УДК 004.056.52

О.А. Суліма, м. Київ

АНАЛІЗ ВПЛИВУ ПАРАМЕТРІВ ДАНИХ НА ПРОЦЕСИ НАДАННЯ ПОВНОВАЖЕНЬ

Abstract. Analyzes the processes of changes in the overall security of the system depending on different factors such as the accuracy of the input task the accuracy implementation of the algorithm in relation to the requirements of that describe the features of their use.

Актуальність

В роботах [1 – 3] обґрунтовано актуальність, поставлено та розв'язано задачу, розроблення технології адаптивного захисту систем доступу до мережевих інформаційних ресурсів. Основу технології складають модельні описи поточної поведінки споживачів послуг комп'ютерної мережі та методи динамічного налаштування параметрів систем захисту інформаційних ресурсів для підтримки бажаного рівня їх захищеності від шкідливих дій споживачів.

Актуальною є задача розширення функціональних можливостей даної технології за рахунок побудови додаткових критеріїв враховуючих міри таємності, значимості та обґрунтованості використання даних.

Постановка задачі

Алгоритм надання повноважень (ANP) реалізує всі операції, які є необхідні, при реалізації процесу доступу до таємних даних. Користувач, після отримання доступу до системи, вводить необхідні дані про задачу Za_i і фрагменти алгоритму її реалізації, які потребують таємну інформацію, для своєго функціонування. Таким чином, не залежно від користувача, задача Za_i безпосередньо ідентифікується в системі надання повноважень, для отримання даних. Запит потрібних даних представляє собою текстові описи їх інтерпретації $D_w^z = [x_i^z, \dots, j(x_{ik}^z)]$. Система надання повноважень (SNP) вміщає крім самих даних не тільки їх значення , а і інтерпретаційні описи цих даних $D_i^s = [j(x_1^s), \dots, j(x_m^s)]$. Система SNP по $j(x_1^s)$ визначає відповідні дані $j(x_{i1}^s)$. На основі інтерпретаційного опису $j(x_i^z)$ система визначає відповідні параметри даних. Наприклад, якщо має місце $\sigma[j(x_1^s) * j(x_i^z)]$, які семантично відрізняються більше ніж на δσ, то пошук даних продовжується. Якщо серед всіх даних типу r_i^t вибрано дані, що задовольняють вимогам вибору, то встановлюються базові параметри даних.

До таких параметрів відносяться наступні параметри даних:

- міра таємності даних $r_i^{kt}(x_i)$;
- міра значимості даних $\aleph_i(x_i)$;
- міра обґрунтованості використання даних $\lambda_i(x_i)$;

Проаналізуємо їх вплив на SNP та державну інформаційну систему (DIS)

якої вона належить.

Вирішення задачі

Перевірка параметру $\lambda_i(x_i)$ дозволяє викрити системі SNP спробу несанкціонованого вибору даних $r_i^{kt}(x_i)$. Якщо в результаті семантичного аналізу $\sigma[j(x_1^s) * j(x_i^z)]$ вибрано деякі дані $[r_i^{kt}(x_i^z) * r_i^{kt}(x_i^s)]$, то перевіряється параметр таємності Za_i, якщо ці параметри відрізняються більше ніж на задану величину $\Delta(r_i^{kt})$, то повноваження відповідній Za_i на отримання даних не надаються. Параметр $\aleph_i(x_i^s)$ в процесі функціонування державної інформаційної системи (DIS) змінюється, оскільки він визначається частотою його використання на заданому інтервалі часу ΔT. Міра відмінності між $\aleph_i(x_i^z)$ та $\aleph_i(x_i^s)$задається величиною $\Delta\aleph_i$. Перевірка параметру $r_i^{kt}[x_i(x_i^z)]$ є специфічна, оскільки, для його визначення, використовується дані отримані в результаті використання $r_i^{kt}[x_i(x_i^s)]$ задачею Za_i, які розміщаються в описі цілі розв'язку задачі $C(Za_i)$.

В процесі перевірки умов надання повноважень Za_i, може виявитися, що $r_i^t(x_i^z) \neq r_i^t(x_i^s)$ і більше ніж на $\sigma(r_i^t)$. В цьому випадку, система SNP може вибрати дані, які відповідають вказаному значенню параметра r_i^t, при умові, що $r_i^t(x_i^z) \ll r_i^t(x_i^s)$, де знак $\ll$ означає нижчий діапазон значень таємності даних. Після цього, SNP перевіряє, чи $C_i[Za_i(r_i^{*t}(x_i))]$ відповідає цілі, що задана в параметрах задачі. Якщо така відповідність існує, то задача отримує по цьому параметру дозвіл на використання даних, в яких $[r_i^{kt}(x_i)\&(k \ll m)]$, де k – рівень діапазону таємності, який вибрала система SNP, m – рівень діапазону таємності, який замовляла задача. Така ситуація є можливою, оскільки текстова інтерпретація даних $j(x_i^z)$, які замовляються Za_i, не відповідає в повній мірі текстовій інтерентитації $j(x_i^s)$, яка розміщається в системі. Така невідповідність може привести до того, що дані будуть вибрані з нижчого діапазону таємності.

Така ситуація може обумовлюватися наступними причинами:

- рівень таємності в DIS для даних x_i^z міг зменшитися в силу різних відомих причин;
- інформація про дані у користувача може бути не точна, оскільки предметна область інтерпретації, якою є соціальне середовище описується з певним наближенням.

При виборі даних, за якими звернулася задача до системи SNP, остаточне рішення по наданню тих, чи інших даних, SNP приймається на основі даних аналізу всіх контрольованих параметрів, якими є $\{r^t, \aleph_i, \lambda_i\}$

Система SNP, при наданні повноважень Za_i, реалізує не тільки аналіз параметрів даних, а і аналіз параметрів самої задачі Za_i. Першим параметром, який перевіряється, є параметр суперечності цілі розвязку задачі з іншими компонентами, що надаються користувачем, при пред'явлені задачі. Компоненти представляють собою логічний опис з відповідним їх наближенням. Наприклад, компонентами можуть бути алгоритм задачі $Al_i \in$

Za_i, ціль задачі, якщо остання представляє собою деяку конструкцію, наприклад створення деякого фрагменту для W_i, то такою компонентою є логічний опис цієї конструкції або параметри вихідних даних, якщо ціль $C_i(Za_i)$ передбачає тільки перетворення вхідних даних. Наявність суперечності свідчить про неконкретне формулювання задачі і тоді, SNP відмовляє у наданні повноважень до використання даних.

Міра таємності задачі повинна бути узгоджена з мірами таємності вхідних даних D_w і особливо, вихідних даних (D_ϑ). Очевидно, що $r^t(D_w) \geq r^t(D_\vartheta)$. В більшості задач Za_i, що стосуються соціальних середовищ виконується приведене співвідношення. На величину $r^t(D_v)$ впливає такий фактор як міграція даних $(Im(x_i))$, з входу $Al(Za_i)$ до виходу процесу розв'язку задач, яким є $C_i(Za_i)$. Міграція полягає у збереженні ключових елементів опису інтерпретації даних $I(D_w) = j(x_s^w), \dots, j(x_m^w)$ по відношенню до $I(D_v) = j(x_i^v), \dots, j(x_k^v)$. Очевидно, що рівності $I(D_w)$ і $I(D_v)$ досягнути не можливо, але міра відповідності цих двох компонент визначає величину міграції інформації в процесі розв'язку задачі Za_i. Можна було б припустити, що об'єднання даних з різними параметрами таємності, приведе до того, що міра таємності результату буде вища. Ця обставина визначається на основі інтерпретації алгоритму розв'язку задачі і задається параметром міри таємності самої задачі $r^t(Za_i)$. Цей параметр перевіряється системою SNP і враховується, при наданні повноважень доступу до даних. Автор програми повинен сам визначати міру таємності самої програми, яку він проектує. Обгрунтування міри таємності для програми по аналогії з мірою таємності даних пов'язане з аналізом величини втрат, до яких може привести несанкціоноване використання такої програми. При такій інтерпретації визначення міри таємності спроектованої задачі або спроектованого алгоритму, слід визначати по величині втрат до яких може привести несанкціоноване використання розвязку задачі. Виходячи з цього, можна було б ввести інтегральний критерій вибору задач, які не потребували б для своєї характеристики параметру таємності. Але в цьому випадку може виникати протиріччя, яке полягає у наступному. Дані, що можуть потребувати параметр таємності, виникають не завжди в результаті діяльності людини, а можуть виникати в окремих випадках на основі досліджень в галузях природничих наук. Наявність такого типу таємних даних обумовлює можливість, а у багатьох випадках і необхідність створювати алгоритми і розв'язувати задачі, які необхідно характеризувати параметрами таємності.

Значимість задачі в рамках SNP визначається порівняно просто. Проводиться аналіз величини змін, які переважно описуються в цілі задачі $C_i(Za_i)$, які відбудуться в W_i в результаті використання розв'язку Za_i. Величина змін визначається по кількості елементів x_i, які будуть впроваджені, $m^x(x_i)$ в W_i, по кількості процесів, які будуть впроваджені в W_i, або $m^p(Pr_i)$, по кількості аномалій, які будуть ліквідоввуатися в W_i, в результаті розв'язку задачі, $m^a(An_i)$ та по кількості критичних ситуацій, які

передбачається ліквідувати в результаті розв'язку Za_i, або $m^K(Kr_i)$. Кожний з коефіцієнтів m^x, m^p, m^a та m^k має власне значення, або вагу, яка відображає значимість результатів розв'язку Za_i для функціонування W_i. Така значимість змінюється у відповідності із співвідношенням $m^x < m^p < m^a < m^k$. У випадку коефіцієнтів m^x та m^P мова може йти не тільки про збільшення x_i та m^P, а і про зменшення їх в W_i, якщо це не приведе до зменшення параметру актуальності $Ak(Za_i)$ відповідної задачі. Якщо в рамках однієї задачі реалізуються зміни кількості x_i в W_i, зміни кількості $Pr_i \in W_i$, чи елімінація An_i, то значення параметру $\aleph(Za_i)$ визначається наступним співвідношення: $\aleph(Za) = m^x + m^{Pr} + m^a$.

В більшості випадкі, в елімінація критичних ситуацій Kr_i реалізується окремими Za_i, оскільки такі задачі в рамках системи $(DIS\&W_i)$ мають найвишчий пріоритет.

Актуальність задачі $Ak(Za)$, для своєго визначення, потребує додаткових даних про W_i в DIS. Одним з класів таких даних є критерії прогресивності змін, до яких приводить використання результатів Za в W_i. Критерії прогресивності змін в W_i можна отримувати на основі використання еволюційних моделей [4], прикладом якої може служити модель, що використовує генетичні алгоритми [5]. По своїй природі DIS є базою даних і, тому вводити в DIS алгоритми типу генетичних не достатньо коректно. У зв'язку з тим, приймемо критерії, якими будемо визначати прогресивність кожної окремої задачі, яка використовує таємні дані.

Перш ніж формулювати критерії, підкреслимо, що всі дані, які знаходяться в DIS є елементами W_i, яку DIS обслуговує. Результати процесу розв'язку задачі Za_i можуть бути елементами, які будуть включатися в склад W_i і відповідно, будуть розширяти DIS_i. Формулювання критеріїв, переважно полягає у порівнянні, що найменше двох факторів і на основі такого порівняння реалізується вибір одного з факторів.Система DIS_i вміщає дані з W_i, яке є джерелом вхідних даних, що може використовуватися при порівнянні, для формування критеріїв. Передбачувані результати розв'язку задачі описуються в певному наближенні в описі цілі задачі. Тоді, критерії можуть ґрунтуватися на результатах аналізу цілі задачі та даних, що отримані в результаті її розвязку і порівнянні даних отриманих результатів аналізу. Сформулюємо ряд критеріїв та обґрунтуємо їх доцільність.

Критерій 1. Якщо в результаті перетворень, які реалізуються алгоритмом $Al_i(Za_i)$ задачі Za_i рівень таємності вихідних даних є нижчий у порівнянні з рівнем таємності вхідних даних, то відповідні перетворення і, відповідно Za_i можна вважати актуальною.

У відповідності з прийнятими положеннями, необхідність використання таємних даних обумовлюється тим, що останні можуть бути використані для реалізації негативного впливу на W_i, наприклад, для формування в W_i аномалій $An_i(W_i)$. Зниження рівня таємності даних, як і зменшення кількості таємних даних, які описують деяку W_i допускає інтерпретацію відповідних

перетворень, як прогресивних, оскільки такі зміни в даних приводять до зменшення можливості реалізації негативного впливу на W_i і, відповідно на DIS.

Критерій 2. Якщо результатом розв'язку Za_i є нове правило перетворень, що передається в W_i, яке не приводить до суперечності в існуючій системі правил перетворень, то відповідну задачу Za_i можна вважати актуальною.

У будь-якому середовищі, або достатньо складному об'єкті завжди реалізуються ті, чи інші процеси, особливо, коли мова йде про соціальні середовища, на обслуговування яких орієнтована система DIS. Процеси реалізуються на основі використання перетворень, система яких повинна бути не суперечна. Якщо система правил перетворень розширюється новим перетворюванням, яке не приводить до виникнення суперечності у відповідній системі, то останнє сприяє можливості функціонального розширення існуючих процесів і може сприяти можливості реалізації нових процесів. Розширення асортименту можливих процесів, що відбуваються в W_i допускає інтерпретацію еволюційного розвитку відповідної системи.

Критерій 3. Якщо, в результаті передачі розв'язку задачі Za_i в систему W_i, в останній елімінується аномалія, то така задача приймається актуальною.

Цей критерій не потребує додаткових коментарів, а його використання та виділення в окремий критерій ґрунтується на тому, що аномалія $An_i(W_i)$ може існувати в W_i і певний час не приводити до порушень в текучі моменти процесу функціонування. Тому, відповідна задача визначається як актуальна.

Критерій 4. Якщо в результаті розв'язку задачі Za_i, до W_i додається деяка компонента $\varphi_i(x_{is}, \dots, x_{ik})$, яка представляє собою деяку структуру, що не є супечною із структурами вхідних даних Dw_i та структурами предметної області W_i, то відповідна задача Za_i допускає інтерпретацію актуальної задачі.

Додавання до системи W_i, яка має власну структуру, деякої компоненти $\varphi_i(x_{is}, \dots, x_{ik})$, яка не приводить до виникнення в W_i суперечності, не тільки збільшує кількісно предметну область W_i, а і розширює її функціональні можливості, оскільки додаткова структура також може приймати участь у процесах функціонування, які уже реалізуються в W_i і тим самим їх змінювати,або їх модифікувати.Такі зміни в W_i допускають інтерпретацію прогресивних, еволюційних змін і тому, відповідна задача може характеризуватися як актуальна в рамках W_i.

Слід відмітити, що параметр актуальності задачі $Ak(Za_i)$ має дискретний характер, що виникає з приведених критеріїв, це означає, що цей параметр може інтерпретуватися як величина, значення якої визначається, на деякому неперервному інтервалі. У випадку критерія 1 величина $Ak(Za_i)$ може вимірюватися кількістю таємних компонент, для яких був знижений рівень таємності. У випадку критерія 2 актуальність вимірюється кількістю нових правил перетворень, які сформувалися в результаті розв'язку задачі

Za_i, яких може бути більше одного. Тоді $Ak(Za_i)$ визначається на інтервалі, який описує максимальну кількість можливих правил перетворень.

У випадку критерія 3, кількість елімінованих аномалій може бути більше однієї. Тоді, $Ak(Za_i)$ приймає ряд значень величин $Ak(Za_i)$, які відповідають кількості усунених аномалій An_i.

У випадку критерія 4, розмір компоненти може мати різну величину. Розмір компоненти в найпростішому випадку, може вимірюватися кількістю елементів x_{ij}, які входять в її склад, що дозволяє величину $Ak(Za_i)$визначити на відповідному інтервалі чисел. Крім того, такий інтервал визначення величини $Ak(Za_i)$ може бути збільшений на кількість процесів, в яких відповідна компонента приймає участь в рамках середовища W_i.

Розглянемо загальний параметр безпеки задачі $\eta(Za_i)$. Цей параметр необхідний, в першу чергу для того, щоб можна було оцінити загальну величину небезпеки, яка обумовлюється розв'язком задачі Za_i. При цьому, не проводиться оцінка різних режимів реалізації розв'язку задачі, наприклад, режимів, що відповідають помилковим розв'язкам, чи відсутності розв'язку. Приймається, що задача є сформульована коректно, а алгоритм Za_i розв'язку цієї задачі побудовано таким чином, що всі варіанти розв'язку задачі, що відтворюються в Al_i є коректні та обґрунтовані. Крім того, приймемо, що ціль задачі неорієнтована на створення аномалії в W_i і, тим більше, на активізацію критичної ситуації в W_i. В даному випадку під коректною задачею будемо розуміти таку задачу, яка характеризується параметрами важливості або значимості задачі $\aleph_i(Za_i)$ та параметрами її актуальності $Ak(Za_i)$.

Небезпека задачі Za_i, або $Nb(Za_i)$ може носити характер безпосередній та опосереднений. Безпосередній характер безпеки задачі $\eta^b(Za_i)$. полягає у тому, що по передачі результатів розв'язку Za_i в середовище W_i, відразу виникають негативні фактори, що найменше у вигляді аномалій різного типу $An(W_i)$.

Розглянемо завдяки чому може мати місце ситуація, коли $\eta(Za_i) \neq max$. Величина $\eta(Za_i)$ задається на діапазоні $[\alpha\beta]$де $\beta = max\ \aleph(Za_i), \alpha = min\ \aleph(Za_i)$. Приймаємо, що алгоритм $Al(Za_i)$ та ціль $C_i(Za_i)$ сформовані коректно. Тоді, відхилення $\aleph_i(Za_i)$ від максимального значення може виникнути, через наступні причини.

Вхідні дані в Za_i задаються шляхом надання$\{j(x_{is}), \dots, j(x_{ik})\}$, де $j(x_{ik})$-текстовий опис даних, які не можуть абсолютно адекватно їх описувати. Тому, вхідні дані, які отримує Za_i, будуть давати похибку ΔDw_i.

Аналогічно і ціль $C_i(Za_i)$ не може описувати результат розв'язку абсолютно точно, бо інакше не треба було б таку задачу розв'язувати. Звідти виникає похибка типу $\Delta C(Za)$. Аналогічну ситуацію створює компонента, що представляє собою $Al(Za_i)$, а помилка яку допускає алгоритм, буде давати відхилення $\Delta Al(Za_i)$. Тоді, в загальному випадку, рівень безпеки можна записати у наступному вигляді: $\eta(Za_i) = \delta[f(\Delta Dw, \Delta R, \Delta Al)]$

З цього співвідношення виходить, що з ростом ΔDw, ΔR і ΔAl рівень

безпеки $\eta(Za_i)$ зменшується. Розглянемо причини через які $\eta(Za)$ не може бути максимальним. Коли задача Za_i отримує вхідні дані Dw з DIS, то в силу того, що ці дані вибираються на основі семантичного аналізу $\{[j(x_{is}^z), \dots, j(x_{ik}^z)]\&[j(x_{is}^s), \dots, [j(x_{ik}^s)\}$ відповідні значення Dw будуть надані з похибкою ΔDw, оскільки семантичний опис x_i^z може не завжди співпадати з необхідною точністю з даними, що описуються в DIS або x_i^z. Ціль задачі $C_i(Za_i)$ в якій описуються вихідні дані, також не може бути описана достатньо точно, інакше не було б сенсу розв'язувати задачу. Рівень безпеки задачі $\aleph_i(Za_i)$ є тим вищий, чим більш точно розв'язок задачі відповідає цілі. З цього витікає, що рівень безпеки задачі по параметру $\Delta C_i(Za_i)$ ніколи не буде максимальним. Величина $\Delta C_i(Za_i)$ привносить певний вклад в пониження рівня безпеки. Алгоритми задач, які реалізують процеси їх розв'язку, не можуть достатньо точно відображати ті процеси, які описує розв'язок задачі. Будь-який алгоритм процесу функціонування,що має природний характер, чи процесу, що має соціальний характер та інші процеси, описуються з певними наближеннями до своїх реальних процесів, які вони моделюють. Тому, вони не можуть бути абсолютно адекватним відповідному процесу [6]. Це приводить до відхилення $\Delta Al(Za_i)$ [4]. Якщо дотримуватися інтерпретації поняття безпеки задачі, яке, представляється, як спосіб забезпечення максимальної точності розв'язку, то можна стверджувати, що абсолютно адекватного способу розв'язку задачі досягнути не можливо.

В багатьох випадках аспекти, про які йшла мова вище,впливають на точність розв'язку задачі [8]. В нашому випадку, точність розв'язку задачі впливає на рівень безпеки система, яка використовує отримані результати. Тому, в даній ситуації ми мусимо керуватися не просто точністю її розв'язку, а інтерпретацією отриманих результатів з точки зору вимог до безпеки об'єкту, для якого задача проводить обчислення. Це означає, що необхідна точність розв'язку задач визначається рівнем безпеки.

Коротко розглянемо можливий зв'язок рівня безпеки задачі $\eta(Za_i)$ з точністю розв'язку. Кожна задача Za_i, що розв'язується в рамках співпраці з DIS_i, орієнтована на певний процес, або на певний фрагмент з предметної області W_i. Це означає, що необхідна точність формується, як одна з початкових умов проектування процесу розв'язку відповідної задачі. Тому, що у відповідності з умовою, яка визначає необхідну точність, вибираються основні характеристики задачі, до яких відносяться: тип алгоритму розв'язку задачі Al, допустима неточність вхідних даних (Dw). Незважаючи на попередній вибір параметрів, що визначають точність реалізації розв'язку задачі, в силу причин, які були описані вище, необхідна точність може виявитися незабезпеченою. При роботі з реальними об'єктами, на потреби яких створюється DIS та розв'язуються ті або інші задачі, в більшості випадків, не має можливостей організувати повторне проектування задачі, а також часто не має можливостей повторно розв'язувати саму задачу,

наприклад, змінивши її вхідні дані, чи інші параметри, що піддаються швидкій зміні. В цьому випадку, користувач отримує результати такі, які вдалося отримати, і виникає задача оцінки рівня безпеки їх використання в предметній області W_i. В цьому випадку мова йде про те, що користувач отримує певне рішення і самостійно пробує його використати в W_i. Переважно W_i функціонує на основі використання інформаційно-управляючих засобів з якими співпрацюють системи типу DIS. Тому, результати розв'язування задач, що орієнтовані на використання в W_i, недоцільно замикати на користувача, як на особу, що безпосередньо реалізує впровадження. Доцільно результати розв'язку задач, які можна було б реалізувати на системах з середовища W_i, доповнити інформаційними управляючими системи, безпосередньо в W_i. В цьому випадку, можна було б автоматизувати процеси визначення рівня безпеки задачі або $\eta(Za_i)$. Очевидно, що у випадку, коли виявиться, що рівень безпеки не достатній, то її результати не будуть використовуватися в рамках W_i. Інтерпретація недостатнього рівня безпеки Za_i, може полягати в тому, що використання такого типу результатів може привести до виникнення в W_i аномалій різного типу, або може привести до виникнення критичних ситуацій $Kr_i(W_i)$, що є недопустимим.

Висновки

Аналіз базових параметрів даних, таких як міри таємності, значимості та обґрунтованості використання даних, показав вплів факторів, таких як точність вхідних даних задачі, точності реалізації алгоритму на зміну рівня загальної безпеки системи.

Також відзначимо, що в інформаційних технологіях дослідження та розв'язування нових задач в дещо вузьких рамках сформульованої задачі, в більшості випадків, приводить до необхідності розширяти сферу впровадження отриманих результатів на суміжні системи, які є оточенням середовища в якому проводяться дослідження. Підтвердженням цього є необхідність розширення розв'язку задач надання повноважень до використання, в даному випадку, таємних даних до задач використання процесів, що використовують відповідну систему в DIS, а також в системах, які є предметною областю інтерпретації основної задачі.

Кількість параметрів, які можна використовувати, для характеристики задач, можна розширити, таке розширення може привести до можливості отримання додаткових результатів у забезпеченні їх безпеки.

1. *Davydenko A.*. Formalization level of abstraction of state information resourses access systems / A. Davydenko // Scientific letters of academic society of Michel Baludansky, ISSN 1338-9432. Volume 4, 1 2016, p.35-38.

2. *Давыденко А.Н.* Расширение теоретических возможностей математических моделей нейронных сетей обуславливаемых их использованием для решения задач защиты систем доступа / А.Н. Давыденко // Збірник наукових праць Інститут проблем моделювання в енергетиці НАН України : Зб. наук. праць вип. 45.. – К., 2008,– С. 112-

115.
3. *Давыденко А.Н.* Анализ основных информационных компонент систем доступа / А.Н. Давыденко // Моделювання та інформаційні технології: Зб. наук. праць вип. 59. – К., 2011, – С.11-20
4. *Редько В. Г.* Эволюция, нейронные сети, интеллект. Модели и концепции эволюционной кибернетики / В. Г. Редько . – М. : Эдиториал УРСС, 2005 . – 224 с.
5. *Гладков Л. А.* Генетические алгоритмы / Л. А. Гладков, В. В. Курейчик, В. М. Курейчик . – 2-е изд., испр. и доп . – М. : Физматлит, 2006 . – 320 с
6. *Акимов О. Е.* Дискретная математика: логика, группы, графы, фракталы / О. Е. Акимов . – М. : Акимова, 2005 . – 656 с.
7. *Уотшем Т.Дж.* Количественные методы в финансах / Т.Дж Уотшем, К. Паррамоу - М.: Юнити, 1999
8. *Хованов Н. В.* Анализ и синтез показателей при информационном дефиците / Н. В. Хованов – СПб.: Издательство Санкт-Петербургского университета, 2011

Поступила 22.08.2016 р.

УДК 004.4

С.М.Головань, А.М.Давиденко, Т.Л.Щербак, м.Київ

МЕТОДИ РОЗРАХУНКУ НАДІЙНОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ НА ЕТАПІ ЇХ ПРОЕКТУВАННЯ

Abstract. The following basic methods of natural and technical sciences in calculating the reliability of modern information systems, which in practice is a hardware-software implementation of technical systems. One of the main objects of study on reliability of systems is a mathematical model of functioning of the system for complete in time and in space the sequence preset functions.

Вступ. Відомо [1-4], що незважаючи на стрімкий рівень розвитку інформаційних систем, їх широке використання у різних предметних областях, надійність як інтегральна характеристика функціонування таких систем залишається основною властивістю систем зберігати значення своїх характеристик в часі і в просторі у межах заданих режимів і умов експлуатації, технічного обслуговування, зберігання і транспортування. В останній період число публікацій по проблемам надійності інформаційних систем у порівнянні з минулими періодами значно зменшилась по різним причинам. Але актуальність і важливість науково-технічної проблеми надійності таких систем не тільки не зменшилась, а навпаки зросла.

Постановка завдання. Навести основні методи природничих і технічних наук для розрахунків характеристик надійності сучасних інформаційних систем на етапі їх проектування.

