УДК 004.056

С.І. Болобан, О.М. Перегуда, В.В. Умінський

Житомирський військовий інститут ім. С.П. Корольова НАУ, Житомир

МЕТОДИ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

В статті розглянуто особливості найбільш розповсюджених методів аутентифікації користувачів інформаційно-комунікаційних систем. Визначено перелік критеріїв для оцінки якості систем аутентифікації, які побудовані на основі цих методів. Детально розглянуто наступні методи аутентифікації: статичні й одноразові паролі (символьні та графічні), біометричні методи, методи засновані на використанні переносних пристроїв для аутентифікації (токенів та смарт-карт). Проведено порівняльний аналіз методів аутентифікації, визначено переваги та недоліки розглянутих методів, перспективи їх подальшого розвитку.

Ключові слова: *аутентифікація, символьний пароль, графічний пароль, біометрія, токен.*

Вступ

Постановка проблеми. Кожний користувач сучасних інформаційно-комунікаційних систем декілька разів на день стикається з процедурами ідентифікації та аутентифікації. Ці процедури виконуються кожний раз, коли користувач вводить пароль для доступу до інформаційної системи, до мережі, до бази даних або при запуску прикладної програми. В результаті їх виконання оператор або отримує доступ до певних ресурсів інформаційної системи, або ні. Процедура аутентифікації користувача є обов'язковим етапом функціонування будь-якої сучасної інформаційно-комунікаційної системи.

Існує декілька методів аутентифікації, які різняться своєю складністю, надійністю, вартістю та іншими показниками. Кожний з цих методів має свої позитивні та негативні сторони, аналізу яких присвячена дона робота.

Аналіз останніх досліджень і публікацій. Аналіз робіт [1-4, 10], присвячених порівнянню відомих методів аутентифікації, дозволив виявити ряд недоліків цих робіт: обмежене коло розглянутих методів, відсутність чітко визначених показників оцінки їх якості, відсутність системності при проведені оцінювання (оцінювання всіх методів за всіма визначеними критеріями), відсутність, в більшості випадків, кількісних характеристик (оцінки виражені в нечіткій лінгвістичній формі), велика доля суб'єктивізму при оцінюванні зумовлена в тому числі комерційними (маркетинговими) інтересами.

Метою статті є аналіз і систематизація на базі визначених показників переваг та недоліків сучасних методів аутентифікації користувачів інформаційно-комунікаційних систем, визначення подальших перспектив розвитку зазначених методів.

Основний матеріал

Для вирішення задачі порівняльного оцінювання методів аутентифікації користувачів перш за все необхідно визначитись з вичерпним переліком показників, за якими будуть оцінюватись системи аутентифікації. За результатами аналізу досліджень, проведених в [1-2, 4, 10], запропоновано наступні показники:

1. Стійкість до перебору.
2. Захищеність від підглядання.
3. Захищеність від викрадання аутентифікатора за допомогою програмних закладок.
4. Захищеність у разі викрадання матеріальних носіїв, на яких зберігається аутентифікатор.
5. Вартість системи аутентифікації.
6. Простота запам'ятовування аутентифікатора.
7. Простота зміни аутентифікатора.
8. Простота процедури аутентифікації.
9. Завадозахищеність системи аутентифікації (рівень похибок першого та другого роду).
10. Можливість використання аутентифікатора не уповноваженим суб'єктом.
11. Стійкість до дій зовнішніх факторів: температура, волога, механічне пошкодження.

Через те, що в роботі проводиться саме порівняльний аналіз систем, в ній не розглядаються традиційні вимоги до системи аутентифікації: відношення часу зламу системи аутентифікації до часу старіння інформації, яка захищається, а також відношення вартості системи аутентифікації до вартості інформації, яка захищається.

Проведемо оцінку основних методів аутентифікації користувачів за визначеними показниками. Розглянемо наступні групи методів

аутентифікації: статичні й одноразові паролі, біометричні методи та методи засновані на використанні переносних пристроїв аутентифікації.

Статичні й одноразові паролі

Символьні паролі. Найбільш розповсюдженою системою аутентифікації є використання паролю у вигляді набору букв, цифр та спеціальних символів. Кожна організація, з метою підвищення захищеності своїх інформаційних ресурсів, вимагає від співробітників при створенні паролів виконання певних умов:

обмеження мінімальної довжини паролю;

відсутність відношення паролю до користувача (прізвище, ім'я дітей, дати народження тощо);

комбінація верхнього, нижнього регістрів та спеціальних символів;

примусова зміна паролю через певні проміжки часу тощо.

Зазначені умови значно ускладнюють пароль з погляду можливості його запам'ятовування, та вимагають певних зусиль для його визначення. В результаті користувачу доводиться або записувати пароль на матеріальному носії інформації, що підвищує імовірність його викрадення, або нехтувати виконанням певних умов, що призводить до спрощення паролю та підвищення ймовірності його підбору. Крім того, у випадку, коли пароль не складно запам'ятовується, особливо при рідкому його застосуванні, він забувається.

Процес введення паролю досить простий та швидкий, але незахищений від простого підглядання, або знімання на скрито розташовану відеокамеру.

Яким складним не був би пароль, існує дві можливості його зламу (не враховуючи варіанти підглядування та викрадення з матеріальних носіїв): шляхом автоматичного підбору всіх можливих комбінацій знаків та використовуючи програмну закладку («троянський кінь», «руткіт»), яка викрадає пароль із спеціальної області операційної системи.

Для боротьби із системами автоматичного підбору необхідно збільшувати кількість можливих комбінацій знаків, що призведе до збільшення необхідного часу для виконання операцій перебору всіх можливих варіантів. За цей час інформація застаріє і буде не актуальною або буде змінений пароль і всю процедуру необхідно буде розпочати знову.

Зазвичай для оцінки стійкості паролю застосовують формулу Андерсена [3]. Але в даній статті для порівняння систем аутентифікації використаємо такий показник, як кількість можливих комбінацій знаків, який напряму пов'язаний з необхідним часом для зламу паролю, а значить і зі стійкістю паролю. Його розрахунок здійснимо за виразом:

$$x = m^n,$$

де x – кількість можливих комбінацій паролю; m - довжина алфавіту; n – довжина паролю.

Зазвичай, довжина паролю обмежується в 6-8 символів. Пароль може складатись з цифр, спеціальних символів, букв латинського або українського алфавіту з використанням верхнього та нижнього регістрів, тобто символів, що складають таблицю ASCII. Всього таких символів 224. Це і є довжина алфавіту. Тоді при довжині паролю 8 символів, кількість можливих комбінацій символів становить $6{,}3\times10^{18}$.

Для боротьби з програмними закладками необхідно використовувати антивірусні програми.

Виникнення помилок першого та другого роду при використанні парольної системи аутентифікації можливе лише у випадках порушення правильної роботи системи аутентифікації і призводить, в першому випадку, до обмеження користувача в правах доступу до певних ресурсів (на доступ до яких він має право), а у другому випадку - до надання суб'єкту прав доступу до певних ресурсів (на що він прав не має).

Іншим недоліком системи парольної аутентифікації є те, що пароль, насправді, дозволяє аутентифікувати не конкретний суб'єкт, а лише зафіксувати відповідність аутентифікатора суб'єкта його ідентифікатору, тобто пароль може беззастережно використовувати будь-який суб'єкт, незважаючи на те, яким чином він його отримав.

Функції символьної парольної аутентифікації вбудовані в більшість операційних систем, тому побудова системи парольної аутентифікації на їх основі не потребують додаткових витрат.

Графічні паролі. Проблема суміщення легкості запам'ятовування, з одного боку, та високого рівня стійкості пароля до відтворення, з іншого, призвела до появи системи аутентифікації на основі графічних зображень. Психофізіологія людини така, що наш мозок здатен до зберігання великої кількості графічної інформації – в порівнянні з символьними паролями графічні легше і на більш довгий час запам'ятовуються, а тому з меншою ймовірністю потребують збереження їх на матеріальних носіях. Але навіть записаний на матеріальному носії графічний пароль в окремих випадках досить складно інтерпретувати. Графічні дані в електронному вигляді представляють мільйони байтів інформації і забезпечують великі можливості для унікальності вибору паролю.

Існує декілька варіацій систем на основі графічного паролю.

Графічний пароль (I). Перший варіант графічного паролю передбачає використання мнемонічної пам'яті. Такий варіант, наприклад,

реалізований в програмі ImagiPass 1.1 [5]. Запропонований метод передбачає генерацію строкового паролю (і подальше його використання як звичайного строкового паролю) на основі комбінації декількох графічних образів, які послідовно вводить користувач (в якості образів можуть бути використані малюнки із звірами, технікою, графічними фігурами тощо).

Перевагою даного методу є те, що комбінацію картинок набагато легше запам'ятати, ніж складну послідовність символьного паролю. До того ж, використовуючи мінімальну графічну комбінацію з 4-х образів (всього їх 64 для ImagiPass 1.1) можна досягти довжини генерованого ключа у 64 символи (довжина визначається користувачем). Алфавіт генерованого ключа складає 224 символи (згідно таблиці ASCII, як для символьного паролю) – тобто складність ключа набагато вища, ніж комбінація графічних образів для його генерації. Але звідси і недолік даного методу – якщо зловмисник знає, яку саме програмну реалізацію генератора використовує користувач, то злам паролю зводиться до простого перебору серед комбінацій графічних образів.

Система аутентифікації на основі графічного паролю (I) не захищена від викрадення паролю шляхом його простого підглядання (або зйомки на відеокамеру) в процесі введення. В процесі безпосереднього введення паролю (або його зміни) можливе викрадення паролю за допомогою програмних закладок.

Графічний пароль (II). В даному випадку користувач повинен здійснити короткострокові натиснення маніпулятором «миша» в декількох (трьох, чотирьох, п'яти – все залежить від необхідної стійкості паролю) точках (в межах заданої похибки) на великій фотографії (рисунку) [9].

Пароль, що запам'ятовується користувачем, описати одним словом неможливо. Це зорові уявлення, згадки та асоціації. Але вони надійні.

Враховуючи те, що при використанні графічного паролю в якості парольної інформації зберігаються координати пікселей екрану, то цю інформацію, як і при символьному паролі, можна підібрати або викрасти програмною закладкою. Для оцінки стійкості графічного паролю до перебору, як і при використанні символьного паролю, проведемо розрахунок кількості можливих комбінацій знаків.

Знаком, в даному випадку, вважається піксел екрану, який характеризується координатами на площині. Тоді і довжина алфавіту буде визначатись кількістю пікселів екрану. В найгіршому випадку кадр уміщує 640×480 пікселів. Задамо величину похибки попадання в заданий точку на рівні 5 пікселів в будь-яку сторону. Тоді довжина алфавіту, з якого буде складатися пароль, становить 64×48 точок, тобто 3072 елементи. Якщо прийняти, що довжина паролю становить 8 точок, то кількість можливих комбінацій символів буде складати $7{,}9\times10^{27}$, що на 9 порядків більше ніж при символьному паролі. Теоретично можливий злам графічного паролю (II) шляхом перебору варіантів, але для цього потрібно точно знати величину допуску зони натискання (а вона може бути різною для кожного за порядком кліку) і використовувати спеціальне програмне забезпечення (аналогів якого на даний час не відомо).

У випадку використання системи аутентифікації на базі графічного паролю (II) можливе викрадення паролю шляхом підглядання (запису на відеокамеру) і знову таки через неточне знання величини допуску зони натискання (для кожного за порядком кліку) використання отриманої інформації в подальшому дещо ускладнюється.

Якщо розглядати варіант викрадення парольної інформації за допомогою програмної закладки, то, на відміну від символьного паролю, коли цю інформацію достатньо ввести в рядок введення паролю, при графічній системі аутентифікації необхідно ще знайти точки з заданими координатами на екрані, що також ускладнює процес зламу системи.

Можливо ускладнити даний вид паролю за рахунок використання подвійних та потрійних кліків, змінного алгоритму (послідовності) натискання по контрольним точкам.

Графічний пароль (III). Третя система має ще кращі властивості, щодо захищеності від злому. Суть її полягає в переконанні системи, що ви дійсно знаєте пароль [9].

При створенні паролю користувачу пропонується вибрати та запам'ятати декілька піктограм з певної кількості можливих. При необхідності введення паролю система видає на екран певну кількість піктограм, які випадково змішані, серед яких обов'язково присутні три, обрані користувачем. Для введення паролю їх необхідно об'єднати в трикутник і здійснити короткострокове натиснення маніпулятором «миша» всередині трикутника. Після цього піктограми перемішуються, одні зникають, інші з'являються і процедура повторюється знову. Так відбувається декілька раз, тому процес введення паролю, в даному випадку, можна охарактеризувати як найбільш складний та довгий за часом, порівняно з іншими методами аутентифікації.

Сам пароль в процесі його введення не показується, тому підглядати його безглуздо. У випадку зйомки процесу введення паролю на відеокамеру визначення паролю можливе лише після складного аналітичного аналізу результатів зйомки (можливо з використанням спеціального програмного забезпечення, аналогів якого на

теперішній час не відомо). Крім того, як і в попередній системі, пароль неможливо (або надто складно) записати на матеріальному носії, що зменшує імовірність його викрадення або втрати.

Викрадення графічного паролю (ІІІ) з використанням програмних закладок неможливе у зв'язку з тим, що в явному вигляді пароль не зберігається і не вводиться.

Виникнення помилок першого та другого роду при використанні графічних паролів можливе лише у випадках порушення правильної роботи системи аутентифікації, так як і для символьних паролів.

Як і в системах символьної парольної аутентифікації графічний пароль пов'язаний лише з ідентифікатором суб'єкта, а не з самим суб'єктом. Тобто пароль може бути використаний будь-яким суб'єктом. Слід зазначити лише той факт, що навіть проста передача графічного паролю іншому суб'єкту, а тим більше його викрадення більш складні процеси порівняно з випадком використання символьного паролю.

Реалізація функцій графічної парольної аутентифікації потребує створення спеціального програмного забезпечення. Але в подальшому воно може бути реалізоване у вигляді окремого модуля розробниками операційних систем, що також не буде вимагати додаткових витрат при застосуванні.

Біометрія

Біометрія – метод автоматизованого розпізнавання людини по її унікальним фізіологічним або поведінковим характеристикам.

Останнім часом біометрична аутентифікація стала стрімко розвиватись. Ряд потужних організацій на ринку інформаційних технологій (Microsoft, IBM, Novel, Compaq тощо) створили консорціум BioAPI [6], який має на меті зробити розпізнавання мови, обличчя і відбитків пальців базовими технологіями персональних комп'ютерів.

Взагалі існує більше 600 різних варіантів біометричних методів. Розглянемо найбільш розповсюджені з них:

Аутентифікація за відбитками пальців

Одна з відносно дешевих і розповсюджених систем аутентифікації, яка використовується в багатьох країнах світу, але має досить суттєвий недолік: у 80 % випадків дактилоскопічний сканер можна «обманути» за допомогою спуфінга [7]. Поширено два основних типи таких систем: оптичне сканування та ультразвукове сканування. Оптичне сканування здійснюється мікрокамерою (яка може вбудовуватися в клавіатуру). Потім отримане зображення перетворюється в карту мікрокрапок, які визначаються розривами й перетинаннями ліній. Ця карта шифрується й записується в базу даних. При цьому користувачі можуть не турбуватися про недоторканість свого приватного життя, оскільки сам відбиток пальця не зберігається й не може бути відтворений по мікрокрапках. Варто відмітити, що недорогі сканери досить легко піддаються обману. Перевагою ультразвукового сканування є можливість роботи із брудними пальцями й пальцями в рукавичках.

Аутентифікація по обличчю

Алгоритми розпізнавання по обличчю дають близько 10 % збоїв навіть при оптимальному освітленні та намаганні людини, що перевіряється, зберігати спокійний вираз [7].

Аутентифікація по райдужній оболонці ока

Унікальний для кожної людини малюнок райдужної оболонки ока сканується простою камерою зі спеціальним програмним забезпеченням.

Перелічені методи біометричної аутентифікації знайшли найбільш широке використання. Існують й інші методи: по розташуванню вен на долоні, за формою тіла людини, по термограмі особи, за рукописним або клавіатурним почерком, по голосу, за запахом, метод на основі аналізу ДНК тощо.

Велика перевага біометричних методів аутентифікації полягає в досить великій унікальності біометричних параметрів, які використовуються для аутентифікації (наприклад, ймовірність повторення райдужної оболонки складає 10^{-78}). Тому теоретично злам біометричної системи аутентифікації шляхом перебору можливих варіантів значення біометричного параметра надто складний, але з урахуванням недосконалості апаратно-програмних засобів біометричної аутентифікації можливий.

Сама процедура біометричної аутентифікації відносно проста (наприклад, прикласти палець чи руку, підставити під камеру, або пристрій для сканування обличчя або око) і не потребує будь-якого фізичного або психологічного напруження; немає потреби щось запам'ятовувати, періодично змінювати, або приховувати, чи постійно щось з собою носити.

З урахуванням того, що в біометричних системах інформація, яка використовується для аутентифікації, незмінна, виникає можливість підміни біометричних параметрів (наприклад, виготовлення та використання силіконового пальця для дактилоскопічної системи). Але ця процедура теж має певну вартість, яка може співвідноситись з вартістю самої системи аутентифікації і тому, має сенс лише у випадку, коли вартість інформації, яка захищається, суттєво вища вартості спуфінга. Зі

спуфінгом можливо боротися із застосуванням спеціальних технологій, наприклад, технології «живого пальця» [8].

На відміну від будь-яких інших систем, системи біометричної аутентифікації дозволяють ідентифікувати саме суб'єкт аутентифікації, а не його ідентифікатор, тому виключається можливість несанкціонованого застосування інформації, яка використовується для аутентифікації, іншим суб'єктом (крім випадків спуфінга). До того ж спрощується процедура контролю за потенційно небезпечними суб'єктами – у всіх інших випадках ідентифікатор та аутентифікатор можна змінити (викинути смарт-карту, змінити логін і пароль тощо).

Надійність збереження біометричних аутентифікаторів (тобто біометричних параметрів суб'єкта) порівняно з паролями та токенами досить велика, але системи біометричної аутентифікації незахищені від випадків суттєвої зміни біометричних параметрів – пошкодження пальців, рук і інших частин тіла, які використовуються при аутентифікації.

Важливий недолік біометричних систем аутентифікації – неможливість одночасного зменшення рівня помилок першого та другого роду. Якість вирішення цієї проблеми пропорційна вартості систем.

Загальний недолік всіх біометричних методів – відносно висока вартість, яка пов'язана з необхідністю розробки та встановлення на кожне робоче місце додаткових пристроїв для введення біометричної інформації.

Переносні пристрої для аутентифікації (токени та смарт-карти)

Переносні пристрої для аутентифікації – пристрої, які використовуються для збереження аутентифікатора (інформації, яка використовується для аутентифікації) на спеціальному матеріальному носії. Залежно від способу введення в інформаційно-комунікаційну систему аутентифікатора можливо виділити наступні групи таких пристроїв:

пристрої, які не мають власного інтерфейсу для зв'язку з інформаційно-комунікаційною системою – введення аутентифікатора здійснюється користувачем (токен виступає в якості електронної записної книжки, як правило, з захисним pin-кодом);

пристрої, які мають контактний інтерфейс для зв'язку з інформаційно-комунікаційною системою;

пристрої, які мають безконтактний (радіо, інфрачервоний, ультразвуковий тощо) інтерфейс для зв'язку з інформаційно-комунікаційною системою;

смарт-карти – особливий вид токенів, більш складний за своєю будовою, алгоритмами обробки і обміном інформацією. Смарт-карти містять у собі CPU, мініатюрну операційну систему, годинники, програми на ROM, буферне RAM для криптографічних обчислень, енергонезалежну пам'ять або EEPROM (Electrically Erasable Programmable Read-Only Memory) для зберігання ключів. Останнім часом подібні пристрої з'явились з USB-інтерфейсом.

Токени, як правило, захищаються pin-кодом. Залежно від узгодженості роботи токена з інформаційно-комунікаційною системою (терміналом системи аутентифікації) розрізняють синхронні та асинхронні токени.

Токени максимально спрощують процедуру введення та зміни аутентифікатора. Перевагою систем аутентифікації на основі токенів є відсутність необхідності запам'ятовування аутентифікатора (окрім, можливо, нескладного pin-коду). Це дозволяє використовувати достатньо довгі ключі, а, за необхідності, надає можливість реалізувати процедуру зміни ключа при кожному вході в систему, мережу тощо. Також виключається можливість підглядання інформації, яка використовується для аутентифікації.

При зазначених перевагах дана система аутентифікації має певні недоліки:

токен можна загубити або його можуть вкрасти (від негативних наслідків в цьому випадку захищає pin-код та алгоритми блокування або стирання інформації після фіксованого числа невірних спроб введення pin-коду);

окремі токени не захищенні від копіювання аутентифікатора безпосередньо з носія інформації з використанням спеціальних засобів, або ж шляхом механічного зламу токена;

окремі токени не мають засобів криптозахисту аутентифікатора, тому вразливі до перехоплення аутентифікатора за допомогою програмних закладок, або обладнання для «прослуховування» каналів зв'язку;

з використанням спеціальної апаратури можливий підбір (перебір) можливих значень аутентифікатора безпосередньо на терміналі системи аутентифікації;

використання токенів в більшості випадків вимагає наявності додаткового обладнання на терміналах аутентифікації інформаційної-комунікаційної системи;

як і в системах парольної аутентифікації токен пов'язаний лише з ідентифікатором суб'єкта, а не з самим суб'єктом, тобто токен може бути використаний будь-яким суб'єктом.

Виникнення помилок першого та другого роду при використанні токенів можливе лише у випадках порушення правильної роботи системи аутентифікації.

Надійність роботи токенів залежить від особливостей їх реалізації: наявність спеціальних вологозахисних, пилозахисних, ударостійких оболонок значно подовжує термін роботи токенів. Контактні токени, особливо смарт-карти та токени з USB-інтерфейсом, менш довговічні.

Вартість систем аутентифікації на основі токенів суттєво відрізняється одна від одної і залежить від надійності експлуатаційних характеристик, надійності збереження аутентифікатора, складності та обсягу додаткового обладнання.

Висновки

1. Перспективним напрямком розвитку систем аутентифікації є розвиток біометричних систем. Основні зусилля в даному напрямку спрямованні на розвиток та вдосконалення апаратно-програмних засобів, які дозволили б досягти одночасного і значного зменшення рівня помилок першого та другого роду, а також були захищені від спуфінг-загроз. Масовий випуск таких систем дозволить значно зменшити їх вартість.

2. Більшість систем аутентифікації майбутнього будуть побудовані за комбінованим типом – з одночасним використанням двох і більше методів аутентифікації (контактні токени з вбудованими чипами безконтактної аутентифікації та захищені pin-кодом, токени з вбудованими засобами біометричної аутентифікації тощо).

3. Розвиток токенів можливий за наступними напрямками: мініатюризація, розвиток та вдосконалення безконтактних інтерфейсів (захищеність інформаційного каналу, мінімізація енерговитрат), збільшення строку служби, вживлення в організм людини.

4. В найближчому майбутньому частину систем аутентифікації на основі символьного паролю буде замінено на системи на основі графічного паролю, як більш захищені. Проте певна незручність введення графічного паролю обмежить його застосування в найпростіших системах.

Список літератури

1. Сарбуков А. Аутентификация в компьютерных системах / А. Сарбуков А. Грушо .// Системы безопасности. – 2003. - №5 (53). – С. 25-29.

2. Чепиков О. Особенности применения двухфакторной аутентификации / О. Чепиков // Информационная безопасность. – 2005. – №3. – С.35-41.

3. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства. – М.: ДМК Пресс, 2008. – 544 с.

4. Шрамко В.Н. Защита компьютеров: электронные системы идентификации и аутентификации В.Н. Шрамко // PCWeek/RE. – 2004. - №12.

5. ImagiPass 1.1. – Режим доступу: www.atlantiswordprocessor.com /en/imagipass.

6. BioAPI – Режим доступу: www.bioapi.org.

7. Новые системы паролей. – Режим доступу: http://windows2008.at.ua.

8. Системы идентификации аутентификации. – Режим доступу: http://acoder.org

9. Графический пароль не даёт смотрящему украсть себя. – Режим доступу: http://www.membrana.ru.

10. Задонский А. Ю. Вопросы аутентификации в современных информационных системах. – Режим доступу: http://www.compserv.ru.

Надійшла до редакції 27.08.2009 р.

Рецензент: доктор технічних наук, професор М.В. Коваленко, Житомирський державний технологічний університет, Житомир.

МЕТОДЫ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМ

С.И. Болобан, А.М. Перегуда, В.В. Уминский

В статье рассмотрены особенности наиболее распространенных методов аутентификации пользователей информационно-коммуникационных систем. Определен перечень критериев для оценивания качества систем аутентификации, реализованных на основе этих методов. Детально рассмотрены следующие методы аутентификации: статические и одноразовые пароли (символьные и графические), биометрические методы, методы основанные на использовании переносных устройств для аутентификации (токенов и смарт-карт). Проведено сравнительный анализ методов аутентификации, определены преимущества и недостатки этих методов, перспективы их дальнейшего применения.

Ключевые слова: *аутентификация, символьный пароль, графический пароль, биометрия, токен.*

AUTHENTIFICATION METHODS OF INFORMATIONAL-COMMUNICATION SYSTEMS USERS

S.I. Boloban, A.M. Pereguda, V.V. Uminsky

Features of the most widespread methods of authentication of informational-communication systems users are considered in the article. The list of criteria for estimation of quality of systems of the authentication realised on the basis of these methods is defined. Following methods of authentication are in details considered: static and disposable passwords (character and graphics), biometric methods, methods grounded on usage of portable devices for authentication (tokens and smart cards). Comparative analysis of methods of authentication, advantages and disadvantages of these methods, perspectives of their further application are defined.

Keywords: *authentication, the character password, the graphics password, biometrics, a token.*