УДК 681.3.06:519.248.681

ПРОБЛЕМНІ ПИТАННЯ ЕЛЕКТРОННОЇ АВТЕНТИФІКАЦІЇ В СИСТЕМАХ КОНТРОЛЮ ДОСТУПУ

Д.В. ІВАНЕНКО, Є.П. КОЛОВАНОВА

В даній статті викладено результати аналізу основних напрямів здійснення електронної автентифікації та розробка відповідних пропозицій з орієнтацією на роботи в технологічно розвинених державах. Електронна автентифікація може базуватися на застосуванні криптографічних та біометричних методів. За цієї умови забезпечується необхідна якість автентифікації.

Ключові слова: електронна аутентифікація, системи контролю доступу.

В Україні та у всьому світі в цілому в галузі захисту інформації широке впровадження отримують інфраструктури з відкритими ключами. Створення інфраструктури дозволяє вирішити ряд питань: забезпечити надання користувачам базових послуг таких як конфіденційність, цілісність, доступність, але залишаються відкритими та актуальними задачі, що пов'язані з електронною ідентифікацією та автентифікацією суб'єктів та об'єктів. На сьогодні виникає необхідність мати гарантії особи, що звернулася до системи, і забезпечити належний рівень автентифікації, як особи, що сформувала запит до системи, так і сформованої відповіді на електронний запит.

У нинішній час цьому напряму призначається значна увага. У світі вирішенням цієї задачі займаються декілька країн, але кожна з них використовує різні підходи. Метою цієї статті є викладення результатів аналізу основних напрямів здійснення електронної автентифікації та розробка відповідних пропозицій з орієнтацією на роботи в технологічно розвинених державах.

Найвпливовішим поштовхом вирішення цього питання у США можна назвати Президентську Директиву США про внутрішню безпеку (HDSP-12). Очікувалось, що директива змінить становище ринку негайно, але проблеми фінансування проекту та ненадходження відповідного сертифікованого обладнання призвело до зниження темпів впровадження. З часом уряд почав більше приділяти уваги цьому питанню – зріс бюджет, до директиви почали прислухатися комерційні організації, внаслідок, зріс попит та приплив позабюджетних коштів. Основна робота направлена на автентифікацію, управління конфіденційними даними та контроль доступу до даних, синхронізацію облікових записів тощо. Найбільш вагомим результатом є розробка та прийняття федерального стандарту США FIPS 201, який висуває вимоги до електронних даних осіб, життєвих циклів посвідчень тощо.

У Великобританії напрям застосування був більш комерційний, за що набув широкого попиту. Британською асоціацією індустрії безпеки розробляються рекомендації до використання систем контролю доступу на виробництвах. Ці рекомендації розкриватимуть загальні характеристики побудови таких систем, будуть підкреслювати особливі моменти (положення) національного та міжнародного стандартів, що регламентують використання систем контролю доступу.

У РФ значна увага приділяється методам та механізмам автентифікації. Посилаючись на досвід інших країн у розв'язанні задач контролю доступу, зрозуміло, що найактуальнішим питанням є електронна автентифікація особи. Роблячи на цьому акцент, було розроблено та прийнято відповідний стандарт ГОСТ Р 52633-2006 «Требования к средствам высоконадежной биометрической аутентификации».

Можна стверджувати, що всі країни-розробники систем контролю доступу до даних прийшли до висновку, що необхідно приділяти особливу увагу електронній автентифікації. Надійність такої автентифікації можна забезпечити з використанням, наприклад, біометричних характеристик людини. Це насамперед стало можливо завдяки деяким перевагам цієї технології:

• біометричні шаблони важко фальсифікувати;

• в силу унікальності біометричних характеристик достовірність автентифікації за біометричними даними дуже висока;

• біометричний ідентифікатор не можна забути або загубити, як пароль чи картку.

З розвитком технологій розроблені та знаходять використання різні біометричні методи автентифікації. Характеристики найбільш розповсюджених методів автентифікації за біометричними параметрами людини наведені в табл. 1.

Таблиця 1

Біометричні методи

Біометричний метод	FAR (імовірність допуску «іншого»), %	ERR (імовірність відмови від допуску «свого»), %	Час верифікації, с
Геометрія обличчя	0,1	0,1	1
Параметри сітківки ока	0,0001-0,00078	0,4 - 0,00066	1,5 - 4
Відбиток пальця	0,1-0,0001	0,01-3	0,5 – 3
Геометрія руки	0,0001	1	2
Райдужна оболонка	0,01	0,18	-

Проведений аналіз показав, що при розробці кожного з цих методів виникають проблеми: нечіткість відтворення біометричних даних, нерівномірний розподіл біометричної інформації. Також в процесі використання треба враховувати наступні складності:

• при використанні динамічних біометричних даних потрібно враховувати залежність фізичного та емоційного стану особи;

• біометричні дані не є секретними, оскільки люди залишають їх повсюди (наприклад, відбитки пальців).

Наші дослідження показали, що незважаючи на всю різноманітність методів біометрії, самим розповсюдженим залишається такий метод як відбитки пальців (майже 60% ринку біометрії). При виборі оптимального методу акцент робиться на економічні показники (витрати), мобільність (малогабаритність устаткування), стійкість, і проаналізувавши залежність (див. рис. 1) цих показників вибір пав на метод відбитків пальця. Наш вибір автентифікації за відбитком пальців підтверджується вибором США біометричного методу для стандарту (FIPS 201).

Розгортаючи системи контролю доступу потрібно звертати увагу на розмежування доступу для більш якісного захисту. Слушний метод вирішення саме цього питання було запропоновано США та затверджено у стандарті FIPS 201. Насамперед стандарт передбачає введення своїх рівнів гарантії автентифікації особи (табл. 2.):

– довіра базового рівня, коли забезпечується базовий ступінь гарантії справжності (автентичності) особи;

– довіра вищого рівня, коли забезпечується суттєво підвищений ступінь гарантії справжності (автентичності) особи;

– дуже високий рівень, коли забезпечується надвисокий ступінь гарантії справжності (автентичності) особи.

Таблиця 2

Рівні гарантії

Рівні електронної автентифікації		Зіставні PIV Рівні запевнення
Номер Рівня	Опис	
Рівень 2	Деяка довіра до заявленої перевіреної особи	ДЕЯКА довіра
Рівень 3	Висока довіра до заявленої перевіреної особи	ВИСОКА довіра
Рівень 4	Дуже Висока довіра до заявленої перевіреної особи	ДУЖЕ ВИСОКА довіра

FIPS 201 пропонує розмежувати доступ на фізичний та логічний, також до кожного з них він рекомендує свої механізми автентифікації (див. табл.3. та табл.4.). Залежно від рівня гарантії стандарт пропонує різні механізми автентифікації особи, розповімо про кожний з ростом складності:

• VIS – механізм автентифікації, що ґрунтується на використанні візуальних посвідчень, як правило підтримується для управління доступу до фізичних ресурсів та засобів;

• CHUID – механізм автентифікації, що ґрунтується на використанні унікального ідентифікатора утримувача картки, який доступний як з контактних, так і без контактних інтерфейсів;

• Механізм автентифікації з використанням біометричної автентифікації, в залежності від доступу поділяється на два типа:

1. BIO – автентифікація на основі біометричної інформації без контролю зі сторони служби безпеки;

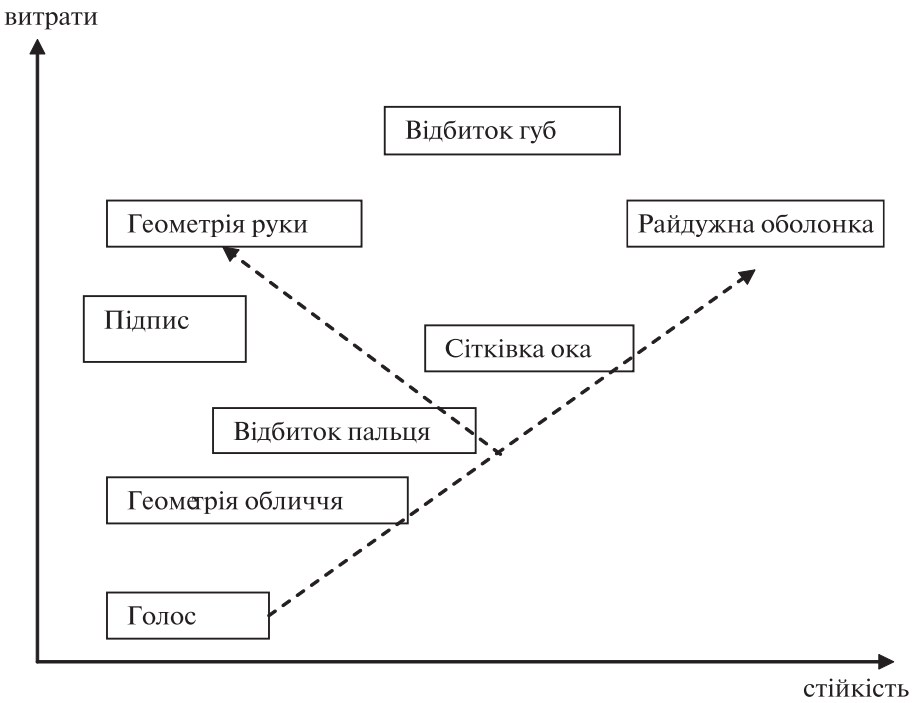

Рис. 1. Залежність вибору біометричного методу від рівня стійкості та витрат на його впровадження

2. BIO-A – автентифікація на основі біометричної автентифікації з контролем зі сторони служби безпеки (наприклад, за ходом автентифікації спостерігає інспектор або адміністратор з безпеки).

• PKI – механізм автентифікації з використанням асиметричних криптографічних перетворень.

Таблиця 3

Логічний доступ

Рівень гарантій	Механізм автентифікації, що застосовується	
	середовище локальної робочої станції	середовище віддаленої мережевої системи
Довіра базового рівня	CHUID	PKI
Довіра вищого рівня	BIO	
Довіра дуже високого рівня	BIO-A, PKI	

Таблиця 4

Фізичний доступ

Рівень гарантій	Механізм автентифікації
Довіра базового рівня	VIS, CHUID
Довіра вищого рівня	BIO
Довіра дуже високого рівня	BIO-A, PKI

Перевагою даної структури є теще механізми автентифікації вищого рівня гарантії можуть бути застосовані до нижчого рівня гарантії, кожен механізм може бути додатково посилений використанням інфраструктурою верифікації стану сертифіката. Таким чином, США була зроблена кропітка робота по розробленню оптимальних рекомендації щодо створення систем контролю доступу, які були направлені на створення своїх рівнів гарантії, та полегшив вибір механізмів ідентифікації та автентифікації при створенні аналогічної системи.

В роботі розглянуто проблемні питання систем контролю доступу при їх розробці та використанні, був досліджений досвід інших країн, які вже використовують систем контролю доступу. Насамперед стало зрозуміло, що значну увагу слід приділяти електронній автентифікації, для чого необхідно врахувати такі фактори, як:

• рівні гарантії;

• доступ;

• механізми автентифікації, відповідно до наведених вище факторів.

З проведеного аналізу можна зробити висновок, що на теперішній час актуального стає автентифікація за біометричними ознаками. Враховуючи такі фактори, як рівень стійкості та витрати на впровадження біометричного методу, найбільш актуальним та перспективним є автентифікція за відбитками пальців.

Література:

[1] FIPS PUB 201.Personal Identity Verification (PIV) of Federal Employees and Contractors. 2006

[2] HDSP-12. Homeland Security Presidential Directive 12.2003

[3] British Security Industry Association. http://www.bsia.co.uk/

[4] ГОСТ Р 52633-2006 Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации.

[5] Биометрическая защита.http://www.securitylab.ru/contest/387619.php

Надійшла до редколегії 18.06.2010.

Іваненко Дмитро Вікторович, аспірант кафедри безпеки інформаційних технологій ХНУРЕ. Область наукових інтересів: інформаційні технології, захист інформації, методи та засоби автентифікації даних.

Колованова Євгенія Павлівна, асистент кафедри безпеки інформаційних технологій ХНУРЕ. Область наукових інтересів: інформаційні технології, захист інформації, методи та засоби автентифікації даних, розпізнавання зображень

УДК 681.3.06:519.248.681

Проблемные задачи электронной аутентификации в системах контроля доступа / Д.В. Иваненко, Е.П. Колованова // Прикладная радиоэлектроника: научн.-техн. журнал. – 2010. Том 9. № 3. – С. 401-403.

В статье изложены результаты анализа основных направлений осуществления электронной аутентификации и разработка соответствующих предложений с ориентацией на применение в технологически развитых государствах. Электронная аутентификация может базироваться на применении криптографических и биометрических методов. При этом условии обеспечивается необходимое качество аутентификации.

Ключевые слова: электронная аутентификация, системы контроля доступа.

Табл. 03. Ил.01. Библиогр.: 05 назв.

UDC 681.3.06:519.248.681

Problem issues of electronic authentication in access control systems / D.V. Ivanenko, I.P. Kolovanova // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 401-403.

The paper presents the results of analyzing the main trends of electronic authentication implementation and development of appropriate proposals oriented on the implementation in technologically developed countries. Electronic authentication can be based on applications of cryptographic and biometric methods. The required quality of authentication is provided under this condition.

Key words: electronic authentication, access control systems.

Tab. 03. Fig. 01. Ref.: 05 items.