10. Ильясова А. В. Методические подходы к эффективному управлению ресурсным потенциалом сельскохозяйственных кредитных кооперативов / А. В. Ильясова // XXI век: итоги прошлого и проблемы настоящего, – 2013. – № 11 (15). – Т.2. – С. 248-254.
11. Кокова Э. Р. Развитие стратегии диверсификации интеграционного процесса в региональном АПК / Э. Р. Кокова // Вектор науки Тольяттинского государственного университета, 2013. – № 1 (23). – С. 184-187.

Інформаційна технологія захисту конфіденційної управлінської інформації

Кумченко Ю. О.
кандидат технічних наук, старший викладач
ДВНЗ «Криворізький національний університет»

Актуальність теми захисту конфіденційної управлінської інформації обумовлена активним збільшенням інформаційних потоків на підприємствах та інформатизацією сучасного світу. Аналіз систем контролю доступу свідчить про очевидний рух у бік біометричних технологій завдяки їх надійності та достовірності. Потрібно також зазначити, що за даними International Biometric Group та Acuity Market Intelligence проекти, згідно з якими до 2020 року дохід від мобільного біометричного ринку досягне 34,6 млрд. доларів щорічно.

Наукова задача монографії полягає у захисті конфіденційної управлінської інформації з використанням інформаційної технології (ІТ) для ідентифікації персоналу за біометричними параметрами. Задача є актуальною, оскільки її вирішення забезпечить суттєве спрощення захисту інформації, а також підвищить надійність систем безпеки на підприємствах і фінансових установах.

Об’єкт дослідження – процеси ідентифікації персоналу за біометричними параметрами.

Предмет дослідження – методи та моделі для ідентифікації персоналу.

Методи дослідження базуються на комплексному використанні фундаментальних положень, теоретичні дослідження базуються на системному підході, застосуванні методів лінійного програмування, методів спектрального аналізу, методів виділення кордонів, методів комп’ютерної графіки, підході опису інформаційних зв’язків та методології функціонального моделювання.

На основі аналізу сучасних біометричних систем розпізнавання персоналу запропоновано використати мультимодальну (бімодальну) систему ідентифікації, яка складається з двох характеристик: обличчя та голос. Ухвалення рішення про доступ користувача до конфіденційної управлін-

ської інформації являє собою логічну схему, що враховує результати всіх модулів системи ідентифікації.

Побудова математичної моделі для іт ідентифікації персоналу

Для підтримки інформаційної безпеки або контролю доступу до конфіденційної управлінської інформації, у системах біометричної ідентифікації, персоналу необхідно надати деяку кількість біометричних параметрів.

Нехай маємо *n* різних параметрів людини *P1, P2, ... ,Pn* та *m* кількість персоналу *L1, L2, ... ,Lm.* У таблиці 1 наведено кількість параметрів *Pi*, притаманних одній людині *Lj*.

Задача полягає у такому: необхідно організувати доступ персоналу до конфіденційної інформації так, щоб задовольнялася мінімальна норма для доступу *dk*, який встановлюється для кожної людини окремо, в залежності від рівня безпеки, та вартість *cr* такої системи була мінімальною.

Таблиця 1

Вихідні дані для математичної моделі ІТ ідентифікації персоналу на основі комплексу біометричних параметрів

Персонал, *m*	Біометричні параметри людини, *n*				Мінімальна норма для доступу
	P1	*P2*	…	*Pn*	
L1	*x11*	*x12*	…	*x1n*	*d1*
L2	*x21*	*x22*	…	*x2n*	*d2*
…	…	…		…	…
Lm	*xm1*	*xm2*	…	*xmn*	*dk*
Вартість системи	*c1*	*c2*	…	*cr*	

1. *X* – кількість біометричних параметрів людини.
2. Система обмежень:

$$\begin{cases} x_{11} + x_{12} + \text{K} + x_{1n} \ge d_1, \\ x_{21} + x_{22} + \text{K} + x_{2n} \ge d_2, \\ \Lambda\ \Lambda\ \Lambda\ \Lambda\ \Lambda\ \Lambda\ \Lambda\ \Lambda\ \Lambda \\ x_{m1} + x_{m2} + \text{K} + x_{mn} \ge d_k, \end{cases} \qquad (1)$$

$x_{ij} \ge 0$, де $i, j = \overline{1,n}$; $d_i \ge 0$, де $i = \overline{1,k}$.

Таблиця 2

Вирішення задачі лінійного програмування

Персонал, m /	Параметри людини для доступу, P				F
технологія доступу	*Відбиток пальця*	*Радужна оболонка*	*Пароль*	**Мін. для доступу, d**	**max**
Адміністратор системи контролю доступу 1	65	65	100	230	1056
Директор 1	60	60	100	220	1056
Охоронець 1	55	55	100	210	1056
Інший персонал 1	50	50	100	200	1056
Вартість системи, x10^4	0.6	10	0.08		
технологія доступу	*Голос*	*Обличчя*	*Пароль*		
Адміністратор системи контролю доступу 2	60	70	100	230	108
Директор 2	60	60	100	220	108
Охоронець 2	55	55	100	210	108
Інший персонал 2	50	50	100	200	108
Вартість системи, x10^4	0.2	1.1	0.08		
технологія доступу	*Вени долоні*	*Сітківка ока*	*Пароль*		
Адміністратор системи контролю доступу 3	65	65	100	230	935
Директор 3	60	60	100	220	935
Охоронець 3	55	55	100	210	935
Інший персонал 3	50	50	100	200	935
Вартість системи, x10^4	9	1.3	0.08		

	Fmin
Значення функції (умова 1 адміністратор):	697
Значення функції (умова 1 директор):	644
Значення функції (умова 1 охоронець):	591
Значення функції (умова 1 інші):	538
Значення функції (умова 2 адміністратор):	97
Значення функції (умова 2 директор):	86
Значення функції (умова 2 охоронець):	79.5
Значення функції (умова 2 інші):	73
Значення функції (умова 3 адміністратор):	677.5
Значення функції (умова 3 директор):	626
Значення функції (умова 3 охоронець):	574.5
Значення функції (умова 3 інші):	523
Найменші 4 значення:	**73;79.5;86;97**

	Pc
Відбиток пальця	80 %
Радужна оболонка	100 %
Пароль	100 %
Голос	60 %
Обличчя	80 %
Вени долоні	90 %
Сітківка ока	90 %

Нормоване значення вартості системи: C=Cr/10000
Fmax – максимальне значення функції
Fmin – мінімальне значення функції
Pc – середні статистичні показники розпізнавання

3. Мінімум цільової функції:

$$F(X) = c_1 x_1 + c_2 x_2 + \text{K} + c_r x_n \to \min. \quad (2)$$

Отже, було введено визначники для невідомих X у задачі та зафіксовано обмеження для них: $x_{ij} \geq 0,$ де $i, j = \overline{1,n};\ \ d_i \geq 0,$ де $i = \overline{1,k}$. Складено систему обмежень (1) задачі відносно мінімальної норми для доступу *dk* та цільову функцію з встановленим екстремумом: $F(X) = c_1 x_1 + c_2 x_2 + \text{K} + c_r x_n \to \min.$

Вище наведена модель належить до задач лінійного програмування, тому представлено її вирішення в пакеті Excel (табл. 2).

З розрахунку видно, що найменші 4 значення функції (73; 79.5; 86 та 97) у технології доступу, яка використовує поєднання голосу, обличчя та пароля. Обране поєднання біометричних параметрів відповідає встановленому екстремуму цільової функції (2).

Опис схеми інформаційних зв'язків розробленої іт ідентифікації персоналу на основі комплексу біометричних параметрів

Опис схеми інформаційних зв'язків виконаємо використовуючи сучасний американський стандарт NIST Special Publication 800-183 (липень 2016 р.) від National Institute of Standards and Technology [1]. Даний документ був випущений у серії SP 800, Computer Security, що має на увазі його безпосереднє відношення до інформаційної безпеки. Автором NIST SP 800-183 є Jeffrey Voas, відомий ще з початку 1990-х років публікаціями з теорії оцінювання та тестування програмного забезпечення.

У NIST SP 800-183 пропонується унікальний підхід в описі інформаційних зв'язків. Для цього використовується п'ять типів примітивів: 1) Sensor, 2) Aggregator, 3) Communication Channel, 4) External Utility (eUtility), 5) Decision Trigger (рис. 1).

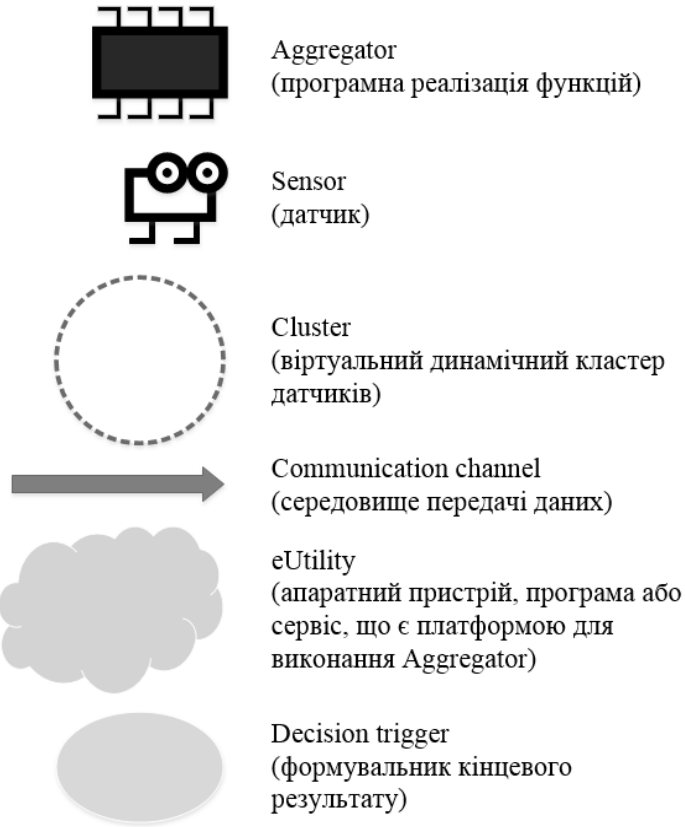

Рисунок 1 – Примітиви стандарту NIST SP 800-183

Primitive № 1: Sensor

Sensor – це датчик, призначений для вимірювання фізичних параметрів (температура, вологість, тиск, прискорення тощо).

Primitive № 2: Aggregator

Sensor передає інформацію в Aggregator, який представляє собою програмну реалізацію функцій (можливо, з використанням штучного інтелекту), що перетворюють вихідні (raw) дані в проміжні агреговані дані.

Для Aggregator введено ще поняття акторів (Actor) обробки даних двох типів: Cluster & Weight. Під Cluster мається на увазі віртуальний динамічний Cluster of Sensors, який організовується та змінюється в залежності від підходу до агрегації даних. Під Weight мається на увазі ваговий коефіцієнт (також, можливо, динамічний), який застосовується для обробки даних за допомогою Aggregator.

Primitive № 3: Communication Channel

Communication Channel представляє собою віртуальну або фізичну середу передачі даних, що об'єднує всі інші примітиви.

Primitive № 4: eUtility (External Utility)

Під eUtility мається на увазі будь-який апаратний пристрій, програма або сервіс, що є платформою для виконання Aggregator. У майбутньому передбачається конкретизувати даний примітив, виділивши кілька категорій.

Primitive № 5: Decision Trigger

Decision Trigger формує кінцевий результат, необхідний для виконання цільової функції конкретної системи [2].

Схема інформаційних зв'язків розробленої ІТ ідентифікації персоналу на основі комплексу біометричних параметрів для захисту конфіденційної управлінської інформації складається з таких компонентів: 1) U – користувач (об'єкт ідентифікації), 2) C – кластер датчиків, 3) S – датчик, 4) A – програмна реалізація функцій, 5) eU – апаратний пристрій, програма або сервіс, 6) віртуальна та фізична середа передачі даних, 7) формувальник кінцевого результату (рис. 2). Для опису невеликої ІТ кількість компонентів достатня, а при збільшенні розмірності можна застосувати ієрархічні структури.

Користувач U безконтактно надає дві свої біометричні характеристики обличчя та голос на два кластера C1 і C2, кожен з яких складається з двох сенсорів: S1, S2 – звичайна та інфрачервона камери; S3, S4 – два мікрофона. Фізично U контактує з сенсором S5 – для введення паролю.

Сенсори S1, S2, S3, S4 передають інформаційних потік від U до агрегаторів A1 та A2, які є складовими мультимодального апаратного пристрою eU1. Пристрій eU1 фізично пов'язаний двома лініями зв'язку (USB та 3,5 мм аудіо кабелем) з ЕОМ eU2.

ЕОМ eU2 містить чотири програми eU2.1, eU2.2, eU2.3, eU2.4 та підключену клавіатуру eU3, яка є платформою для агрегатора A3. eU2.1 попередньо оброблює зображення та формує еталонний зразок обличчя [3]. eU2.2 попередньо оброблює звук та формує еталонний зразок голосу. eU2.3 приймає два потоки інформації з попередньо обробленими сигналами від eU2.1, eU2.2 та потік від eU3 для локального шифрування еталонних зразків засобами CryptoJS.

Зашифровані зразки передаються до БД eU4. Агрегатор БД A7 пов'язаний із двома агрегаторами A8 та A9 хмарного сервісу eU5 (SkyBiometry – Cloud Based Biometrics API as a Service, Microsoft Cognitive Services, Google Speech), який виконує роль порівняльного алгоритму.

Веб-браузер eU2.4 (Google Chrome) отримує інформацію від eU5 у вигляді двох потоків інформації *x* та *y*, і передає дані формувальнику кінцевого результату для виконання цільової функції системи *D=f(x,y)*. На виході отримаємо результат про дозвіл або заборону доступу до конфіденційної інформації конкретного користувача U.

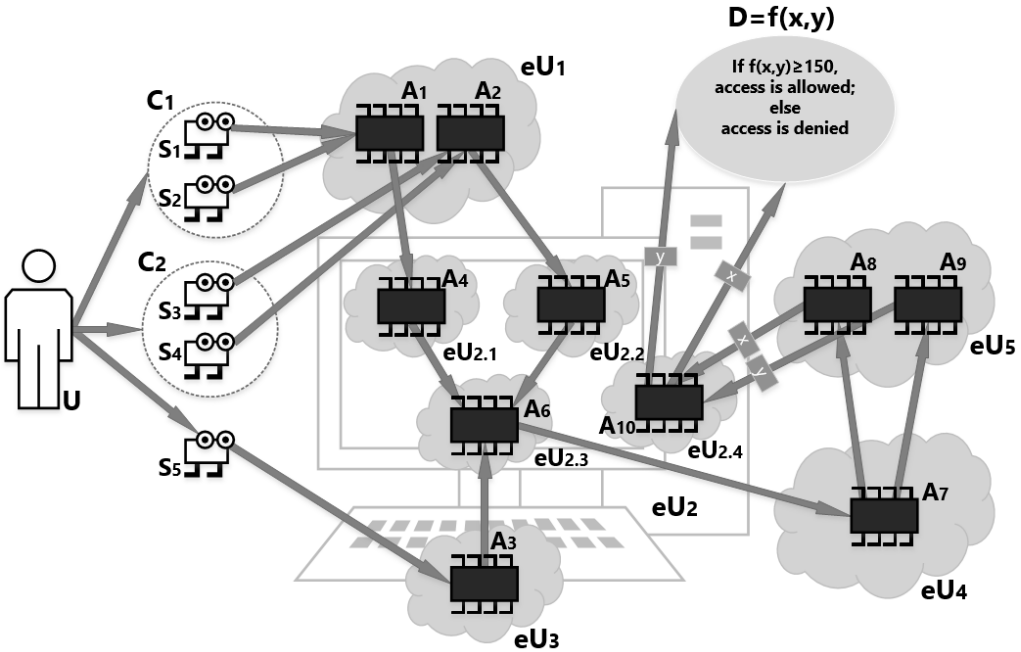

Рисунок 2 – Схема інформаційних зв'язків розробленої ІТ ідентифікації персоналу на основі комплексу біометричних параметрів

Розробка структурно-функціональної моделі ІТ ідентифікації персоналу на основі комплексу біометричних параметрів

Для розробки структурно-функціональної моделі використовуються різноманітні методики графічного представлення. Одним з них є IDEF0 [4, 5] – нотація графічного моделювання, яка використовується для створення функціональної моделі, що відображає структуру і функції системи, а також потоки інформації і матеріальних об'єктів, що зв'язують ці функції [6].

Спочатку необхідно побудувати контекстну діаграму – це сама верхня діаграма, на якій об'єкт моделювання представлений єдиним блоком з граничними стрілками. Ця діаграма називається A-0 (А мінус нуль). Стрілки на цій діаграмі відображають зв'язку об'єкта моделювання з навколишнім середовищем. Діаграма A-0 встановлює область моделювання та її границю (рис. 3).

Наступним кроком буде декомпозиція. Нотація IDEF0 підтримує послідовну декомпозицію процесу до необхідного рівня деталізації. Дочірня діаграма, створювана при декомпозиції, охоплює ту ж область, що і батьківський процес, але описує її більш детально. Згідно з методологією IDEF0 при декомпозиції стрілки батьківського процесу переносяться на дочірню діаграму у вигляді граничних стрілок (рис. 4).

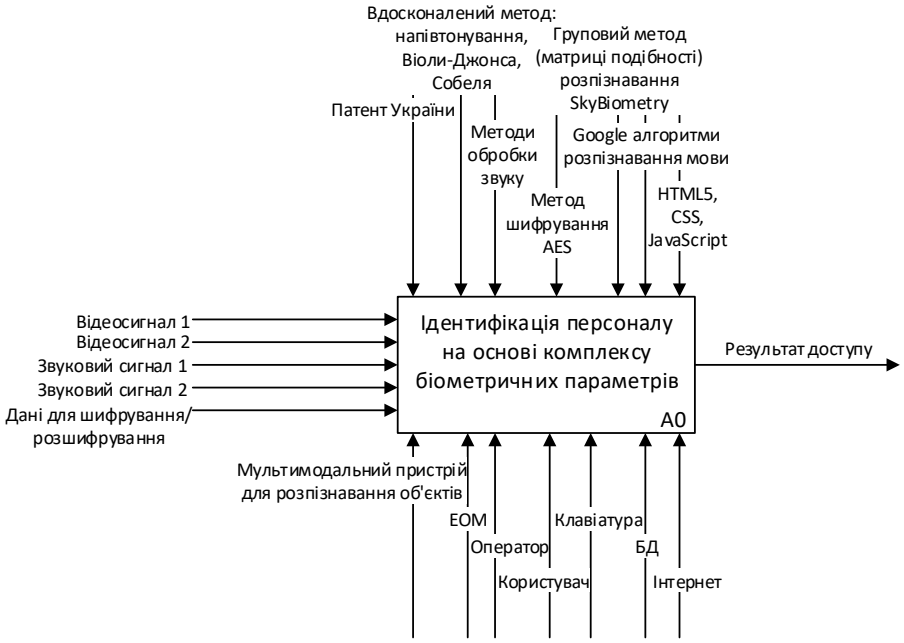

Рисунок 3 – Контекстна діаграма IDEF0 IT ідентифікації персоналу на основі комплексу біометричних параметрів

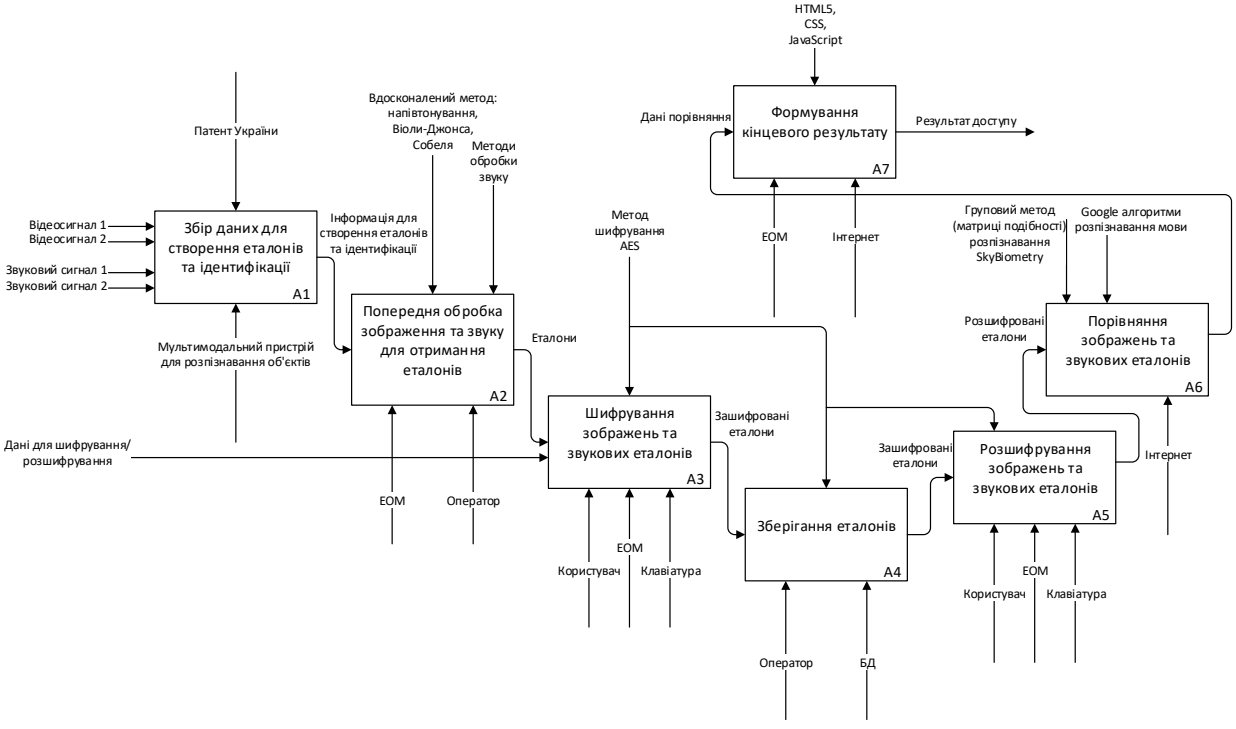

Рисунок 4 – Дочірня діаграма IDEF0 IT ідентифікації персоналу на основі комплексу біометричних параметрів

Блоки діаграми IDEF0, зі складним внутрішнім функціонуванням, потребують додаткової декомпозиції. У нашому випадку блок А2 «Попередня обробка зображення та звуку для отримання еталонів» (рис. 5) підлягає більш детального розгляду його функціонування.

Будемо вважати, що рівень декомпозиції розглянутих діаграм достатній для відображення мети моделювання, і на діаграмах нижнього рівня використовуються елементарні функції, з точки зору користувача системи.

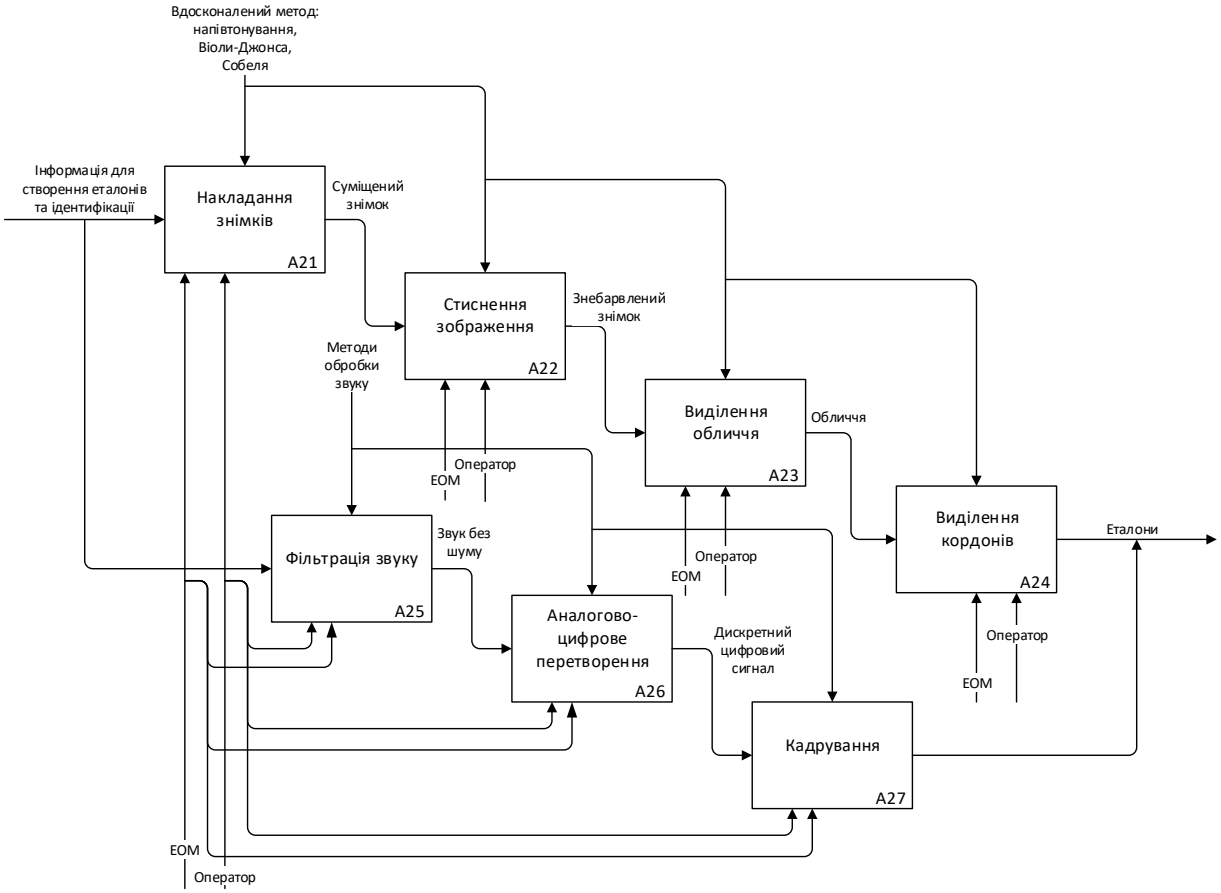

Рисунок 5 – IDEF0-діаграма декомпозиції блоку А2
«Попередня обробка зображення та звуку для отримання еталонів»

Оцінка точності роботи біометричної ІТ ідентифікації персоналу

Для оцінки точності роботи будь-якої біометричної технології прийнято використовувати характеристичну криву: DET – Detection error tradeoff (помилка виявлення, отримана при компромісному виборі параметрів), яка встановлює залежність між помилками FRR – False Rejection Rate (рівень помилкових відмов) і FAR – False Acceptance Rate (рівень помилкових дозволів) (табл. 3). Для мультимодального рішення отримаємо наступну DET-криву (рис. 6).

Отже, з таблиці 3 видно, що якщо використовувати унімодальну або мультимодальну систему в організації з кількістю персоналу:

$N = \sqrt{\frac{1}{0.0001}} = 100$ (осіб), то система з використанням голосу не пропустить 48% (FRR) персоналу, який має доступ, обличчя – 6.5% (FRR), мультимодальна – 3% (FRR).

Таблиця 3

Залежність між помилками FRR і FAR унімодальних біометричних систем та розробленої мультимодальної

№	Біометрична характеристика (ознака)					
	Унімодальна				Мультимодальна	
	Голос		Обличчя		Голос та обличчя	
	FRR, %	FAR, %	FRR, %	FAR, %	FRR, %	FAR, %
1.	48	0.01	6.5	0.01	3	0.01
2.	46	0.02	5.1	0.02	1.9	0.02
3.	42	0.05	5	0.05	1.8	0.03
4.	35	0.1	4.8	0.1	1	0.05
5.	30	0.2	4	0.2	0.9	0.07
6.	20	0.4	3	0.4	0.8	0.1
7.	18	0.5	2.2	0.5	0.8	0.2
8.	10	1	2	1	0.7	0.3
9.	7.5	2	1.5	2	0.6	0.4
10.	4	5	1	5	0.5	0.45
11.	3	10	0.48	10	0.35	0.5
12.	1.5	15	0.48	15	0.3	0.8
13.	0.9	20	0.48	20	0.25	1
14.	0.2	37	0.3	30	0.15	1.1
15.	0.02	38	0.02	42	0.02	1.2

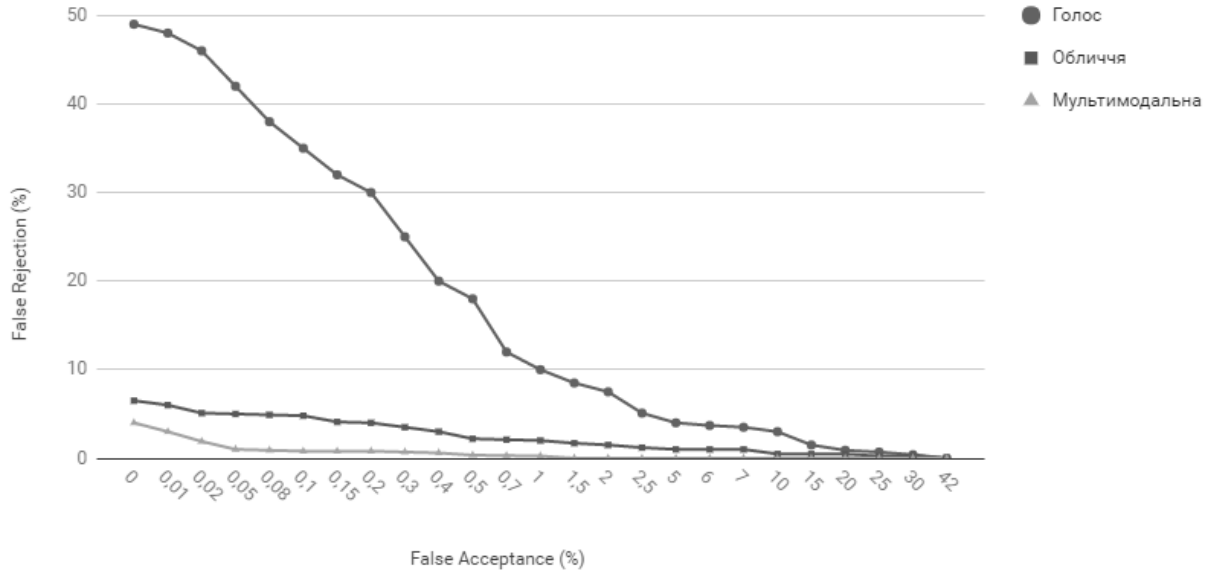

Рисунок 6 – Оцінка точності роботи біометричної системи (DET-криві)

При аналізі останнього рядка таблиці 3 (15) видно, що якщо в організації: $N = \sqrt{\frac{1}{0.01}} = 10$ (осіб), то мультимодальна система у 33 рази надійніша ніж унімодальні системи: голос – 38% (FAR), обличчя – 42% (FAR), мультимодальна (голос та обличчя) – 1.2% (FAR).

Метод шифрування для створених еталонних зразків біометричних характеристик персоналу

Метод, який буде запропоновано, дозволить користувачам ІТ вибирати еталонні зразки власних біометричних характеристик і шифрувати їх на стороні клієнта з використанням коду доступу.

У серверному коді необхідності не буде, ніяка інформація між клієнтом і сервером передаватися не буде – це підвищить довіру користувача до запропонованого методу загалом. Для реалізації використаємо HTML5 FileReader API та бібліотеку шифрування JavaScript – CryptoJS.

CryptoJS [7] є зростаюча колекція стандартних і надійних криптографічних алгоритмів, реалізованих у JavaScript з використанням передового досвіду і моделей. Вони швидкі, мають послідовний і простий інтерфейс. CryptoJS – це програмне забезпечення з відкритим вихідним кодом.

Для вирішення нашої задачі шифрування зразків для доступу до конфіденційної управлінської інформації обрано алгоритм Advanced Encryption Standard (AES) – симетричний алгоритм блочного шифрування (розмір блока 128 біт, ключ 128/192/256 біт), фіналіст конкурсу AES і прийнятий в якості американського стандарту шифрування урядом США. Вибір припав на AES з розрахуванням на широке використання і активний аналіз алгоритму, як це було з його попередником – DES. Державний інститут стандартів і технологій (National Institute of Standards and Technology, NIST) США опублікував попередню специфікацію AES 26 жовтня 2001 року, після п’ятилітньої підготовки. 26 травня 2002 року AES оголошено стандартом шифрування. Станом на 2009 рік AES є одним із найпоширеніших алгоритмів симетричного шифрування [8].

HTML5 FileReader API [9] – спосіб читання вмісту файлу або Blob (Binary Large Object – бінарний великий об’єкт) об’єкту у пам’яті. Об’єкт FileReader дозволяє нам читати вміст локальних файлів за допомогою JavaScript, але тільки тих файлів, які були обрані користувачем безпосередньо через діалогове вікно, що пропонує обрати файл. Браузери які підтримують дану технологію наведено на рисунку 7.

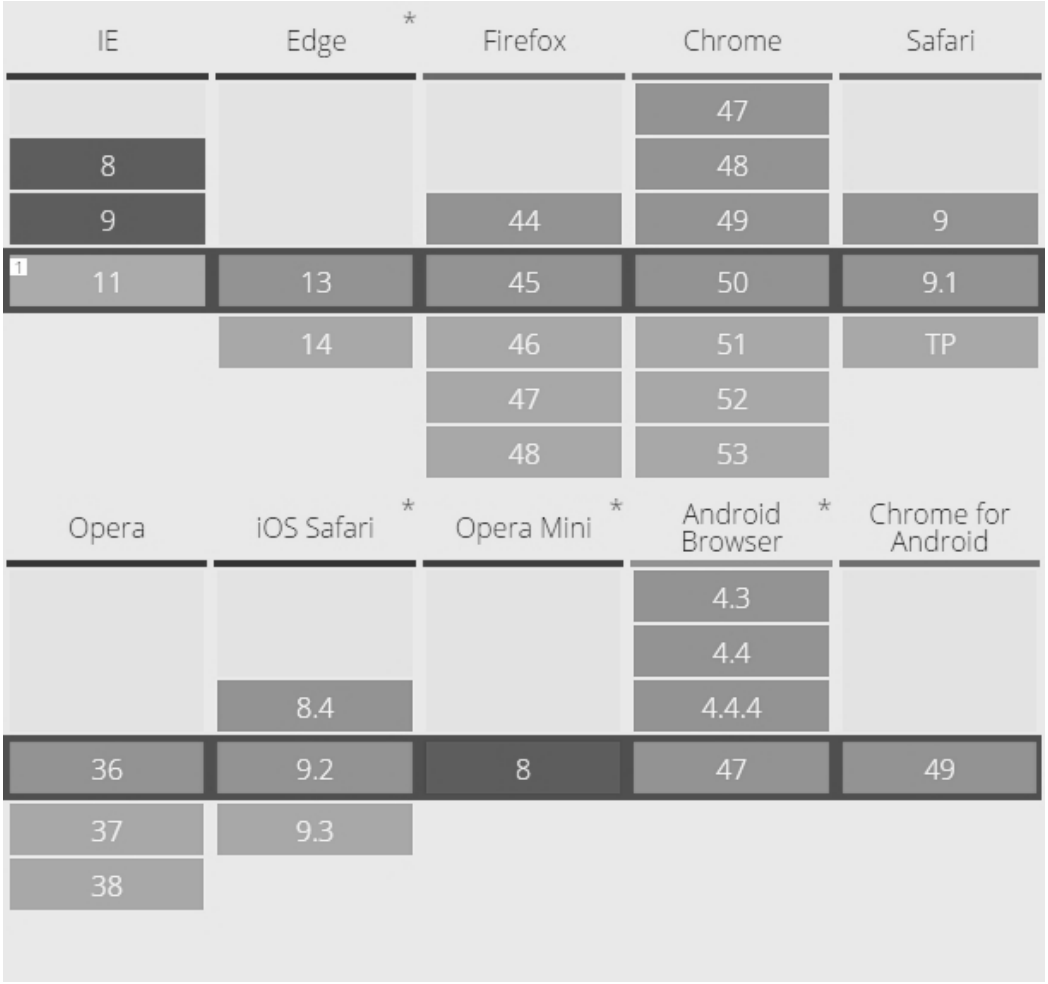

Рисунок 7 – Підтримка технології FileReader API

Після завантаження файлу еталона біометричної характеристики його вміст перетворюється на строку URI-даних. Перевага полягає в тому, що еталон зберігає свій початковий вміст безпосередньо в URI, тому ми можемо записати вміст файлу у вигляді тексту, а також додати до нього запропоноване вище шифрування с обраним паролем. Під час розшифровки відбувається зворотна процедура [10].

Для реалізації розробленого алгоритму створення еталону зображення та подальшого шифрування біометричних зразків використаємо сучасні мови Web-програмування: HTML5 та JavaScript, а також спеціальну мову CSS (каскадні таблиці стилів), щоб візуально представити сторінки, написаних мовами розмітки даних.

На рисунку 8 представлено головну сторінку створеного сайту, який має наступну структуру сторінок: головна, БД, публікації та шифрування. Структура кожної окремої сторінки містить: header (верхня частина сторінки), nav (навігаційне меню), menu (меню правої секції), body (основна частина сторінки) та footer (нижня частина сторінки).

Усього сайт використовує 14 різних стилів, які прописані у <style>… </style> та має адаптивний дизайн.

Рисунок 8 – Головна сторінка створеного сайту Kumchenko Biometry

Першим кроком при роботі з сайтом є додавання біометричної характеристики для цієї дії необхідно натиснути кнопку «Додати», а для завантаження нової – «Очистити». Після того, як біохарактеристика відобразиться у браузері, можна переходити до наступних кроків.

Другий та третій кроки – це знебарвлення та виділення області ідентифікації.

Четвертий крок – це виділення кордонів та додавання еталону до БД.

П’ятий, останній крок, реалізує шифрування еталона засобами CryptoJS.

Висновки

Використання ІТ ідентифікації персоналу, з застосуванням мультимодальних біометричних параметрів, для захисту конфіденційної управлінської інформації має суттєві переваги. Завдяки поєднання методів, що враховують відразу кілька біометричних характеристик, можна підвищити захищеність інформаційних ресурсів від несанкціонованого доступу загалом.

Розроблено математичну модель у вигляді задачі лінійного програмування з обмеженнями біометричної ІТ ідентифікації персоналу для зменшення вартості.

З розрахунку розробленої математичної моделі ІТ ідентифікації персоналу на основі комплексу біометричних параметрів видно, що найменші 4 значення функції: 73; 79.5; 86 та 97 у технології доступу, яка використовує поєднання голосу, обличчя та пароля. Обране поєднання біо-

метричних параметрів у дослідженні відповідає встановленому екстремуму цільової функції: $F(X) = c_1 x_1 + c_2 x_2 + \text{K} + c_r x_n \to \min$.

Зроблено опис схеми інформаційних зв'язків розробленої ІТ ідентифікації персоналу на основі комплексу біометричних параметрів використовуючи сучасний американський стандарт NIST Special Publication 800-183 від National Institute of Standards and Technology та розроблено структурно-функціональну модель за допомогою IDEF0-діаграм.

При оцінці точності роботи ІТ біометричної ідентифікації персоналу було встановлено, що якщо використовувати унімодальну або мультимодальну систему в організації з кількістю персоналу: 100 осіб, то система з використанням голосу не пропустить 48% (FRR) персоналу, який має доступ, обличчя – 6.5% (FRR), мультимодальна – 3% (FRR), а якщо в організації: 10 осіб, то мультимодальна система у 33 рази надійніша ніж унімодальні системи: голос – 38% (FAR), обличчя – 42% (FAR), мультимодальна (голос та обличчя) – 1.2% (FAR).

Запропоновано та реалізовано метод шифрування для створених еталонних зразків біометричних характеристик людини, який дозволяє користувачам ІТ вибирати еталонні зразки власних біометричних характеристик і шифрувати їх на стороні клієнта з використанням коду доступу. Ніяка інформація між клієнтом і сервером передаватися не буде – це підвищить довіру користувача до розробленого методу загалом.

Реалізовано розроблений алгоритм створення еталону біометричної характеристики, подальше його шифрування та зберігання шляхом використання сучасних мов Web-програмування: HTML5 та JavaScript, а також спеціальної мови CSS (каскадні таблиці стилів), щоб візуально представити сторінки, написаних мовами розмітки даних.

Список літератури

1. Voas J. NIST Special Publication 800-183 [Електронний ресурс] / Jeffrey Voas // National Institute of Standards and Technology (NIST). – 2016. – Режим доступу до ресурсу: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf.
2. Скляр В. NIST рекомендует: строительные блоки для описания IoT [Електронний ресурс] / Владимир Скляр. – 2016. – Режим доступу до ресурсу: https://habrahabr.ru/post/314956/.
3. Kupin A., Kumchenko Y. Improved Algorithm for Creating a Template for the Information Technology of Biometric Identification //Metallurgical & Mining Industry. – 2015. – №. 4.
4. Методология функционального моделирования IDEF0 [Електронний ресурс] // ИПК Издательство стандартов. – 2000. – Режим доступу до ресурсу: http://www.nsu.ru/smk/files/idef.pdf.
5. Моделирование бизнес-процессов: Нотация IDEF0 [Електронний ресурс] // Документация Business Studio. – 2016. – Режим доступу до ресурсу: http://www.businessstudio.ru/wiki/docs/v4/doku.php/ru/csdesign/bpmodeling/idef0.

6. Методология IDEF0 [Електронний ресурс] // ITteach. – 2014. – Режим доступу до ресурсу: http://itteach.ru/bpwin/metodologiya-idef0.
7. CryptoJS. JavaScript бібліотека криптографічних стандартів [Електронний ресурс] – Режим доступу до ресурсу: https://code.google.com/archive/p/crypto-js/.
8. Biryukov, Alex and Khovratovich, Dmitry. Related-key Cryptanalysis of the Full AES-192 and AES-256. – Advances in Cryptology – ASIACRYPT 2009.
9. File API [Електронний ресурс] // W3C Working Draft. – 2015. – Режим доступу до ресурсу: https://www.w3.org/TR/FileAPI/#dfn-filereader.
10. Angelov M. Creating a File Encryption App with JavaScript [Електронний ресурс] / Martin Angelov // Tutorialzine. – 2013. – Режим доступу до ресурсу: http://tutorialzine.com/2013/11/javascript-file-encrypter/.

Концепція управління ризиками в системі розвитку фінансово-економічного потенціалу залізорудного підприємства

Капканець В. С.
аспірант,
ДВНЗ «Криворізький національний університет»

Процес інтеграції України у глобальний економічний простір диктує сучасним промисловим підприємствам важкі, а й іноді досить жорсткі умови існування. З огляду на це, кожен суб'єкт господарювання не лише повинен гнучко адаптуватись до мінливих вимог зовнішнього середовища, а й враховувати вплив різного роду економічних ризиків. Особливо це стосується системи розвитку фінансово-економічного потенціалу, дієвість та збалансованість якої ґрунтується на ефективному розподілі фінансових ресурсів в умовах невизначеності. Тому, на сьогодні усе більшої актуальності набуває питання формування загальної концепції нейтралізації ризиків в процесі управління фінансово-економічним потенціалом підприємств промислових галузей господарства.

Проблема дослідження впливу економічних ризиків на перебіг процесів у будь-якій сфері діяльності являється предметом вивчення багатьох зарубіжних й вітчизняних науковців, а в системі управління фінансово-економічним потенціалом підприємств знаходить своє другорядне відображення в працях таких провідних економістів як: В. Артеменко, Є. Афанасьєв, В. Бикова, І. Бланк, Н. Гнип, Б. Данілішин, П. Єгоров, В. Ковальов, П. Комарецька, Н. Левченко, М. Мескон, Т. Момот, Б. Мочалов, В. Савчук, Ю. Сердюк-Копчекчи, Е. Сорокіна, А. Стрікленд, А. Томпсон, О. Федонін, О. Щекович та інші [1-4]. Однак, незважаючи на широке коло досліджень, присвячених означеній проблемі в цілому, ще недостатньо приділено уваги вивченню особливостей впливу ризиків на системне акумулювання, накопичення та розподіл фінансових ресурсів в господарській діяльності підприємств залізорудної галузі гірничо-металургійного комплексу України.