eversible Gaussian propagation. 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory, ATIT 2021. Proceedings, 2021, pp. 67-70.

[14]. Roman Kyrychok, Oleksandr Laptiev, Rostyslav Lisnevsky, Valeri Kozlovsky, Vitaliy Klobukov. Development of a method for checking vulnerabilities of a corporate network using bernstein transformations. Eastern-European journal of enterprise technologies. Vol. 1 №9 (115), 2022, pp. 93-101. ISSN (print) 1729-3774. ISSN (on-line) 1729-4061. DOI: 10.15587/1729-4061.2022.253530.

[15]. Valentyn Sobchuk, Iryna Zelenska and Oleksandr Laptiev. Algorithm for solution of systems of singularly perturbed differential equations with a differential turning point. Bulletin of the Polish Academy of Sciences Technical Sciences, Vol.71, No 3, 2023, Article number: e145682 DOI: 10.24425/bpasts.2023.145682 WoS.

MATHEMATICAL APPARATUS FOR FINDING THE OPTIMAL CONFIGURATION OF A SECURED COMMUNICATION NETWORK WITH A GIVEN NUMBER OF SUBSCRIBERS

Information flows in the world are growing very quickly. The exchange of information is growing rapidly. In connection with this fact, the existing mathematical apparatus and its practical application are constantly developing. The scientific-mathematical apparatus is aimed at finding the optimal configuration of the information communication network, solving the problem of building protected channels for the transmission of a large amount of data. A scientific task arises to develop a new and improve the existing mathematical apparatus for finding the optimal configuration of a protected communication network with a given number of subscribers. This scientific work is dedicated to the solution of this urgent task. The paper formulated and proved four Lemmas. The Lemma's formulation made it possible to prove two new theorems that allow solving the task of finding the optimal configuration of a protected communication network with a given number of subscribers. Solutions to both partial and general tasks of the process of optimization and protection of transmission channels of a large amount of data are provided. Thus, the paper proposes a solution to the scientific task of finding the optimal configuration of a protected communication network with a given number of subscribers. The direction of further research may be the development of a software implementation of the given mathematical apparatus.

Keywords: secure networks, optimal configuration, information protection, data security, cyber security.

Лаптєв Олександр Анатолійович, доктор технічних наук, старший науковий співробітник, доцент кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка, Київ, Україна.

Oleksandr Laptiev, Doctor of Technical Science, Senior Researcher, Associate Professor the Department of Cyber Security and Information Protection, Faculty of Information Technology, Taras Shevchenko National University of Kyiv.
E-mail: olaptiev@knu.ua.
Orcid ID: 0000-0002-4194-402X.

Аль-Далваш Аблуллах Фоуад, аспірант Національного авіаційного університету, Київ, Україна.

Al-Dalvash Ablullah Fowad, graduate student of the National Aviation University, Kyiv, Ukraine.
E-mail: abdullah.dalosh@gmail.com.
Orcid ID: 0000-0001-1003-9182.

DOI: 10.18372/2410-7840.26.18821
УДК 004.056.52:004.056.53

ДОСЛІДЖЕННЯ ВЗАЄМОЗВ'ЯЗКІВ МІЖ СЕМАНТИЧНИМИ ПАРАМЕТРАМИ ДЛЯ ГАЛУЗІ БЕЗПЕКИ СИСТЕМ ДОСТУПУ

Анатолій Давиденко, Олена Висоцька, Михайло Пригара, Володимир Бичков

Системи розмежування доступу привертають увагу за рахунок першочерговості під час контакту з інформаційною системою та критичністю збоїв при її роботі. Тому вона є важливою типовою підсистемою будь-якої інформаційної системи. Перед розробником нової інформаційної системи завжди виникає дилема – або розробка цієї підсистеми з нуля або адаптація вже готового рішення. Якщо виключити аспекти вартості та авторського права, критичним для вирішення дилеми є технічна можливість та складність такої адаптації. У цій статті досліджується потенційне застосування типової підсистеми розмежування доступу в різних предметних областях, з акцентом на унікальність сфери застосування та визначення вимог та обмежень, що виникають при процедурі адаптації. Інтуїтивно зрозуміло що близькість предметних областей інформаційних систем впливає на ефективність адаптації, але для попередньої оцінки доцільності її використання потрібна методологія, яка дозволяє отримати якісний або кількісний результат. Можливим підходом є семантичний аналіз та експертна оцінка на основі різних математичних методів в тому числі нечітких. Метою статті є дослідження можливостей та перспективи використання технології адаптації систем розмежування доступу при розширенні предметної області. Методи дають можливість створювати більш гнучкі засоби оцінювання на основі семантичного аналізу. Використання методів дозволяє отримувати результати, як в кількісній, так і в якісній формі.

***Ключові слова**: розмежування доступу, ідентифікація, надання прав користувачу, семантичний аналіз, міра семантичної надмірності.*

ВСТУП

Різноманіття систем доступу визначається їх природою. Системи доступу забезпечують комунікативну функцію між об'єктом доступу і користувачем засобів, які надає об'єкт користувачеві [1]. Комунікативна функція реалізується у вигляді інтерфейсу між користувачем і об'єктом доступу. Існує розбіжність між формами відображення даних об'єкту та користувача, особливо якщо таким користувачем є не процес, а людина, що вирішує свою прикладну задачу. Тому, система доступу повинна мати досить розвинену інформаційну структуру. Така інформаційна структура необхідна для вирішення завдань перетворення області інтерпретації даних користувача, які представлені у відповідній формі, у форму, яка прийнятна для об'єкта доступу. Також мають існувати і зворотні функції перетворення форм представлення даних. Відповідні перетворення форм представлення даних базуються на описах предметних областей інтерпретації, якими користується користувач, і областей інтерпретації, які допустимі в об'єкті доступу.

Враховуючи [2], що таких користувачів з різними областями інтерпретації їх прикладних задач у одного об'єкта доступу може бути багато, стає очевидними складність вирішення завдання перетворень одних форм представлення даних в іншу і навпаки та нелінійне зростання цієї складності з ростом кількості областей інтерпретації. У сучасних системах доступу завдання перетворення вхідних даних в необхідну для об'єкта форму розподілене за всіма складовими, які використовують систему доступу.

Таким чином, для системи доступу виділена лише частина функціональних перетворень, які вирішують задачу узгодження даних, що йдуть від користувача до об'єкта доступу і навпаки. До таких завдань, які визначені для системи доступу, можна віднести наступні:

- надання користувачеві успадкованого інтерфейсу;
- вихідне перетворення даних користувача в форму подання, яка прийнятна для об'єкта;
- перетворення даних, що надходять від об'єкта доступу до користувача, в форму прийнятну для окремого користувача;
- формування додаткових коментарів до даних, що призначені окремому користувачеві, якщо користувачем є людина і остання сформувала запит на такі коментарі;
- ідентифікація користувача, метою вирішення якої є визначення окремого користувача, якщо таких користувачів може бути більше, ніж один.

Наведені вище завдання це класичний набір функцій системи доступу [3], для випадку, коли не розглядаються завдання безпеки системи доступу, об'єкта доступу і забезпечення безпеки користувачів, які використовують відповідну систему доступу.

Інформаційна система (IS) повинна ґрунтуватися на описах предметних областей, які описують інтерпретацію даних, які використовуються в усіх фрагментах системи розмежування доступу (SRD). Тому розглянемо основні компоненти IS, які необхідні для вирішення завдань інформаційного забезпечення системи безпеки SRD, яку скорочено будемо позначати символами BSD. До таких компонентів віднесемо наступні:

- словники, що містять опис базових елементів предметних областей;
- система синтаксичних правил формування описів інтерпретації базових елементів;
- система семантичних параметрів, які характеризують особливості інтерпретації базових елементів і інших компонентів BSD
- система семантичних правил, які регламентують способи побудови опису інтерпретації елементів, які використовуються при функціонуванні системи BSD;
- система правил перетворення описів компонент системи BSD.

Дослідженню проблем, пов’язаних із процесом обробки та розмежування доступу до інформації у спеціалізованих розподілених інформаційних системах, що є об’єктом дослідження, присвячується значна частина публікацій зарубіжних вчених, таких як: Whitfield Diffie, Martin Hellman, David Elliott Bell, Leonard J. LaPadula, Carl E. Landwehr, David D. Clark та інші [4-8].

Особливістю вітчизняного підходу є наявність як унікальних механізмів захисту, наприклад еліптичні криві, та методів оцінки систем розмежування доступу, наприклад на основі нечітких множин [9-12]. Однак, незважаючи на значну кількість підходів до вирішення даної проблеми, вона залишається актуальною не тільки для України, але і для всієї світової спільноти.

ОСНОВНА ЧАСТИНА

Постановка задачі

Перераховані при постановці проблеми функціональні перетворення, які вирішують задачу узгодження даних для адаптації системи доступу не завжди можуть бути коректними для перерахованих вище завдань, тому метою роботи є ви-

значення кількісної оцінки обсягу варіабельності предметної області [1]. Для цього необхідно визначити міру семантичної надмірності та з'ясувати додаткові обмеження вирішення задачі адаптації.

Розглянемо відмінності, які притаманні процесу доступу саме при вирішенні завдань безпеки SD. Для зручності, будемо говорити про безпеку SD маючи на увазі безпеку всіх перерахованих складових. В цьому випадку необхідна досить розвинена система інформаційного забезпечення тих підсистем, які безпосередньо орієнтовані на вирішення завдань захисту всіх компонент SD. При коректному проектуванні SD, причинами зміни рівня безпеки можуть бути, в першу чергу, зовнішні фактори, які можуть впливати на роботу SD. Внутрішні чинники, які теж можуть негативно впливати на роботу SD розглядати не будемо. Оскільки зовнішні фактори, які впливають негативно на SD, ініціюють відповідні дії недетерміновано, то характерними для вирішення завдань захисту SD є такі методи:

– методи прогнозування виникнення атак на SD з боку зовнішніх небезпек;

– методи адаптації SD до зовнішніх умов, в яких функціонує SD;

– методи розпізнавання негативних зовнішніх впливів на SD або розпізнавання атак;

– методи визначення поточного рівня безпеки окремих компонент і системи SD в цілому;

– методи протидії атакам, які були виявлені на різних етапах їх реалізації, включаючи кінцевий етап реалізації атаки, якщо остання є успішною.

З наведених базових методів вирішення завдань забезпечення безпеки видно, що для їх реалізації і ініціації не існує або досить складно визначити детермінований набір вхідних даних, які забезпечували б можливість однозначно визначити алгоритм реалізації відповідних методів вирішення задач, які в сукупності вирішували б завдання забезпечення безпечного функціонування системи SD. У зв'язку з цим, доцільно для вирішення наведених завдань використовувати засоби, які в максимально можливій мірі були б придатні для реалізації наведених вище методів вирішення окремих складових завдання забезпечення безпеки функціонування системи SD. Досвід авторів показує доцільність використання при цьому засобів штучного інтелекту на основі нейронних мереж.

Необхідність дослідження взаємозв'язків між семантичними параметрами обумовлюється наступними факторами та особливостями цих параметрів:

–існуванням взаємозалежностей між параметрами;

–необхідністю семантичної інтерпретації різних значень величини цих параметрів;

–існуванням критичних значень величин семантичних параметрів, обмеженими діапазонами їх значень і особливими точками значень відповідних параметрів.

Введення чисельних значень семантичних параметрів має сенс, якщо семантичною інтерпретацією володіють не тільки самі параметри, але і окремі величини їх значень. Визначення такої інтерпретації можна здійснювати наступними способами:

– на основі апріорних методів формування інтерпретації різних значень семантичних параметрів;

– на основі дослідження зміни значень параметрів, які визначаються із взаємозв'язків між параметрами;

– на основі експериментальних досліджень фрагментів предметної області і змін в текстових описах в цілому, при зміні значень окремих параметрів;

– на основі об'єктивних обмежень, які накладаються на діапазони значень параметрів, виходячи з аналізу специфіки предметної області.

Останній спосіб визначення семантичної інтерпретації значень параметрів, використовується по відношенню до базових семантичних параметрів, до яких відносяться:

–семантична значимість $z(x_i)$;

–семантична ефективність $e(x_i)$ та інші базові параметри, які можуть вводитися при необхідності.

Вирішення поставленої задачі

Розглянемо більш детально спосіб введення обмежень на величини значень семантичних параметрів на якісному рівні. Нехай деяка компонента x_i із $j(x_i)$ має інтерпретаційне розширення $j(x_i)$, котре складається із m інформаційних елементів, що формально описується співвідношенням $j(x_i) =< a_1, ..., a_m >$. В цьому випадку величини семантичної значущості x_i визначаються співвідношенням: $z(x_i) = \sum_{i=1}^{n} Sg(a_i)$.

Для реалізації способу інтерпретації значень поточних величин базових семантичних параметрів, скористаємося поняттям рівня абстракції ко-

мпонентів x_i словника S_c. При розгляді поняття рівня абстракції використовуються два функціональних перетворення:

– $F_{Ai}(S_{ci})$ – перетворення окремих елементів з S_c яке призводить до зміни рівня абстракції груп із S_c;

– Q_{Ai} – функція, відповідно до якої визначається величина зміни рівня абстракції.

У загальному випадку, збільшення рівня абстракції деякої підмножини $\{x_{i1}, ..., x_{iM}\} \subset X$ має семантичну інтерпретацію, яка може на якісному рівні характеризуватися такими особливостями:

– збільшення рівня абстракції позначення окремих елементів S_c доцільно в тому випадку, якщо нові елементи x_j^* мають більш загальне значення по відношенню до x_i;

– Використання x_j^* для створення φ_j^* дозволяє формувати фрагменти, які описують відповідні фрагменти предметної області без урахування окремих деталей, які носять приватний характер і не потрібні для встановлення більш загальних, для даної предметної області, описів;

–оскільки збільшення рівня абстракції, в даному випадку, пов'язується з можливістю формування більш загальних описів процесів або компонент, які присутні в предметній області, то використання різних рівнів абстракції дозволяє будувати алгоритми реалізації окремих процесів таким чином, щоб рішення задачі, на яку орієнтований відповідний процес, можна було досягти більш ефективним способом;

–в загальному випадку, можна стверджувати, що використання об'єктів більш високого рівня абстракції для опису процесів, в яких вони беруть участь у багатьох випадках, дозволяє отримати рішення відповідного завдання в більш загальному вигляді.

Розглянемо більш детально, що являє собою функція $F_{Ai}(S_{ci})$, в рамках розглянутого підходу. Оскільки F_{Ai} здійснює перетворення фрагмента $S_{ci} \subset S_c$, то для спрощення розгляду, обмежимося одним елементом x_i. Для опису $j(x_i)$ використовуються компоненти $\{a_1, ..., a_n\}$, які в предметній області W є словами природної мови V. Елементи x_i із S_c повинні представляти собою слова, які для предметної області W теж відносяться до відповідної природної мови V, оскільки фрази і речення, які формуються в рамках інформаційних засобів, орієнтовані на використання користувачами системи доступу. Очевидно, що в рамках самої системи відповідні елементи позначаються ідентифікаторами. Якщо $\{x_1, ..., x_m\} \cup \{a_1, ..., a_n\} = v$, то v є множиною слів для V, які описує W. Для зручності V і W будемо ототожнювати, оскільки предметна область реалізується за допомогою описів відповідною природною мовою.

Для формування φ_i і Ψ_i використовується, окрім семантичних правил і обмежень, синтаксичні схеми $\Omega = \{\omega_1, ..., \omega_2\}$. Оскільки v є загальною для x_i і для $j(x_i)$, то можна прийняти, що в $j(x_i)$ окремі фрази із $a_{i1}, ..., a_{im}$ формуються також у відповідності з правилами Ω, тим більш, що і для створення опису $j(x_i)$ і $\varphi_i(x_{i1}, ..., x_{ik})$ використовуються однакові вимоги щодо нормалізації відповідних текстових відображень. Отже, можна записати, що V або W являє собою мову, яка описується наступним співвідношенням:

$$W = (v, \Omega, X_i^B),$$

де X_i^B – набір елементів S_c найбільш низького рівня абстракції.

Функція $F_{Ai}(x_i)$ по суті є функцією, що породжує, оскільки базовий елемент X_i^B не може бути переведеним на вищий рівень абстракції, оскільки X_i^B має певну $j(X_i^B)$, яка сформована на виході. Тому, правильніше було б функцію породження представити в наступному вигляді:

$$X_i^m = F_{Ai}(X_{i1}^{m-1}, ..., X_{ik}^{m-1}), \quad (1)$$

де X_i^m – елемент S_c з рівнем абстракції m, X_{ij}^{m-1} – елемент S_c з рівнем абстракції m - 1.

Співвідношення (1) описує породження суворої ієрархії, коли рівень абстракції m формується основі попереднього рівня абстракції m-1. Частіше всього функція F_{Ai} реалізує перетворення вільної ієрархії. Це означає, що має місце співвідношення:

$$X_i^m = F_{Ai}(X_{i1}^{m-1}, ..., X_{ik}^{m-1}, ..., X_{im}^B),$$

де елемент X_i^m породжується не тільки на основі елементів попереднього рівня абстракції, а й на основі перетворення елементів різних нижчих рівнів ієрархії, включаючи і базовий рівень X_{im}^B. Для спрощення розгляду приймемо, що:

$X_i^2 = F_{A1}(X_{i1}^B, ..., X_{ik}^B)$ або $X_i^2 = F_{A1}(X_j^B)$.

В цьому випадку, F_{Ai} буде здійснювати перетворення $j(x_i)$ таким чином, щоб в множині $\{a_{i1}, ..., a_{im}\}$ з'явився хоча б один елемент із X_j^B і відповідно з S_c. Формально це можна записати в такий спосіб:

$$X_j^2 = F_{A1}(X_j^B) = F_{A1}(< a_{j1}, ..., a_{jm} >) = < a_{j1}, ..., x_i^B, ..., a_{jm} > .$$

Природно, що $x_i^B =< a_{i1}, ..., a_{ik} >$, тоді можна записати: $X_j^2 = x_i^B$.

Наведені перетворення не означають, що за допомогою F_{Ai} в W можна породити фізично новий елемент поточного рівня абстракції, як правило, є нові поняття про W, нові процеси, які можуть виникати в W, і в крайньому випадку, нові фізичні об'єкти, якщо в рамках системи, яка використовує відповідну інформаційну компоненту, можливо фізичне виготовлення нового фізичного елементу x_i^m.

Співвідношення (1), яке описує новий елемент S_c з новим рівнем абстракції, в силу вищого рівня абстракції x_i^m має семантичну значимість відмінну від семантичної значущості елемента $x_i * j(x_j)$. Цей факт забезпечується в даному випадку, додаванням інтерпретаційного розширення $j(x_i)$.

Таке додавання здійснюється відповідно до правил Ω. Таким чином, функція F_{Ai}, по суті, вибирає додаткові елементи $x_{i1}, ..., x_{ik}$, із S_c і розширює ними $j(x_j)$. Отже, можна прийняти, що збільшення семантичної значущості $z(x_i)$ визначається величиною, яка визначається кількістю інформаційних компонент в $j(x_i)$. Процес вибору компонент, якими передбачається розширювати $j(x_i)$, не може бути довільним. Це означає, що функція $F_{Ai}(x_i)$ повинна визначатися більш конструктивно. Перш за все, на процес вибору впливають синтаксичні схеми, відповідно до яких побудовано розширення $j(x_i)$. На підставі $\omega_i(x_i)$ визначається місце розміщення розширювача $j(x_j)$ в $j(x_i)$. В більшості випадків, таке розширення реалізується в кінці опису $< a_{i1}, ..., a_{im} >$, якщо параметри суперечливості та узгодженості фрагмента $j[\varphi_i(a_{ij})]$ у існуючого $j(X_i)$ задовольняють заданим вимогам, оскільки мова W одна для $j(X_i)$ і для $A_i(X_i)$, то семантичні параметри, які введені для текстових описів прикладної системи $A = \{A_1, ..., A_m\}$, використовуються і для аналізу текстових описів інтерпретації $J(A_i)$. Для їх розрізнення, в останньому випадку, відповідні позначення будемо писати у вигляді того ж символу з індексом *j* зверху, або z^j, e^j, h^j і u^j. Приймемо, що $j(X_i)$ можуть являти собою фрази φ^j або речення Ψ^j, тому параметр $k(\Psi_i, \Psi_j)$ для $J(A)$ не розглядається. Наступним обмеженням, яке уточнює спосіб реалізації $F_{Ai}(X_i)$, є задані допустимі значення величини зміни семантичних параметрів z^j, e^j, h^j і u^j. Такі значення є загальними для всієї предметної області W_i. Відзначимо, що в рамках S_c предметних областей може бути кілька, наприклад, в разі використання в рамках BSD різних методів ідентифікації.

Функція Q_{Ai} відрізняється від F_{Ai} тим, що вона визначає міру зміни рівня абстракції перетвореного фрагмента S_{ci} в словнику S_c. Як мінімум, вона повинна враховувати факт того що зміна величини рівня абстракції між двома описами предметної області, що послідовно розглядаються, не може перевищувати 10% від загальної кількості базових елементів опису предметної області, яка модифікується, хоча, в загальному випадку, ця функція може визначатися більш складним способом, який враховує більш широко параметри прикладної системи, наприклад, рівень безпеки системи доступу або рівень ризику роботи користувача з об'єктом доступу, який оснащений відповідною системою доступу.

З викладеного вище видно, що функція F_{Ai} відповідає класичному уявленню про аналітичні функції [13]. Ця функція являє собою систему умов і окремих алгоритмів вибору і алгоритмів аналізу семантичних параметрів в $J(A)$.

Розглянемо обмеження на діапазон значень параметра $Z_i(x_i)$. Оскільки $j(x_i)$ має являти собою фразу, то система синтаксичних правил визначає мінімальну допустиму кількість слів, яка необхідна для того, щоб фраза була сформована синтаксично коректно. В даному випадку приймемо, що мінімальна за розміром фраза повинна

складатися, як мінімум з трьох слів. Ця умова передбачається в конкретних схемах $\omega \in \Omega$. Для визначення верхньої межі кількості допустимих слів в межах фрази φ^j введемо додатковий семантичний параметр, який описується наступним визначенням.

Визначення 1. Семантична надмірність фрази $\eta(\varphi_i)$ визначається похідною від функції $f(z_i)$, яка визначена на φ_i, по змінній збігається з віссю розташування слів у фразі φ_i.

Формально це можна записати у вигляді:

$$\eta(\varphi_i) = df(z_i)/d_i,$$

де $f(z_i)$ – крива, яка апроксимує величини значень z_i для кожного з послідовно розміщених в фразі φ_i слів x_i, i – номер слова в φ_i, починаючи від початку фрази і закінчуючи останнім словом фрази.

Цю похідну можна замінити для дискретного випадку, кутом нахилу лінії, що зв'язує дві сусідні точки значень семантичної значущості двох послідовних слів x_i і x_j в фразі φ_i. Середнє значення відповідних кутів по всій фразі φ_i буде характеризувати міру семантичної надмірність $\eta(\varphi_i)$. Слід зазначити, що для визначення семантичної надмірності, кут нахилу вибирається між гіпотенузою і вертикальною віссю, оскільки елементарний прямокутний трикутник будується паралельно до вертикальної і горизонтальної осей z і i. Формально, це запишеться у вигляді співвідношення:

$$\eta(\varphi_i) = \{\sum_{i=1}^{m-1} arctg\,[(\left|z_j^i - z_{i-1}^k\right|)/ (i_i^j - i_{i+1}^k)]\}/(m-1), \quad (2)$$

де i_j – номер чергового слова у фразі φ_i.

Розглянемо якісну інтерпретацію цього параметра. Нехай деякі два послідовних слова x_i і x_j в фразі φ_i мають однакову семантичну значимість. При цьому, можна припустити, що семантична значимість визначається не одним, а низкою базових семантичних параметрів.

У випадку, якщо $z(x_i) \approx z(x_j)$, то два слова x_i і x_j є синонімами і їх спільне вживання суперечить вимогам нормалізованого уявлення текстових відображень. У співвідношенні (2) в знаменнику, якщо розглядати два послідовних слова, знаходиться одиниця, оскільки масштаб горизонтальної осі визначається кількістю слів на заданому відрізку цієї осі. Тому, відстань між двома суміжними словами завжди дорівнює одиниці або вимірюється кількістю слів у фразі φ_i.

Відповідно до вимог використання нормалізованих методів побудови текстових образів, система Ω передбачає певні обмеження на допустимий розмір фраз φ_i і відповідно, на допустимий розмір речень Ψ, які можуть використовуватися в прикладній системі A_i. Проте, в межах допустимих розмірів фраз можуть виникати семантичні надмірності внаслідок використання семантично близьких слів. Щоб допустима довжина фраз обмежувалася не тільки синтаксичними схемами але і семантичними чинниками, необхідно для кожної φ_i визначати величину $\eta(\varphi_i)$. Якщо $\eta(\varphi_i) < \eta(\varphi_i)_{\min}$, то розмір відносно φ_i не допустимий. Таким чином верхня межа допустимого розміру фрази φ_i в A_i і $J(x)$ є плаваючою і може бути різною для різних φ_i.

Розглянемо діапазон допустимих значень для параметра $e(x_i)$. У результуючому вигляді $e(x_i)$ має фіксоване початкове значення, що визначає для кожного $e(x_i)$ його мінімальну межу в діапазоні значень цього параметра. У рамках даного підходу розглядається ситуація, коли φ і Ψ із A_i формуються при проектуванні прикладної системи A_i. Такі фрази і речення становлять базову систему текстового відображення прикладної системи A_i.

Це не означає, що вся A_i повинна бути описана в текстовому вигляді. Текстовому відображенню підлягають тільки ті фрагменти, які не можуть бути описані в рамках формальних засобів, які використовуються для проектування відповідної прикладної системи A_i. Прикладом такої ситуації, характерної для області захисту даних і, зокрема, для області безпеки систем доступу, є BAN-логіка [14].

На підставі аналізу використовуваних інформаційних елементів X_i з S_c визначимо S_t, в базовій системі фраз і речень, що будуть визначатися, початкове значення параметра $e(x_i)$ і на момент проектування A_i відповідне значення для окремого $e(x_i)$ приймається в якості граничного. Встановлення діапазону значень $e(x_i)$ для S_c в

частині нижньої його межі здійснюється відповідно до співвідношення:

$$min\,[gr\,(e\,(x_i))] = min\,(e\,(x_i))^B,$$

де $e\,(x_i)^B$ - мінімальне значення $e\,(x_i)$, встановлене на основі аналізу базових φ_i і Ψ_i з S_t.

Максимальне значення в даному випадку, не будемо вводити в якості обмеження діапазону значень, оскільки, це вимагає більш глибокого аналізу семантики всієї предметної області в цілому на кожному етапі її розвитку. Відзначимо лише, що в межах даного дослідження, в якому не передбачається реалізація можливості формування в автоматичному режимі, в процесі функціонування системи нових фраз або речень Ψ, а використання інформаційних засобів дозволяє тільки модифікувати φ_i і Ψ_i, які знаходяться в S_t. Природно, що процес послідовних модифікацій, який реалізується на різних етапах функціонування системи може привести до появи нових φ_i і Ψ_i, які не відповідають φ_i^B і Ψ_i^B.

Розглянемо допустимі діапазони значень для параметра $h(\varphi_i)$. Семантична суперечливість в межах однієї фрази φ_i є альтернативним поняттям для семантичної надмірності $\eta\,(\varphi_i)$. Як і у випадку $\eta\,(\varphi_i)$, для семантично повного визначення $h\,(\varphi_i)$ може виникнути необхідність у більш широкому асортименті базових семантичних параметрів, ніж параметри $z\,(x_i)$ і $e\,(x_i)$. Оскільки, в даному випадку, ми обмежуємося базовим параметром $z\,(x_i)$, то межі значень параметрів $h\,(\varphi_i)$. Мінімальне значення встановлюються таким чином. $h\,(\varphi_i)$ відповідає мірі параметра $\eta\,(\varphi_i)$ і дорівнює мінімально допустимій величині параметра $\eta\,(\varphi_i)$. Таким чином можна записати:

$$min\,[gr\,(h\,(\varphi_i))] = min\,(\eta\,(\varphi_i))],$$

де $gr\,(y)$ означає граничне значення аргументу y.

Максимальне значення діапазону допустимих значень для параметра $h\,(\varphi_i)$ визначається, для випадку двох суміжних слів, співвідношенням:

$$max\,[gr\,(h\,(x_i, x_j)] = max\,[gr\,[z\,(x_i)] - 3].$$

Цей випадок відповідає ситуації, коли слово x_i має максимальне значення z, яке визначається граничною величиною, а слово x_j має максимальне значення z, яке, відповідно до прийнятого вище, визначається трьома інформаційними компонентами в $j\,(x_j)$. Оскільки верхня межа значень параметра $z\,(x_i)$ істотно залежить від семантики предметної області W і від семантичної інтерпретації процесів, які відбуваються в W під час функціонування відповідної прикладної системи A_i, то максимально допустимі граничні значення для $\eta\,(\varphi_i)$ встановлюються на основі даних отриманих в результаті експлуатації відповідної прикладної системи A_i в W. Кінцевими критеріями, які використовуються в даному випадку, для визначення $gr\,(h\,(\varphi_i))$, є критерії рівня безпеки системи BSD, яка представляє собою предмет досліджень.

Граничні значення діапазону допустимих величин визначаються на основі аналізу граничних значень для $h\,(\varphi_i)$, оскільки $u\,(\varphi_1, ..., \varphi_n) = u\,(\Psi)$ визначається через $h_1\,(\varphi_i)$, ..., $h_n\,(\varphi_n)$. Тому, більш детально розглядати це питання не будемо.

Діапазон значень параметра $K\,(\Psi_i, \Psi_j)$ для випадку суміжних речень Ψ_i і Ψ_{i+1} розглядати не будемо, оскільки, цей випадок, аналогічний ситуації з параметром $h\,(\Psi_i)$. Складніша ситуація з визначенням діапазонів значень для $K\,(\Psi_i, \Psi_j)$ обумовлюються тим, що між Ψ_i і Ψ_j можуть розташовуватися інші речення. Параметр K для цього випадку будемо позначати символом $K_R\,(\Psi_i, \Psi_j)$. Очевидно, що один із способів визначення величини $K_R\,(\Psi_i, \Psi_j)$, для визначення діапазонів значень може складатися в зведенні до послідовності K, що формально записується у вигляді:

$$K_R\,(\Psi_i, \Psi_j) = F\,[K\,(\Psi_i, \Psi_{i+1}), ..., K\,(\Psi_{j-1}, \Psi_j)].$$

Можливість реалізації такої редукції ґрунтується на тому, що текстове відображення в довільний момент процесу функціонування являє собою деякий єдиний текст, який описано в W. У цьому випадку, предметом обговорень може бути тільки функція F. Оскільки охоплюється цілий фрагмент, то природно припустити, що в такому фрагменті відображаються глобальні для системи захисту доступу параметри. У зв'язку з цим конструктивний розгляд можливо в рамках розгляду

BSD в цілому або в рамках окремих режимів функціонування BSD.

З викладеного вище, особливо, в частині що стосується встановлення граничних значень параметрів $z(x_i)$, $h(\varphi_i)$ а також $K_R(\Psi_i, \Psi_j)$ видно, що для вирішення задач встановлення допустимих значень параметрів, а також для встановлення більш повних взаємозв'язків між семантичними параметрами, необхідно використовувати підходи, в яких досліджується робота системи BSD в цілому, що пов'язано з експериментальними дослідженнями.

ВИСНОВКИ

Проведено дослідження взаємозв'язків між семантичними параметрами для розширення функціональних можливостей при здійсненні контролю доступу.

В роботі визначено кількісну оцінку обсягу варіабельності предметної області та дано визначення семантичної надмірності. Також в роботі показано що для вирішення задач встановлення допустимих значень параметрів необхідно використовувати підходи, в яких досліджується робота підсистеми захисту SD в цілому.

ЛІТЕРАТУРА

[1]. Давиденко А.М. Методи та моделі адаптивного захисту та розмежування доступу до розподілених інформаційних ресурсів. Дисертація доктора технічних наук: 05.13.21. Національний авіаційний університет. Київ, 2021, 347 с.

[2]. Davydenko A., «Formalization level of abstraction of state information resourses access systems», Scientific letters of academic society of Michel Baludansky, vol.4, no. 1, pp. 35-38, 2016.

[3]. Давиденко А., Суліма О., «Використання формальних засобів опису процесів надання повноважень», Захист інформації, Том 18, №2, С.143-149, 2016.

[4]. Bell L. LaPadula. Secure Computer System: Mathematical Foundation, ESD-TR-73-278, V. 1, MITRE Corportation.

[5]. LaPadula D. Bell. Secure Computer Systems: A Mathematical Model, ESD TR-73-278, V. II, MITRE Corportaion.

[6]. Nyanchama M., Osborn S. Modeling mandatory access control in role-based security systems. InDBSec, 1995, pp. 129-144.

[7]. Daniel Servos, Sylvia L. Osborn. Current Research and Open Problems in Attribute-Based Access Control. [Електронний ресурс]. Режим доступу https://www.researchgate.net/publication/312039271_Current_Research_and_Open_Problems_in_Attribute-Based_Access_Control.

[8]. William Fisher. Attribute Based Access Control. National Institute of Standards and Technology, 2015, p. 22.

[9]. ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих.

[10]. Корченко О., Давиденко А., Шабан М., «Декомпозиційна модель представлення смислових констант та змінних для реалізації експертиз у сфері ТЗІ», Захист інформації, Том 21, № 2, С. 88-96, 2019.

[11]. Моркляник Б., Корченко О., Кубів С., Казмірчук С., Телющенко В. «Метод фазифікації інтервалів для вирішення задач кібербезпекового оцінювання на об'єктах критичної інфраструктури», Безпека інформації, Том 29, №3, С. 103-110, 2023.

[12]. Корченко А.О. Методи ідентифікації аномальних станів для систем виявлення вторгнень. Монографія, Київ, ЦП «Компринт», 2019, 361 с.

[13]. Korn Granino A., Korn Theresa M. Mathematical handbook for scientists and engineers: definitions, theorems, and formulas for reference and review. Dover publications, Inc. Mineola, New York, 2000, p. 1551.

[14]. Boyd, Colin; Mao, Wenbo. On a Limitation of BAN Logic. Advances in Cryptology. Eurocrypt '93. Helleseth, Tor., Springer Berlin, Heidelberg, 1994, pp. 240-247.

STUDY OF THE RELATIONSHIP BETWEEN SEMANTIC PARAMETERS FOR THE FIELD OF SECURITY OF ACCESS SYSTEMS

Access control systems attract attention due to the priority of contact with the information system and the criticality of failures in its operation. Therefore, it is an important typical subsystem of any information system. The developer of a new information system is always faced with the dilemma of either developing this subsystem from scratch or adapting a ready-made solution. As far as the cost and copyright aspects are excluded, the technical feasibility and complexity of such adaptation is critical to resolving the dilemma. This article explores the potential application of a typical access differentiation subsystem in various subject areas, with an emphasis on the uniqueness of the scope and the definition of the requirements and constraints that arise during the adaptation procedure. It was intuitively understood that the proximity of the subject areas of information systems affects the effectiveness of adaptation, but for a preliminary assessment of the feasibility of its use, a methodology is needed that allows obtaining a qualitative or quantitative result. A possible approach is semantic analysis and expendation based on various mathematical methods, including fuzzy ones. The aim of the article is to study the possibilities and prospects of using the technology of adaptation of access differentiation systems in the expansion of the subject area. The methods make it possible to create more flexi-

ble means of evaluation based on semantic analysis. The use of methods allows you to obtain results, both in quantitative and qualitative form.
Keywords: differentiation of access, identification, granting rights to the user, semantic analysis, degree of semantic redundancy.

Давиденко Анатолій Миколайович, доктор технічних наук, старший науковий співробітник, провідний науковий співробітник відділу математичного і економетричного моделювання Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Київ, Україна, професор кафедри безпеки інформаційних технологій Національного авіаційного університету, Київ, Україна.
Anatolii Davydenko, Doctor of Technical Sciences, Senior Researcher, Leader Researcher at the Department of Mathematical and Econometric Modeling of the G. E. Pukhov Institute for Modelling in Energy Engineering NAS of Ukraine, Kyiv, Ukraine, professor at the Department of security of information technologies of the National Aviation University, Kyiv, Ukraine.
E-mail: davidenkoan@gmail.com.
Orcid ID: 0000-0001-6466-1690.

Висоцька Олена Олександрівна – кандидат технічних наук, доцент кафедри комп'ютеризованих систем захисту інформації Національного авіаційного університету, Київ, Україна.
Olena Vysotska – Candidate of Technical Sciences, Associate Professor at the Department of Computerized Information Security Systems of the National Aviation University, Kyiv, Ukraine.
E-mail: lek_vys@ukr.net.
Orcid ID: 0000-0002-9543-1385.

Пригара Михайло Петрович – кандидат технічних наук, доцент кафедри технології машинобудування Державного вищого навчального закладу "Ужгородський національний університет", Київ, Україна.
Mykhailo Prygara – Candidate of Technical Sciences, Associate Professor at the Department of Mechanical Engineering Technology of the Uzhhorod National University, Kyiv, Ukraine.
E-mail: mykhailo.prygara@uzhnu.edu.ua
Orcid ID: 0000-0002-0954-4480.

Бичков Володимир В'ячеславович, старший викладач кафедри безпеки інформаційних технологій Національного авіаційного університету, помічник ректора Державного університету інформаційно-комунікаційних технологій.
Volodymyr Bychkov, Senior Lecturer at the Department of Information Technology Security at the National Aviation University, Assistant to the Rector of the State University of Information and Communication Technologies.
E-mail: bychkov.v@duikt.edu.ua.
Orcid ID: 0000-0002-1054-9182.

DOI: 10.18372/2410-7840.26.18822
УДК 336.71:004.056

МЕТОД ВИЯВЛЕННЯ НЕПРАВДИВОЇ ІНФОРМАЦІЇ НА ОСНОВІ ЕКСПЕРТНОЇ ОЦІНКИ

Наталія Лукова-Чуйко, Тетяна Лаптєва

У статті удосконалено метод виявлення неправдивої інформації на основі методу експертної оцінки. Експертні методи використовуються для визначення номенклатури показників якості, коефіцієнтів їх вагомості, для вимірювання показників якості і їх оцінки органолептичним методом. Оцінка показників якості вимірювальним, реєстраційним, розрахунковим методами застосовується для визначення комплексних показників якості різних рівнів ієрархії. Експертні методи засновані на ухваленні евристичних рішень, базою для яких є знання і досвід, накопичені експертами в конкретній області у минулому. Базовим методом для удосконалення, був обраний колективній метод експертних оцінок. Тому, що він має безсумнівні переваги в порівнянні з методами, заснованими на звичайній статистичній обробці результатів індивідуальних опитувань. На відміну від існуючого підходу, удосконалений метод дозволяє проводити відбір експертів у групу, а не корегувати відповіді експертів з метою отримання необхідного результату. Особливістю запропонованого методу є те що відбір експертів робиться за рахунок осереднення оцінок. Осереднення оцінок для кожного експерта. Самооцінки експерта та оцінки того ж самого експерта робочою групою. Це дозволяє значно зменшити похибку реальної оцінки експерта. Можливість встановлювати інтервал довіри до оцінки неправої інформації дозволять отримати результати які задовольняють завданню виявлення неправдивої інформації з належною точністю. Але це спонукає до вирішення завдання оптимізації критеріїв оцінки та часу вирішення встановленого завдання. Наукова новизна полягає в обґрунтуванні та оцінюванні порівняльної важливості факторів, що обмежують призначення кожного окремого експерта для виявлення неправдивої інформації за допомогою методу групової експертної оцінки. Напрямком подальших досліджень є завдання оптимізації критеріїв оцінки.
Ключові слова: *експерт, неправдива інформація, прогнозування, алгоритм, інформаційні технології.*