Н. І. Мазниченко
старший викладач кафедри криміналістики,
Національного юридичного університету
імені Ярослава Мудрого,
м. Харків

ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ КОМП'ЮТЕРНИХ СИСТЕМ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ НА ОСНОВІ СИСТЕМ ІДЕНТИФІКАЦІЇ

З появою і розвитком нових інформаційних технологій стала актуальна проблема інформаційної безпеки, пов'язана із забезпеченням безпечного збереження і конфіденційності інформації, що обробляється та зберігається в комп'ютерних

системах. Актуальність задачі інформаційної безпеки набуває ще більшої значущості у зв'язку зі зростанням злочинності в сфері використання комп'ютерної інформації.

Одним з важливих напрямків діяльності у протидії злочинам є застосування профілактичних заходів щодо попередження, запобігання здійсненню злочину. Враховуючи різноманіття потенційних загроз для комп'ютерної інформації, безпечне збереження і конфіденційність інформації може бути досягнута тільки шляхом створення комплексної системи захисту інформації. Одним з основних і невід'ємних елементів комплексної системи безпеки є підсистема управління доступом до інформаційних ресурсів комп'ютерних систем, що потребують захисту. Система ідентифікації є одним з ключових елементів інфраструктури захисту від несанкціонованого доступу будь-якої інформаційної комп'ютерної системи. Доступ користувачів до різних класів інформації визначається ідентифікацією, тобто процесом розпізнавання параметрів, що однозначно визначають особу користувача.

Можна виділити наступні найпоширеніші підходи до ідентифікації користувачів комп'ютерних систем:

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

Головна перевага парольної ідентифікації – це простота реалізації і використання. Головний недолік – 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. Але при правильному використанні паролі можуть забезпечити прийнятний для багатьох організацій і окремих користувачів рівень безпеки. Проте, по сукупності характеристик її слід визнати найслабкішим засобом перевірки достовірності особи користувача.

2). Електронна (або апаратна) ідентифікація. Цей принцип ідентифікації ґрунтується на визначенні особи користувача по якомусь предметі, ключу, що перебуває в його ексклюзивному користуванні. Кожен апаратний (електронний) ідентифікатор є фізичним пристроєм, зазвичай невеликих розмірів. На даний момент найбільшого поширення одержали два типи пристроїв: різноманітні карти (проксіміті-карти, смарт-карти, магнітні карти і т.д.) та так званні токени (token), які підключаються безпосередньо до одного з портів комп'ютера [1].

Головною перевагою застосування апаратної ідентифікації є досить висока надійність. І дійсно, у пам'яті токенів можуть зберігатися ключі, підібрати які досить складно. Крім того, у деяких пристроях реалізовано чимало різних захисних механізмів.

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, тому що апаратна ідентифікація вимагає певних експлуатаційних витрат.

3). Біометрична ідентифікація. Біометрія – це ідентифікація людини по уні-

кальним, властивим тільки йому, біологічним ознакам [2]. Тобто, можна сказати, що біометричні технології споконвічно розроблялися для точного встановлення особи 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.

Але при всьому теоретичному різноманітті біометричних методів тих, що застосовуються на практиці, небагато. В основному використовують наступні: розпізнавання по відбитку пальця, по зображенню особи (двомірному або тривимірному) і по сітківці або 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.

Основним недоліком біометричної ідентифікації є вартість устаткування. Адже для кожного комп'ютера, що входить до системи, необхідно придбати власний сканер. Але слід відзначити, що останнім часом ціни на біометричні пристрої постійно знижуються.

4). Багатофакторна (або комплексна) ідентифікація. В цьому випадку для визначення особи користувача застосовується відразу кілька параметрів. Причому комбінуватися ці фактори можуть у довільному порядку [3]. Втім, сьогодні найчастіше використається наступна комбінація: парольний захист і токен. Досягти підвищення надійності захисних можливостей автоматизованих систем ідентифікації користувачів можна за рахунок об'єднання біометричних характеристик разом з класичними способами ідентифікації (наприклад, з парольним захистом, PIN-кодом, різнома-нітними картами). Актуальними бачаться розробки та дослідження комплексних систем, що використовують для прийняття рішення доступу до інформаційних ресурсів комп'ютерних систем декілька біометричних характеристик користувача (наприклад, використання одночасно відбитків декількох пальців або об'єднання двох- та трьохмірних зображень обличчя). Втім, у деяких системах застосовуються максимально надійні процедури ідентифікації, де одночасно використовуються паролі, токени й біометричні характеристики людини. Впровадження комбінованих систем збільшує кількість ідентифікаційних ознак і тим самим підвищує захищеність інформаційних комп'ютерних систем від несанкціонованого доступу.

Таким чином, розглянувши сучасні технології ідентифікації користувачів можна зробити висновок, що надалі у міру зростання обчислювальних потужностей все більш запитаним буде вживання систем багатофакторної ідентифікації, яка поєднує декілька підходів до вирішення задач доступу до інформаційних ресурсів комп'ютерних систем, що дозволяє значно підвищити надійність та захисні можливості подібних систем.

Відносно вибору системи ідентифікації безпосередньо в кожній конкретній ситуації користувачу доцільно об'єктивно оцінити співвідношення цінності інформації, що захищається та вартості програмно-апаратного забезпечення процесу ідентифікації (враховуючи супровід); оцінити зручність у використанні (контактні або безконтактні) і сприйняття обраного підходу користувачами; визначити потрібний рівень захищеності інформаційних ресурсів. Але безумовною порадою є використання комплексної системи ідентифікації.

Список літератури

1. Дшхунян В. Л., Шаньгин В. Ф. Электронная идентификация. Бесконтактные электронные идентификаторы и смарт-карты. – М.: АСТ, 2004. –696 с.
2. Кухарев Г. А. Биометрические системы: методы и средства идентификации личности человека. – СПб.: Политехника, 2001. – 240 с.
3. Шрамко В. Н. Комбинированные системы идентификации и аутентификации // PCWeek/RE. – 2004. – №45. – С. 30–32.