УДК 681.3

ІВАНОВ В.Г., МАЗНИЧЕНКО Н.І.

АНАЛІЗ СУЧАСНИХ ПІДХОДІВ В ЗАДАЧАХ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ІНФОРМАЦІЙНИХ СИСТЕМ

Сьогодні важко уявити роботу практично будь-якої організації без інформаційних систем і комп'ютерних мереж, отже, питання інформаційної безпеки набувають все більшого значення [1]. Сучасні технології не лише надають нові можливості організації професійної діяльності, бізнесу, але і створюють потребу в надійних засобах безпеки для захисту конфіденційних даних. Серед основних тенденцій в області інформаційної безпеки, перш за все, можна виділити наступну: побудова єдиної комплексної системи безпеки, об'єднуючої розрізнені засоби захисту. Створення єдиної, централізованої системи безпеки є необхідною умовою існування сучасної інформаційної інфраструктури [2]. Одним з основних і невід'ємних елементів комплексної системи безпеки є підсистема управління доступом до інформаційних ресурсів, яка надає засоби ідентифікації користувачів. Управління доступом – ефективний метод захисту інформації, який регулює використання ресурсів інформаційної системи, для якої розробляється концепція інформаційної безпеки. Методи і системи захисту інформації, що спираються на управління доступом, включають наступні функції захисту інформації в інформаційних системах [3]:

– Ідентифікація користувачів, ресурсів і персоналу системи інформаційної безпеки;

– Впізнання і встановлення достовірності користувача за обліковими даними, що вводяться (на даному принципі працює більшість моделей інформаційної безпеки);

– Допуск до певних умов роботи згідно регламенту, наказаному кожному окремому користувачу, що визначається засобами захисту інформації і є основою інформаційної безпеки більшості типових моделей інформаційних систем;

– Протоколювання звертань користувачів до ресурсів, інформаційна безпека яких захищає ресурси від несанкціонованого доступу і відстежує некоректну поведінку користувачів системи.

Корінням цих питань є поняття ідентифікації і аутентифікації. Система ідентифікації і аутентифікації є одним з ключових елементів інфраструктури захисту від несанкціонованого доступу будь-якої інформаційної системи [4].

Ідентифікація - це пред'явлення користувачем якогось унікального, властивого тільки йому ідентифікатора (ознаки). Аутентифікації дозволяє переконатись, що суб'єкт дійсно той, за кого він себе видає. Як синонім слова "аутентифікація" іноді використовують словосполучення "перевірка достовірності".

Сьогодні існує декілька способів ідентифікації користувачів. У кожного з них є свої переваги і недоліки, тому як розроблювачам програмного забезпечення, так і користувачам приходиться самостійно обирати, який спосіб ідентифікації реалізовувати у власних інформаційних комп'ютерних системах.

Існують наступні найпоширеніші підходи до ідентифікації користувачів:

1). Парольна ідентифікація. Суть її зводиться до наступного. Кожен зареєстрований користувач якої-небудь системи одержує набір персональних реквізитів (звичайно використаються пари логин-пароль). Далі при кожній спробі входу він повинен вказати свою інформацію. Ну а оскільки вона унікальна для кожного користувача, то на підставі її система й робить висновок про особистість та ідентифікує її.

Головна перевага парольної ідентифікації - це простота реалізації й використання [5]. Крім того, введення парольної ідентифікації не вимагає зовсім ніяких витрат: даний процес реалізований у більшості програмних продуктів. Таким чином, система захисту інформації виявляється простою і доступною.

Тепер перейдемо до недоліків. На жаль, їх багато. І самий, мабуть, головний - величезна залежність надійності ідентифікації від самих користувачів, точніше, від обраних ними паролів. Справа в тому, що більшість людей використовують ненадійні ключові слова, які легко

підбираються. До них відносяться занадто короткі паролі, загальновідомі сполучення символів і т.д. Тому деякі фахівці в області інформаційної безпеки радять використати довгі паролі, що складаються з випадкового сполучення букв, цифр і різних символів.

Наступні заходи дозволять значно підвищити надійність парольного захисту:

– накладення технічних обмежень (пароль повинен бути не дуже коротким, він повинен містити букви, цифри, знаки пунктуації і т.п.);

– управління терміном дії паролів, їх періодична зміна;

– обмеження доступу до файлу паролів;

– обмеження числа невдалих спроб входу в систему;

– використання програмних генераторів паролів (така програма, ґрунтуючись на нескладних правилах, може генерувати тільки благозвучні паролі, що запам'ятовуються).

При правильному використанні паролі можуть забезпечити прийнятний для багатьох організацій рівень безпеки. Проте, по сукупності характеристик їх слід визнати найслабкішим засобом перевірки достовірності.

2). Апаратна (електронна) ідентифікація.

Цей принцип ідентифікації ґрунтується на визначенні особистості користувача по якомусь предметі, ключу, що перебуває в його ексклюзивному користуванні. Мова йде про спеціальні електронні ключі. Кожен апаратний (електронний) ідентифікатор є фізичним пристроєм, зазвичай невеликих розмірів для зручності його носіння з собою. На даний момент найбільше поширення одержали два типи пристроїв: всілякі карти (проксіміті-карти, смарт-карти, магнітні карти і т.д.) та так званні токени (token), які підключаються безпосередньо до одного з портів комп'ютера (USB, LPT).

Головним достоїнством застосування апаратної ідентифікації є досить висока надійність. І дійсно, у пам'яті токенів можуть зберігатися ключі, підібрати які досить складно. Крім того, у них реалізовано чимало різних захисних механізмів. Ну а вбудований мікропроцесор дозволяє електронному ключу не тільки брати участь у процесі ідентифікації користувача, але й виконувати деякі інші корисні функції.

Ну а тепер давайте поговоримо про недоліки апаратної ідентифікації. Мабуть, найбільш серйозною небезпекою у випадку використання апаратної ідентифікації є можливість крадіжки зловмисниками токенів або карт у зареєстрованих користувачів. Також вони можуть бути втрачені, передані іншій особі, дубльовані. Другий мінус розглянутої технології - ціна. Взагалі ж останнім часом вартість як самих електронних ключів, так і програмного забезпечення, що може працювати з ними, помітно знизилася. Проте, для введення в експлуатацію системи такої ідентифікації однаково будуть потрібні деякі вкладення. Все-таки кожного зареєстрованого користувача потрібно забезпечити персональними токенами. Крім того, згодом деякі типи ключів можуть зношуватися, можуть бути загублені і т.д. Тобто апаратна ідентифікація вимагає деяких експлуатаційних витрат.

Розглянуті методи аутентифікації (парольна та електронна) страждають одним недоліком - вони, насправді, аутентифікують не конкретного суб'єкта, а фіксують той факт, що аутентифікатор суб'єкта відповідає його ідентифікатору. Тобто, всі перераховані методи не захищені від компрометації аутентифікатора.

3). Біометрична ідентифікація. Біометрія – це ідентифікація людини по унікальним, властивим тільки ньому біологічним ознакам [6]. Тобто, можна сказати, що біометричні технології споконвічно розроблялися для точного встановлення особистості людини, тому рішення використати їх в області інформаційної безпеки виглядає цілком логічним. Причому даний напрямок розвивається дуже активно. Сьогодні експлуатується вже більше десятка різних біометричних ознак.

Серед біометричних механізмів ідентифікації можна виділити такі:

– по статичних ознаках — те, що практично не міняється з часом, починаючи з народження людини (фізіологічні характеристики);

– по динамічних ознаках — поведінкові характеристики, тобто ті, які побудовані на особливостях, характерних для підсвідомих рухів в процесі відтворення якої-небудь дії. Динамічні ознаки можуть змінюватися з часом, але не різко, а поступово.

Серед статичних методів ідентифікації користувача на сьогодні використовуються

наступні: ідентифікація по відбитку пальця; по розташуванню вен на долоні; по сітківці ока; по веселковій оболонці ока; за формою грона руки; за формою обличчя.

Серед динамічних методів можна назвати наступні: ідентифікація по голосу; по почерку; по клавіатурному почерку.

При всьому теоретичному різноманітті можливих біометричних методів тих, що застосовуються на практиці серед них небагато. Основних методів три - розпізнавання по відбитку пальця, по зображенню особи (двомірному або тривимірному) і по веселковій оболонці ока.

Головною перевагою біометричних технологій є найвища надійність. І дійсно, усі знають, що двох людей з однаковими відбитками пальців у природі просто не існує. Але біометричні сканери також можна обманути за допомогою муляжів. Сьогодні вже відомо кілька способів обману дактилоскопічних сканерів. Наприклад, потрібні відбитки пальців можуть бути перенесені на плівку або може бути використана фотографія пальця зареєстрованого користувача. Втім, треба зазначити, що сучасні пристрої вже значно стійкіші до подібної фальсифікації.

Основним недоліком біометричної ідентифікації є вартість устаткування. Адже для кожного комп'ютера, що входять до системи, необхідно придбати власний сканер. Звичайно, останнім часом ціни на біометричні пристрої постійно знижуються. Крім того, не дуже давно з'явилися миші й клавіатури з вбудованими дактилоскопічними сканерами. Причому їхня ціна ненабагато відрізняється від вартості "звичайної" периферії. Правда, варто відзначити, що подібні дешеві сканери недовговічні. Крім того, у них досить високий відсоток помилок другого роду (відмова в доступі зареєстрованому користувачеві). Тому користувачеві доводиться вибирати, яке пристрій придбати - дорожчій й кращій або дешевшій й гіршій.

Хотілося б відмітити, що важко не погодитись, що біометричні технології надійніші та зручніші за засоби захисту, які широко використовувались до останнього часу, та забезпечують немалі переваги, в тому числі для кінцевих користувачів [7].

Поки що було розглянуто три підходи до задачі ідентифікації користувачів різноманітних інформаційних систем. Але останнім часом набуває поширення комплексна або багатофакторна ідентифікація.

4). Багатофакторна ідентифікація. До даного моменту мова йшла про однофакторну ідентифікацію. Тобто в розглянутих системах для визначення особистості користувача використовувався тільки один фактор. Однак подібні процеси сьогодні не можна назвати надійними. Наприклад, зловмисник може вкрасти токен у зареєстрованого користувача (або отримати доступ до паролю) й легко скористатися ним для несанкціонованого доступу до інформації. Саме тому поступово все більшого поширення одержує багатофакторна ідентифікація, коли для визначення особистості застосовується відразу кілька параметрів. Причому комбінуватися ці фактори можуть у довільному порядку. Втім, сьогодні найчастіше використається тільки одна пара: парольний захист і токен. У цьому випадку користувач може не боятися підбора його пароля зловмисником (без електронного ключа вона працювати не буде), а також крадіжки токена (він не буде працювати без пароля). Втім, у деяких системах застосовуються максимально надійні процедури ідентифікації. У них одночасно використаються паролі, токени й біометричні характеристики людини.

Впровадження комбінованих систем суттєво збільшує кількість ідентифікаційних ознак і тим самим підвищує безпеку [8].

На основі аналізу загроз інформаційній безпеці, та існуючих засобів ідентифікації та аутентифікації користувачів інформаційних систем, можна впевнено сказати, що парольний захист на сьогодні є одним з найпоширеніших способів захисту інформації від несанкціонованого доступу як в окремих комп'ютерах і системах, так і в мережах світового масштабу. Проте без використовування інших механізмів захисту, парольний захист сам по собі не може забезпечити серйозного захисту. Досить розповсюдженими в якості ідентифікаторів використовуються також різноманітні електронні ключі (токени, карти і т.і.). Але слід зауважити, що останнім часом все більшого поширення набувають системи ідентифікації, які використовують біометричні характеристики людини при вирішенні задачі доступу до інформаційних систем.

Таким чином, розглянувши різні технології апаратно-програмної, парольної,

біометричної ідентифікації та аутентифікації можна зробити висновок, що надалі у міру зростання обчислювальних потужностей все більш запитаним буде вживання систем багатофакторної ідентифікації та аутентифікації, що дозволить уникнути людських помилок, зв'язаних із застосуванням слабких паролів і посилити вимоги до парольної аутентифікації.

Щодо вибору системи ідентифікації безпосередньо в кожній окремій ситуації, користувач повинен: об'єктивно оцінити співвідношення цінності інформації, що захищається, і вартості програмно-апаратного забезпечення ідентифікації/аутентифікації, яке обираєте (включаючи супровід); оцінити зручність у використанні (контактні, безконтактні) та сприйняття обраного підходу користувачами; визначити потрібний рівень захищеності («що» і від кого потрібно захищати). Але безперечною порадою є обов'язкове використання комплексної системи ідентифікації, яка поєднує декілька підходів до вирішення задач доступу до інформаційних ресурсів комп'ютерних систем.

ЛИТЕРАТУРА

1. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях // Под ред. В.Ф. Шаньгина. 2-е изд. – М.: Радио и связь, 2001. – 376 с.
2. Домарев В.В. Безопасность информационных технологий. Системный подход. – К.: ООО «ТИД «ДС», 2004. – 992 с.
3. Корченко А.Г. Несанкционированный доступ в компьютерные системы и методы защиты. – К.: КМУГА, 1998.
4. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. – СПб: Наука и техника, 2004 г. – 384с.
5. Анин Б. Защита компьютерной информации. – СПб: BHV, 2002. — 384 с.
6. Кухарев Г. А. Биометрические системы: методы и средства идентификации личности человека. – СПб.: Политехника, 2001. – 240 с.
7. Голубев Г.А., Габриелян Б.А., Современное состояние и перспективы развития биометрических технологий // Нейрокомпьютеры: разработка, применение. 2004, № 10. с. 39-46.
8. Галатенко В.А. Информационная безопасность: практический подход. -М.: Наука, 1998.- 301 с.

ІВАНОВ Володимир Георгійович – д.т.н., професор, завідувач кафедрою інформатики і обчислювальної техніки НУ «Юридична академія України ім. Ярослава Мудрого»

Наукові інтереси:

– стиснення та ідентифікація даних різноманітної фізичної природи.

МАЗНИЧЕНКО Наталя Іванівна – ст. викладач кафедри інформатики і обчислювальної техніки НУ «Юридична академія України ім. Ярослава Мудрого»

Наукові інтереси:

– інформаційна безпека, ідентифікація користувачів комп'ютерних систем, біометричні технології.