НУ «Юридична академія України ім. Ярослава мудрого»
В.Г. Іванов, Н.І. Мазниченко

ІДЕНТИФІКАЦІЯ КОРИСТУВАЧІВ ІНФОРМАЦІЙНИХ СИСТЕМ: АНАЛІЗ І ПРОГНОЗУВАННЯ ПІДХОДІВ

Сьогодні важко уявити роботу практично будь-якої організації без комп'ютерних мереж і інформаційних систем, отже, питання інформаційної безпеки набувають все більшого значення. Створення єдиної, централізованої системи безпеки є необхідною умовою існування сучасної інформаційної інфраструктури. Одним з основних і невід'ємних елементів комплексної системи безпеки є підсистема управління доступом до інформаційних ресурсів, яка надає засоби ідентифікації користувачів. Ідентифікація дозволяє суб'єкту (користувачу, процесу, діючому від імені певного користувача, або іншому апаратно-програмному компоненту) назвати себе за рахунок пред'явлення користувачем якогось унікального, властивого тільки йому ідентифікатора (ознаки).

Існують наступні найпоширеніші підходи до ідентифікації:

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. Крім того, введення парольної ідентифікації не вимагає зовсім ніяких витрат: даний процес реалізований у більшості програмних продуктів. Недоліки цього підходу добре відомі, пароль може бути скомпрометований безліччю способів. Парольний захист на сьогодні є одним з найпоширеніших способів захисту інформації від несанкціонованого доступу як в окремих комп'ютерах, так і в мережах світового масштабу.

2). Апаратна (електронна) ідентифікація. Цей принцип ідентифікації ґрунтується на визначенні особистості користувача по якомусь предметі, електронному ключу, що перебуває в його ексклюзивному користуванні. 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 викори-

стання 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, яку на сьогоднішній день неможливо вважати загальнодоступною.

3). Біометрична ідентифікація. Біометрія - це ідентифікація людини по унікальним, властивим тільки їй біологічним ознакам. Тобто, можна сказати, що біометричні технології споконвічно розроблялися для точного встановлення особистості людини. А 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. Причому для найпоширеніших з них (відбитки пальців і райдужна оболонка ока) існує безліч різних за принципом дії сканерів. Головним достоїнством біометричних технологій є найвища надійність. Основним недоліком біометричної ідентифікації є вартість устаткування, адже для кожного комп'ютера, що входять до цієї системи, необхідно придбати власний сканер.

4). Багатофакторна ідентифікація. Розглянуті раніше однофакторні системи ідентифікації сьогодні не можна назвати надійними. Саме тому поступово все більшого поширення одержує багатофакторна ідентифікація, коли для визначення особистості користувача застосовується відразу кілька параметрів. Втім, сьогодні в переважній більшості випадків 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 одночасно паролі, токени й біометричні характеристики людини і саме такі системи можна назвати максимально надійними.

На основі аналізу загроз інформаційній безпеці, та існуючих засобів ідентифікації користувачів інформаційних систем, можна впевнено зробити висновок, що надалі у міру зростання обчислювальних потужностей все більш запитаним буде саме вживання систем багатофакторної ідентифікації, що дозволить значно підвищити рівень надійності систем ідентифікації. Щодо вибору системи ідентифікації безпосередньо в кожній окремій ситуації, користувач також повинен: об’єктивно оцінити співвідношення цінності інформації, що захищається, і вартості програмно-апаратного забезпечення ідентифікації, 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.