УДК 681.327.12 **doi: 10.26906/SUNZ.2021.2.092**

А. І. Поворознюк, О. А. Поворознюк, Г. Є. Філатова

Національний технічний університет «Харківський політехнічний інститут», Харків, Україна

БАГАТОКРИТЕРІАЛЬНА ОЦІНКА АЛЬТЕРНАТИВ ПРИ ПРОЄКТУВАННІ ДВОХФАКТОРНОЇ АВТЕНТИФІКАЦІЇ СУБ'ЄКТІВ-КОРИСТУВАЧІВ В СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

Анотація. Робота присвячена вирішенню актуальної науково-технічної задачі підвищення рівня захищеності інформації шляхом проєктування двохфакторної автентифікації суб'єктів-користувачів в системах захисту інформації при багатокритеріальному порівнянні складових двохфакторної автентифікації. На основі аналізу методів автентифікації суб'єктів-користувачів, які використовуються при захисті інформації, була обґрунтована множина найбільш вживаних методів та сфери їх застосування. **Мета дослідження** – багатокритеріальна оцінка альтернативних методів автентифікації суб'єктів-користувачів при проєктуванні двохфакторної автентифікації в системах захисту інформації. **Результати.** В роботі проаналізовані методи автентифікації суб'єктів-користувачів, зокрема перспективні методи біометричної автентифікації з метою побудови двохфакторної автентифікації. Для багатокритеріального порівняння методів автентифікації обґрунтовано застосування методу аналізу ієрархій (MAI), який реалізує ієрархічну структуру порівняння альтернатив. На кожному рівні MAI будуються відповідні матриці парних порівнянь, елементами яких є експертні оцінки. Розроблена система локальних критеріїв порівняння альтернатив та відповідні матриці парних порівнянь а також матриця парних порівнянь локальних критеріїв та процедура обчислення глобального критерію.

Ключові слова: захист інформації, двохфакторна автентифікація, альтернатива, багатокритеріальне порівняння, метод аналізу ієрархій, локальний критерій, матриця парних порівнянь, глобальний критерій.

Вступ

Бурхливий розвиток засобів обчислювальної техніки, автоматизованих інформаційних систем, поява нових інформаційних технологій супроводжується, на жаль, і появою таких малоприємних явищ, як промислове шпигунство, комп'ютерна злочинність і, перш за все, несанкціонований доступ (НСД) до конфіденційної інформації. Цим обумовлюється актуальність і значимість проблеми захисту інформації.

Будь-яке сучасне підприємство (установа, фірма і т.д.), незалежно від виду діяльності та форм власності, не може сьогодні успішно розвиватися і вести господарську та іншу діяльність без створення надійної системи захисту своєї інформації, що включає не тільки організаційно-нормативні заходи, але і програмно-апаратні засоби контролю безпеки інформації при її обробці, зберіганні і передачі в автоматизованих системах [1, 2].

Тому захищена система обробки інформації для заданих умов експлуатації повинна забезпечувати безпеку (конфіденційність і цілісність) оброблюваної інформації і підтримувати свою працездатність в умовах впливу на неї різних типів загроз [3, 4], зокрема несанкціонованих втручань.

Протидією від несанкціонованого доступу є шифрування інформації [5], а також розмежування доступу суб'єктів-користувачів до інформаційних ресурсів системи [6]. При реалізації доступу користувачів виконується перевірка їх автентичності.

Постановка проблеми в загальному вигляді

Аутентифікація (англ. Authentication) - це основа безпеки будь-якої системи, яка полягає в перевірці достовірності даних про користувача сервером. Вона не тотожна ідентифікації та авторизації. Ці три терміни є елементами захисту інформації. Перша стадія – ідентифікація. На ній відбувається розпізнавання інформації про користувача, наприклад, логін і пароль. Друга стадія – аутентифікація. Це процес перевірки інформації про користувача. Третя стадія – авторизація. Тут відбувається перевірка прав користувача і визначається можливість доступу.

При цьому застосування для автентифікації суб'єктів-користувачів традиційної схеми «логін-пароль» не виключає її принципового недоліку, який полягає у відокремленості особи, що авторизується, від ключа, який використовується для підтвердження її автентичності. Цей недолік відсутній в схемах автентифікації суб'єкта за його індивідуальними біометричними параметрами [7, 8].

Аналіз останніх досліджень і публікацій

В даний час застосовуються такі методи аутентифікації [2]:

1. Парольні. Найпоширеніший метод. Аутентифікація може проходити по одноразовим і багаторазовим паролям. Багаторазовий пароль задає користувач, а система зберігає його в базі даних. Він є однаковим для кожної сесії. До них відносяться PIN-коди, слова, цифри, графічні ключі. Одноразові паролі – різні для кожної сесії. Це може бути SMS з кодом.

2. Комбіновані. Аутентифікація відбувається з використанням декількох методів, наприклад, парольних і криптографічних сертифікатів.

3. Біометричні. Перевірка проходить по фізіологічним характеристикам користувача, зокрема, по відбитку пальця, сітківці ока, тембру голосу, сканеру обличчя і навіть ДНК [8-10].

4. Персональні дані користувача. Вона використовується для відновлення логіна або пароля і для двоетапної автентифікації, щоб забезпечити безпеку. До цього методу відноситься номер телефону, дівоче прізвище матері, рік народження, дата реєстрації, кличка вихованця, місце проживання.

5. Інформація про користувача. Цей метод грунтується на геоданих про місцезнаходження користувача з використанням GPS, а також про точках доступу бездротового зв'язку.

Залежно від кількості методів, що використовуються, розрізняють однофакторну (використовується тільки один метод) та багатофакторну автентифікацію. В якості багатофакторної автентифікації найчастіше застосовується двохфакторна автентифікація, в якій поєднується парольний метод з іншим альтернативним методом.

Мета і задачі дослідження. Метою дослідження є багатокритеріальна оцінка альтернативних методів автентифікації суб'єктів-користувачів при проєктуванні двохфакторної автентифікації в системах захисту інформації.

Результати досліджень

Для формалізації рішення розглянутої задачі багатокритеріальної оцінки альтернатив ефективно використовуються методи підтримки прийняття рішень, зокрема декомпозиційний MAI, метою якого є декомпозиція проблеми і ієрархічне представлення її складових частин для подальшого аналізу по парним порівнянь об'єктів [11].

У найпростішому випадку схема MAI є трирівневої ієрархією, яка представлена на рис. 1 (можливі більш складні ієрархії).

Вершиною ієрархії є домінанта (мета, яка досягається при вирішенні проблеми). Проміжні рівні ієрархії зазвичай являють собою критерії, за допомогою яких оцінюються більш низькі рівні.

Найнижчий рівень представляє з себе можливі варіанти вирішення даної проблеми (альтернативи).

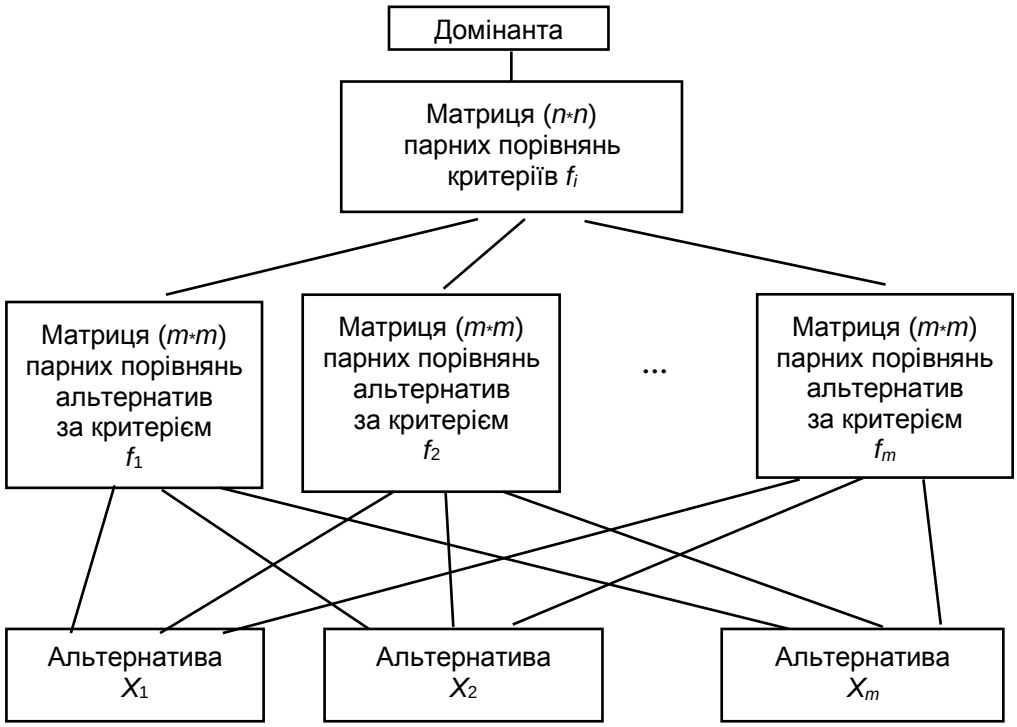

Рис. 1. Трирівнева схема ієрархії MAI

На рис. 1 представлено m альтернатив Xi ($i = \overline{1,m}$), які повинні порівнюватися за системою n локальних критеріїв f_j ($j = \overline{1,n}$) (в загальному вигляді критерії різнорідні і суперечливі).

Для проведення суб'єктивних парних порівнянь і заповнення відповідних матриць парних порівнянь (МПП) експертом використовується 9-ти рівнева шкала бальних оцінок, які відображають ступінь переваги об'єктів, що порівнюються:

1 – рівна важливість порівнюваних об'єктів;

3 – помірна перевага;

5 – істотна перевага;

7 – значна перевага;

9 – дуже сильна перевага;

2, 4, 6, 8 – проміжні значення.

Якщо можлива чисельна оцінка порівнюваних об'єктів, то результати чисельної оцінки приводяться до зазначеної шкалою. Таким чином, експертам пропонується заповнити n МПП альтернатив розмірністю $m*m$ по кожному з локальних критеріїв f_i і одну МПП локальних критеріїв розмірністю $n*n$.

Елементами МПП розглянутої ієрархії a_{ij} є результати суб'єктивних парних порівняння об'єктів нижчого рівня в термінах розглянутої вище 9-рівневої шкали.

З групи МПП нижнього рівня ієрархії формується набір локальних пріоритетів, за якими, з урахуванням МПП наступного рівня формуються глобальні пріоритети альтернатив. Рішення приймаєть-

ся на користь альтернативи, яка має максимальний глобальний пріоритет.

За отриманими МПП кожного рівня ієрархії обчислюються локальні пріоритети порівнюваних елементів згідно виразу

$$w_i = \sqrt[n]{\prod_{j=1}^{n} a_{ij}} \Big/ \sum_{l=1}^{n} \sqrt[n]{\prod_{k=1}^{n} a_{lk}} \qquad (1)$$

де n – розмір матриці парних порівнянь (кількість порівнюваних об'єктів);

a_{ij} – результат парного порівняння і-го та j-го об'єктів;

w_i – локальний пріоритет і-го об'єкта.

Таким чином, формується матриця локальних пріоритетів нижнього рівня $\mathbf{W_1}$ розмірністю $m*n$ елементів і вектор-стовпець верхнього рівня $\mathbf{W_2}$ розмірністю n елементів.

Елементи $\mathbf{W_1}$ і $\mathbf{W_2}$ визначаються по (1) для відповідних МПП. Слід зазначити, що кожен **j**-й стовпець матриці $\mathbf{W_1}$ відповідає своєму локальному критерію f_j (обчислюється по j-й МПП першого рівня), а кожний і-й рядок матриці $\mathbf{W_1}$ відповідає *i*-й альтернативі.

Вектор глобальних пріоритетів альтернатив $\mathbf{W_g}$ розмірністю m елементів визначається множенням відповідних локальних пріоритетів різних рівнів ієрархії за виразом

$$\mathbf{W_g} = W_1 \times W_2 \qquad (2)$$

Остаточним рішенням є та альтернатива X_i, для якої елемент вектору глобальних пріоритетів є максимальним $W_{gi} \to \max$.

Особливістю МАІ є обчислення індексу узгодженості I_s, який дає інформацію про рівень порушення чисельної і транзитивної узгодженості (ступінь достовірності судження експерта щодо порівнюваних елементів)

$$I_s = \frac{\sum_{i=1}^{n} w_i \times \left(\sum_{j=1}^{n} a_{ji} \right) - n}{n-1}, \qquad (3)$$

де n – розмір МПП;

a_{ij} – елементи МПП;

w_i – локальні пріоритети МПП, які визначаються по (1).

Для обчислення помилки узгодженості Δ_s, індекс узгодженості I_s ділиться на індекс узгодженості I_{ss} МПП такої же розмірності, але заповненої випадковим чином.

$$\Delta_s = I_s / I_{ss} . \qquad (4)$$

При обчисленні Δ_s по (4), використовуються табличні значення I_{ss}, які наведені в табл. 1 [11].

Таблиця 1 – **Індекси узгодженості випадкових матриць**

n	1	2	3	4	5	6	7	8	9	10
I_{ss}	0,0	0,0	0,58	0,9	1,12	1,24	1,32	1,41	1,45	1,49

Індекс узгодженості і помилка узгодженості обчислюються для кожної матриці по (3, 4). При помилці узгодженості більше 10% експерту рекомендується переглянути свої судження щодо порівнюваних об'єктів, так як величина відносних ваг може не відповідати дійсній, що може привести до побудови неадекватної моделі.

З вищесказаного випливає, що для багатокритеріальної оцінки альтернатив по МАІ необхідно задати альтернативи X_i ($i = \overline{1,m}$), і локальні критерії порівняння альтернатив f_j ($j = \overline{1,n}$), після чого побудувати ієрархію згідно рис. 1, в якій за допомогою експертів заповнити МПП.

Для побудованої ієрархії по (1) обчислити локальні пріоритети всіх рівнів, а по (2) глобальні пріоритети альтернатив.

Для двохфакторної автентифікації суб'єктів-користувачів в системах захисту інформації розглянемо розглянемо перелік альтернатив біометричних показників і критерії їх порівняння.

X_1 – Відбитки пальців. Сканери мають невеликий розмір, універсальні, відносно недорогі. Біологічна повторюваність відбитка пальця становить 10-5%. В даний час створюються архіви відбитків пальців.

X_2 – Геометрія руки. Відповідні пристрої використовуються, коли з-за бруду або травм важко застосовувати сканери пальців. Біологічна повторюваність геометрії руки близько 2%.

X_3 – Райдужна оболонка ока. Дані пристрої мають найвищу точністю. Теоретична ймовірність збігу двох райдужних оболонок становить 1 з 10^{78}.

X_4 – Термічний образ обличчя. Системи дозволяють ідентифікувати людину на відстані до десятків метрів. У комбінації з пошуком даних по базі даних такі системи використовуються для розпізнавання авторизованих співробітників і відсіювання сторонніх. Однак при зміні освітленості сканери особи мають відносно високий відсоток помилок.

X_5 – Розпізнавання по обличчю. Системи на основі даного підходу дозволяють ідентифікувати персону в певних умовах з похибкою не більше 3%. Даний метод зручний тим, що він дозволяє реалізацію штатними засобами (веб-камера). Деякі (не всі) методи мають недоліком можливість підміни реальної людини на його фотографію.

X_6 – Голос. Перевірка голосу зручна для використання в телекомунікаційних додатках. Необхідні для цього 16-розрядна звукова плата і конденсаторний мікрофон коштують менше 25$. Імовірність помилки становить 2 - 5%.

X_7 – Введення з клавіатури. Тут при введенні, наприклад, пароля відслідковуються швидкість і інтервали між натисканнями.

X_8 – Динамікою рукописного підпису. Для контролю рукописного підпису використовуються дигітайзери.

Розглянемо локальні критерії порівняння альтернатив:

f_1 – надійність ідентифікації;

f_2 – ціна додаткового обладнання;

f_3 – доступність придбання обладнання;

f_4 – наявність спеціалізованого ПЗ;

f_5 –необхідність підготовки персоналу;

f_6 – накладні витрати на встановлення та обслуговування;

f_7 – бренд виробника.

Матриці парних порівнянь нижнього рівня (порівняння альтернатив по кожному локальному критерію) заповнюються експертами один раз, незалежно від типу, призначення та конкретних вимог до системи захисту інформації. Матриці парних порівнянь верхнього рівня (порівняння локальних критеріїв) формується окремо для кожної конкретної системи з врахуванням всіх особливостей і вимог.

Висновки та перспективи подальших досліджень

У статті розроблено математичну модель двохфакторної автентифікації суб'єктів-користувачів при багатокритеріальному порівнянні альтернатив з застосування методу аналізу ієрархій. Сформовано перелік альтернатив біометричних показників та критерії їх порівняння.

Подальші дослідження направлені на програмній реалізації та практичному застосуванні розробленої моделі.

СПИСОК ЛІТЕРАТУРИ

1. Грищук Р.В. Основи кібернетичної безпеки / Р.В. Грищук, Ю.Г. Даник – Житомир: ЖНАЕУ, 2016 – 616 с.
2. Замула О.А. Нормативно-правове забезпечення інформаційної безпеки. Комплексні системи захисту інформації: Навч. Посібник / О.А. Замула, Ю.І. Горбенко, А.І. Шумов– Харків: ХНУРЕ, 2010 – 48 с.
3. Brailovskyi N. Evaluation of the Level of Cyber Security of Information / Brailovskyi N., Khoroshko V., Khokhlacheva Y., Ayasrah Ahmad // Scientific and Prac-tical Cyber Security Journal (SPCSJ), 2019 – Vol 3, N3, – pp. 18-24.
4. Дудатьєв А. В. Моделі для організації протидії інформаційним атакам / А. В. Дудатьєв // Захист інформації, 2015 – № 2. – С.157-162.
5. Горбенко І.Д. «Побудування та аналіз систем, протоколів та засобів криптографічного захисту інформації». . Монографія / І.Д. Горбенко – Харків. Форт. 2015 – 902с.
6. Шевченко В.Л. Несанкціонований доступ до інформаційних ресурсів ERP-системи / В.Л. Шевченко, В.І. Кулажський, О.С. Кульчицький // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України ім. Івана Черняховського, 2014 – № 1(50), – С. 9-12.
7. Царьов Р.Ю. Біометричні технології: навч. посіб. [для вищих навчальних закладів] / Р.Ю. Царьов, Т.М. Лемеха – Одеса: ОНАЗ ім. О.С. Попова, 2016 – 140 с.
8. Методи і технології біометричної ідентифікації за результатами літературних джерел / Л.Г. Коваль, С.М. Злепко, Г.М. Новіцький, Є.Г. Крекотень // Вчені записки ТНУ імені В.І. Вернадського. Серія: технічні науки, 2019 – Том 30 (69), Ч.1, № 2 – С. 104-112.
9. Ковтун В. В. Концепція впровадження автоматизованої системи розпізнавання мовця у процес автентифікації для доступу до критичної системи / В. В. Ковтун // Вісник Вінницького політехнічного інституту, 2018 – № 5 – С. 41–52.
10. Безик О.В. Разработка и анализ алгоритма биометрической аутентификации по рисунку кровеносных сосудов пользователя / О.В. Безик, М.А. Басараб // Молодой ученый, 2016 – № 8. – С. 116–119.
11. Саати Т. Аналитическое планирование. Организация систем / Т. Саати, К. Кернс – М.: Радио и связь, 1991 – 224 с.

Received (Надійшла) 12.02.2021
Accepted for publication (Прийнята до друку) 21.04.2021

Multi-criterial assessment of alternatives in designing of two-factor authentication of users in information protection systems

Anatoly Povoroznyuk, Anna Filatova, Oksana Povoroznyuk

Abstract. The work is devoted to solving the urgent scientific and technical problem of increasing the level of information security by designing two-factor authentication of user subjects in information security systems with a multi-criteria comparison of the components of two-factor authentication. Based on the analysis of the authentication methods of user subjects that are used in the protection of information, a lot of the most used methods and their areas of application were substantiated. **The purpose** of the study is a multi-criteria assessment of alternative methods of authentication of user subjects during designing two-factor authentication in information security systems. **Results.** The paper analyzes methods of authentication of user subjects, including perspective methods of biometric authentication in order to build two-factor authentication. For multicriteria comparison of authentication methods, the use of the hierarchy analysis method (HAM) is justified, which implements the hierarchical structure of the comparison of alternatives. At each level of the HAM, the corresponding matrices of paired comparisons are built, the elements of which are expert assessments. A system of local criteria for comparing alternatives and the corresponding matrices of paired comparisons as well as a matrix of paired comparisons of local criteria and a procedure for calculating the global criterion have been developed.

Keywords: information security, two-factor authentication, alternative, multi-criteria comparison, hierarchy analysis method, local criterion, matrix of paired comparisons, global criterion.