical formalization of relevant information processes and information technology. On the basis of analysis and research the use of methods of space-matrix system representation as well as a common approach to the convergence of indicators of functional and information security allowed to develop a hierarchical complex indicator of security of computer systems of critical application that takes into account both the parameters of functional and information security, and the factor of external influences. As a result, a general scheme of characteristics and indicators relating to the quality of software is formed.

This research carries out comparative studies of the basic approaches of the mathematical formalization of information technology software development, which allow us to formulate the optimization problem of synthesizing the information software development technologies to enhance data security. The main task of synthesizing information technology for software development is the development, improvement and selection of models, methods and tools that provide maximum software security indicators.

Key words: *information technology, software development, software security.*