

УДК 004.75:339.722

Книш В.В.¹, Воскобойник В.О.²

¹ студ. гр. РТ-719, НУ «Запорізька політехніка»

² канд. техн. наук, проф. НУ «Запорізька політехніка»

ЗАСОБИ ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧА ІНФОРМАЦІЙНИХ РЕСУРСІВ

З появою цифрових даних з'явилося і питання з приводу безпеки цих даних. З того часу з'явилася велика кількість способів забезпечення безпеки.

Одним із найефективніших засобів захисту даних був і залишається захист паролем. Тут все просто: чим складніше пароль, тим складніше його буде зламати, але з цього виходять деякі проблеми: чим складніше буде пароль та чим більше додатків будуть вимагати введення пароля, тим вище ймовірність того, що користувачі будуть використовувати один і той же пароль, до того ж записуючи його, що дуже збільшує шанси на те, що захист буде зламано.

Рішень цієї проблеми має достатньо варіантів. Наприклад, була винайдена двоетапна аутентифікація. Основною перевагою такої аутентифікації є наявність фізичного ключа і PIN-коду до нього, що забезпечує додаткову стійкість до злому. Слід зазначити, що втрата апаратного ключа не тягне за собою компрометацію пароля, оскільки, крім ключа, для доступу до системи потрібен ще PIN-код до ключу.

Окремо варто розглянути системи з застосуванням разових паролів, які набувають все більшого поширення в зв'язку з широким розвитком інтернет-технологій, і системи біометричної аутентифікації. В даний час основним способом захисту інформації від несанкціонованого доступу (НСД) є впровадження так званих засобів AAA (Authentication, Authorization, Accounting - аутентифікація, авторизація, управління правами користувачів). При використанні цієї технології користувач отримує доступ до своїх даних лише після того, як успішно пройшов процедури ідентифікації і аутентифікації.

До складу електронних систем ідентифікації і аутентифікації входять контактні і безконтактні смарт-карти і USB-ключі (USB-token). USB-ключі

працюють з USB-портом комп'ютера і виготовляються у вигляді брелків. Такі засоби, також, знайшли себе у вигляді карток-пропусків і безконтактних ключів. Безконтактні смарт-карти широко використовуються в різних додатках як для аутентифікації: режим електронного пропуску, електронний ключ до дверей, для різного роду транспортних, ідентифікаційних, розрахункових і дисконтних програм. Важливою властивістю безконтактних карт, що виділяють її з ряду інших смарт-карт, є відсутність механічного контакту з пристроєм, що обробляють дані з карти. Фактично надійність технічних елементів систем, що їх використовують, визначається надійністю мікросхем. Це призводить до істотного зниження експлуатаційних витрат на систему в порівнянні з аналогічними системами, які застосовують смарт-карти з зовнішніми контактами

Але, всі ці методи захисту не є такими надійними, як біометричні засоби. Біометрія - це ідентифікація користувача по унікальним, властивим тільки йому одному біологічним ознакам. Такі системи є найзручнішими, з точки зору самих користувачів, оскільки не потрібно нічого запам'ятовувати, а втратити біологічні характеристики вельми складно.

При біометричній ідентифікації в базі даних зберігається цифровий код, асоційований з певною людиною. Сканер або інший пристрій, що використовується для аутентифікації, зчитує конкретний біологічний параметр. Далі він обробляється за певними алгоритмами і порівнюється з кодом, що містяться в базі даних. До переваг біометричних сканерів зазвичай відносять те, що вони ніяк не залежать від користувача (наприклад, користувач може помилитися при введенні пароля) і користувач не може передати свій біологічний ідентифікатор іншій людині, на відміну від пароля.

Всі біометричні технології можна розділити на дві групи: статичні методи та динамічні. Статичні методи ґрунтуються на фізіологічній (статичній) характеристиці людини, тобто унікальній властивості, властивому йому від народження і невід'ємне, це форма долоні, відбитки пальців, райдужна оболонка, сітківка ока, форма обличчя, розташування вен на кисті руки. Динамічні методи, які ґрунтуються на поведінковій характеристиці людини - особливості, характерних для підсвідомих рухів в процесі відтворення якого-небудь дії.

Проаналізувавши різні технології апаратно-програмної та паролльної аутентифікації, можна зробити висновок, що застосування паролів все менше відповідає вимогам безпеки, так як зі збільшенням складності пароля і кількості паролів для запам'ятовування буде зростати роль людського фактору. Користувачі завжди будуть вибирати найбільш прості, з їх точки зору, методи ідентифікації. Тому, враховуючи, поширення діджиталізації, повинно знаходити універсальні і зручні засоби ідентифікації користувачів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Нікифоров С.Н. Методи захисту інформації. Шифрування даних. Видавництво «Лань», 2016.–160 с.