Если параметры ε_i при простейшем способе интерпретации $\varphi(\varepsilon_1,...,\varepsilon_k)$ выходят за допустимые пределы, то необходимо по отношению к этому параметру проводить локальный анализ соответствующих $L_i(x_{i1},...,x_{ik})$ и $J[L_i]$ с целью введения соответствующих модификаций.

1. *Петриашвили Г. Г.* Моделирование системы функционирования книжно-журнальных изданий с переменным информационным содержанием / *Г. Г. Петриашвили* // Моделювання та інформаційні технології. — К., 2007. — Вип. 41. — С. 188–194.
2. *Петриашвили Г. Г.* Параметры характеризующие пользовательские свойства книжных изданий / *Г. Г. Петриашвили, Б. В. Дурняк* // Зб. наук. пр. ІПМЕ НАН України. — К., 2006. — Вип. 32. — С. 225–228.
3. *Петриашвили Г. Г.* Влияние геометрии поверхности срезки корешков блоков на параметры прочности книжно-журнальных изданий выполненных способом клеевого бесшвейного скрепления / *Г. Г. Петриашвили* // Зб. наук. пр. ІПМЕ НАН України. — К., 2006. — Вип. 36. — С. 191–194.

Поступила 1.09.2010р.

УДК 004.921

Л.Є.Шведова

МЕТОДИ ЗАХИСТУ ДАНИХ

Захист даних в основному полягає в охороні їх від неуповноваженого, або неправильного використання, випадкового або упередженого уявлення даних, модифікації або знищення. Виділяються такі базові ознаки забезпечення безпеки даних [1]:

— доступність;
— цілісність;
— інтегральність;
— довір'я до даних, або конфіденційність.

Довіра або конфіденційність означає, що отримані дані не були прочитані третіми особами, які не мають повноважень до ознайомлення з цими даними. Особливість цієї ознаки полягає у тому, що із самих даних, на основі аналізу інформації, яка відповідними даними описується, неможливо визначити, чи була змінена ця ознака. Особливістю введених ознак та в цілому засобів захисту даних є те, що рівень забезпечення міри виконання вимог кожної з базових ознак може бути різним. Це означає, що мусять бути введені шкали для міри конфіденційності, міри доступності, міри

інтегральності тощо, які дозволили б визначати міри, або поточні значення параметрів захисту даних і відповідно величини базових ознак.

Інтегральність даних означає, що отримані дані не є змінені в тій чи іншій мірі, у спосіб недопустимий, що визначається політикою забезпечення безпеки даних. На відміну від конфіденційності, теоретично можуть існувати методи виявлення тих чи інших змін в даних на основі аналізу інформації, що цими даними описується. Такі механізми визначення величини порушення інтегральності ґрунтуються на основі таких підходів та методів аналізу:

— аналізу інтерпретаційних описів даних, стосовно яких необхідно виявити порушення інтегральності чи їх модифікації;
— моделювання процесів використання відповідних даних;
— аналізу параметрів семантики відповідних даних, якщо допустимі величини їх значень є заданими і такі дані рознесені просторово з даними, які необхідно захищати.

Доступність даних є ознакою або параметром, який у певній мірі пов'язаний з ознакою конфіденційності. Відрізняється ця ознака від конфіденційності тим, що доступність, яка характеризується певною мірою або певним значенням відповідного параметру, може бути не достатньо великою відносно потенційних користувачів чи певних уповноважених користувачів. Оскільки дані завжди мають певну структуру, то доступність до них може бути узгоджена з відповідною структурою. Це означає, що елементи даних, які визначаються різними параметрами структури, можуть мати різну міру доступності. Тому, у певному наближенні, можна вважати, що доступність, як певна ознака, є величиною оберненою до конфіденційності. З цієї точки зору можна говорити про взаємозв'язок між цими двома ознаками. Спільною ознакою доступності та конфіденційності є те, що порушення міри доступності до даних не можливо виявити на основі аналізу цих даних, якщо при порушенні цієї ознаки вдалося отримати не всі дані, а тільки їх частину. Це пов'язано з тим, що дані визначаються як такі, тільки в тому випадку, коли вони мають певну структуру. Доступ до даних існує в тому випадку, коли при їх зчитуванні коректно зчитується інформація про їх структуру.

Цілісність або пов'язаність даних в основному відноситься до баз даних. Ця ознака визначає, що стан бази даних протягом певного часу не зміниться, або структура даних залишиться певний час стабільною.

Однією з базових компонент, яка призначена для захисту даних, є система захисту та контролю доступу. Елементами такої системи є суб'єкти:

— користувач,
— процеси,
— об'єкти тощо.

До об'єктів можна віднести:

— дані,
— програми,
— операції тощо.

Прикладами операцій можуть бути:

— читання,
— запис,
— формування,
— усунення тощо.

Основою для створення системи захисту доступу є політика, яка визначає цілий ряд факторів, що відображають способи реалізації захисту:

— управління правилами доступу,
— формування правил доступу тощо.

З точки зору політики безпеки можна поділити системи доступу на два класи:

— відкриті системи,
— закриті системи.

У закритих системах захисту доступу використовуються правила, які в загальному можна описати наступним способом — «що не заборонено, — то дозволено». У цьому випадку суб'єкт не отримає доступу до системи тільки в тому випадку, якщо відповідне правило доступу забороняє цей доступ. Закриті системи захисту доступу мають більш високий рівень безпеки, оскільки всі правила, що дозволяють доступ, перш ніж включаються в систему, аналізуються на предмет можливого виникнення небезпеки, яка могла би виникнути в результаті використання відповідного правила доступу.

Для спрощення процесів реалізації політики безпеки, суб'єкти, що мають одинакові повноваження, а об'єкти групуються по однакових класах безпеки. В цьому випадку необхідно розв'язувати проблеми, що пов'язані з приналежністю одного суб'єкта до багатьох груп одночасно та проблеми, пов'язані із змінами приналежності суб'єктів.

Обов'язковий контроль доступу використовує засоби, що обмежують доступ до об'єктів, які ґрунтуються на використанні рівнів безпеки і централізованого управління правилами доступу. Кожному суб'єкту і об'єкту системи надається клас рівня безпеки, який визначається на основі рівня необхідної охорони, наприклад, такими рівнями можуть бути [2]:

— відкритий рівень,
— рівень службового використання,
— таємний рівень,
— надзвичайно таємний рівень,

а також категорією, що визначається сферою використання. Класифікація суб'єктів відбиває рівень довіри до суб'єкта і сферу діяльності відповідного суб'єкту.

Класифікація об'єктів групується на їх вразливості, або мірі важливості їх відношення до інформації, розміщеної у відповідному об'єкті, що допускає наступну інтерпретацію — величиною можливих втрат до яких може призвести уявлення відповідної інформації. Суб'єкт отримує доступ до об'єкта, якщо виконуються необхідні співвідношення між класом безпеки суб'єкта та класом безпеки об'єкта.

Розпізнавальний контроль доступу використовує засоби організації доступу до об'єктів, що ґрунтуються на ідентифікації користувачів, привілеях і розподіленому управлінню правилами доступу. Кожному суб'єкту надаються привілеї, наприклад, читання, модифікація, усування тощо, відносно визначених об'єктів. В такій системі суб'єкт може приймати рішення про зміну привілеїв інших суб'єктів відносно певних об'єктів. Суб'єкт отримує доступ до об'єкту у вибраному режимі (читання, запис, усунення тощо), якщо він має відповідні привілеї відносно такого об'єкту.

Привілеї суб'єктів можуть описуватися відносно об'єктів такими способами:

— опис може бути орієнтований на етикетки або білети,
— опис може бути орієнтований на складання списків суб'єктів.

У першому випадку кожний суб'єкт має список зразків білетів, по одному для кожного об'єкту, до якого відповідний суб'єкт має доступ. У другому випадку, кожний об'єкт, який захищається, має список всіх суб'єктів, які мають повноваження на доступ до відповідного об'єкту, що охороняється.

В системах правил доступу використовуються розширення додатковими предикатами, які описують обмеження, що накладаються на привілеї суб'єктів. Такі обмеження можуть бути пов'язані з наступними особливостями чи характеристиками об'єктів:

— вартістю об'єкта,
— датою і часом доступу,
— способом отримання доступу (локальний чи віддалений),
— історією операцій, що реалізувалися до поточного моменту реалізації доступу і т.д.

В системі з додатковими обмеженнями суб'єкт отримує доступ до об'єкту у вибраному режимі, якщо він має відповідні привілеї відносно цього об'єкта та виконуються всі предикати, що пов'язані з даним доступом. Контроль предикатів виконує операційна система та система управління базою даних, до яких передбачається реалізовувати доступ.

Впровадження політики безпеки реалізують фахівці, які за неї відповідають. Така реалізація здійснюється на основі використання відповідних процедур, які для цих цілей спроектовані при допомозі різних механізмів забезпечення, що реалізують визначену безпеку за допомогою апаратних та програмних засобів. Ці механізми виконують привенційні та детекційні функції. Серед них можна виділити зовнішні та внутрішні механізми. До першої групи належать адміністративні та матеріальні засоби захисту доступу до приміщень, апаратури а також захист від аварій та катастроф. Їх ціллю являються такі вимоги:

— мінімізація можливих порушень охорони;
— мінімізація негативних наслідків можливих порушень охорони;
— гарантування можливості відновлення стану після порушень системи охорони.

До внутрішніх механізмів охорони належать такі:

— механізми ідентифікації і аутентифікації;
— механізми контролю доступу — системи повноважень;
— механізми аудиту.

До механізмів аутентифікації належать наступні методи її реалізації:

— методи, що ґрунтуються на контролі користувача,
— методи, що ґрунтуються на виконанні матеріалів ідентифікації користувача;
— біометричні методи.

Користувач, який хоче отримати доступ до системи, яка охороняється, повинен показати, що він володіє певними знаннями або об'єктом, який його ідентифікує, чи володіє певними фізичними характеристиками. Оскільки кожна з наведених вище методик має певні недоліки, то високий ступінь захисту можна досягнути використовуючи одночасно більш ніж один із методів аутентифікації [3].

Користувач, який виявився аутентифікованим в системі, не повинен залишати доступних йому засобів системи без нагляду. Кожен раз, перед завершенням відповідної праці, суб'єкт, або користувач, повинен виконати дії, які зумовили б необхідність нової аутентифікації у випадку необхідності продовження праці в системі.

До методів, що ґрунтуються на використанні знань користувача, можна віднести найбільш поширений метод, в якому аутентифікація полягає на перевірці того, чи знає він необхідний пароль. Іншою версією цього методу є перевірка того, чи користувачеві відомі певні факти. Основною перевагою системи аутентифікації, що ґрунтується на використанні паролів, є простота реалізації відповідного способу аутентифікації користувача.

Забезпечення певного рівня безпеки вимагає обов'язкового виконання умов використання паролів. До важливих факторів, що впливають на рівень безпеки системи доступу на основі паролів, слід віднести:

— розмір алфавіту за допомогою якого формуються паролі та його оригінальність;
— довжина паролів;
— період актуальності паролів;
— спосіб їх генерації;
— складність паролів;
— метод зберігання та пересилання паролів в системі.

Рівень безпеки паролів залежить від кількості знаків у алфавіті, з якого формується пароль. Від кількості знаків в алфавіті і довжини паролів залежить кількість всіх можливих комбінацій паролів і, як наслідок, складність атаки, що ґрунтується на пошуку паролів шляхом перебору. Кількість паролів довжиною k, яку можна побудувати з алфавіту, що має n знаків, рівна n^k.

Оскільки збільшення довжини паролів пов'язане із збільшенням ймовірності допущення помилки при введені пароля, що призводить до трудності

його запам'ятовування, то замість одинарних паролів у вигляді рядку знаків використовуються часом парольні фрази, які є зручними послідовностями виразів з довжиною не більшою від максимальної довжини паролів. Така фраза перетворюється за допомогою функції згортання до реального паролю, який має фіксовану довжину. Функція згортання, або h-функція, що використовується в системах захисту, є односторонньою функцією, що перетворює повідомлення m довільної довжини в r-бітову згортку $h(m)$. Наслідки розпізнавання паролів можна зменшити шляхом використання окремого пароля. Тому у випадку, коли появляється підозра про те, що пароль є викритим, його необхідно змінити. В ідеальній ситуації пароль використовується один раз.

Паролі можуть формуватися користувачами, які відповідний пароль планують використовувати. Таке формування може ґрунтуватися на використанні наступних засобів чи методів:

— ручного генератора одноразових паролів;
— автоматичних генераторів паролів;
— на основі використання псевдовипадкових, або випадкових, систем.

В цьому випадку адміністратор повинен контролювати засоби формування паролів, щоб не допустити використання простих для відгадування паролів. Паролі, що генеруються автоматично, повинні мати особливості, які допомагають їх запам'ятовувати. Такі особливості полегшують спроби їх розпізнавання.

Методи передачі паролів та способи їх зберігання повинні відповідати вимогам високого рівня безпеки. Це означає, що передача паролів повинна реалізовуватися через спеціально захищені канали, а самі паролі повинні бути щонайменше зашифрованими. Останнім часом все частіше використовується одноразова аутентифікація користувача. Такий підхід дозволяє користувачеві реалізовувати доступ до великої кількості розподілених засобів за одноразовою аутентифікацією, яку реалізує третя сторона, що користується довірою користувача та засобів, до яких реалізується доступ. В цьому випадку центр аутентифікації або сертифікації розв'язує такі задачі:

— зберігає паролі;
— здійснює управління паролями користувачів.

Користувач, який хоче отримати доступ до засобу, пересилає центру сертифікації свій ідентифікатор та пароль. Центр сертифікації підтверджує повноваження даного користувача надаючи йому білет доступу, який зашифрований за допомогою криптографічних алгоритмів, що використовують індивідуальні ключі захищених засобів. Такого типу розв'язки реалізуються в системах типу Kerberos і Passport [3, 4].

Система Passport використовує однойменний протокол Passport, який дозволяє користувачеві доступ до великої кількості різних сторінок WWW за одноразовою аутентифікацією на серверах аутентифікації, які спеціально сформовані для групи сторінок WWW. Білет, який підтверджує право

доступу, знаходиться на диску користувача у формі так званого «тістечка».Він пересилається до сервера разом із запитом HTTP.

У багатьох випадках систем захисту використовуються різні форми паролів. Проблема коректного використання паролів є однією з найважливіших проблем безпеки. Контроль за використанням певних принципів правильного використання паролів можна реалізувати на основі використання спеціальних засобів контролю складності і обміну паролями. Складність паролів можна гарантувати використовуючи програми, що використовують вбудовані словники виразів, назв користувачів, популярних виразів. За допомогою певних правил, наприклад, запису виразів з кінця, такі програми генерують недозволені паролі. Вказані програми можуть функціонувати в активному чи пасивному режимах. Активний контроль паролів може полягати у періодичній ініціації програми пошуку «слабких паролів», які легко можна відгадати. Пасивна перевірка паролів реалізується у момент вибору нового пароля користувачем. Вибрані паролі, які можна легко відгадати чи підробити відповідна програма викреслює. Багаторазове використання одного і того ж паролю не дозволяє створити реєстр історії використаних паролів.

У деяких випадках та системах виробники інсталюють умовні паролі, які часто є ідентичними для всієї партії продуктів. Тому користувач повинен обов'язково змінити такі паролі.

Користувач може довести свою ідентичність на основі використання фізичних ідентифікаторів, серед яких найбільш популярними є ідентифікаційні картки. У цьому випадку процес ідентифікації полягає у зчитуванні інформації, що знаходиться на ідентифікаторі. В більш розвинутих системах аутентифікації в картку вбудовується мікропроцесор, який здійснює додаткове перетворення інформації. Зчитування інформації з карти реалізується контактним чи безконтактним зчитувачем. Контактні зчитувачі використовують для контакту і передачі електричні контакти, зчитування з магнітних носіїв чи оптичні зчитувачі інформації. У безконтактних зчитувачах передача даних реалізується за рахунок використання індукційних зв'язків, інфрачервоного випромінювання, радіовипромінювання тощо.

Головною небезпекою для систем, в яких ідентифікація реалізується на основі використання фізичних ідентифікаторів є можливість викрадення, підробки чи загублення відповідного ідентифікатора. Рівень захисту в цих випадках можна підвищити за рахунок інтеграції систем ідентифікації фізичної з системою паролів. Цього типу підходи використовуються в системах аутентифікації з жетонами. Жетон є ідентифікатором, що генерує одноразовий пароль. Використання жетонів полягає у наступному. Користувач, для ініціалізації процесу аутентифікації вводить персональний ідентифікаційний номер (PIN), після чого, у відповідь на введену послідовність цифр, отриману від системи відносно якої користувач хоче отримати повноваження, на ідентифікаторі жетону висвітлюється пароль

аутентифікації користувача. Функція жетону може реалізовуватися програмно на комп'ютері користувача.

Біометричні методи досить широко використовуються, як унікальні властивості, або параметри людини. До таких характеристик відносяться [4]:

— капілярні лінії;
— форма обличчя та долоні;
— рисунок райдужної сітківки ока;
— голос;
— ручний підпис;
— почерк використання клавіатури.

Аутентифікація за допомогою біометрії реалізується у декілька етапів. Починається вона з вимірювання параметрів користувача. Вимірювальний датчик передає цифрові дані в систему, представляючи результати вимірювань. Ці сигнали перетворюються у відповідний формат. На наступному етапі отримані дані порівнюються з еталонами, які зберігаються в пам'яті. Результат вимірювань може порівнюватися з усіма еталонами чи з еталоном певного користувача. В другому випадку необхідно додатково ідентифікувати користувача, наприклад, шляхом введення назви, або ідентифікатора. У зв'язку з тим, що досить часто результати біометричних вимірювань можуть бути неточними, результат вимірювання параметрів користувача може запам'ятовуватись для нього як еталонний. У цьому випадку важливою є задача визначення допустимих границь відхилень результатів вимірювання біометричного параметру від еталонного зразка. Якщо цей діапазон буде занадто малий, то у системі аутентифікації буде високий показник помилкових відмов у наданні доступу. Якщо цей діапазон буде завеликий, то появиться небезпека того, що система дозволить неуповноважений доступ до засобів захисту. Еталонні значення біометричних параметрів повинні зберігатися в умовах, що забезпечують високий рівень безпеки, оскільки окрім того, що вони використовуються для аутентифікації користувачів, — це є персональні дані користувачів. Вищенаведені приклади описують різні аспекти організації доступу до систем та ресурсів і мають велике значення для реалізації безпеки доступу.

1. *Соколов А. В.* Защита информации в распределённых корпоративных сетях и системах / *А. В. Соколов, В. Ф. Шаньгин*. — М. : ДМК Пресс, 2002.
2. *Ахо А.* Построение и анализ вичислительных алгоритмов / *А. Ахо, Дж. Хонкрофт, Дж. Ульман*. — М. : Мир, 1979.
3. *Смит Р. Э.* Аутентификация: от паролей до открытых ключей. — М. : Изд. дом «Вильямс», 2002.
4. *Загжда Д. П.* Как построить защищённую информационную систему. Технология создания безопасных систем. — Спб. : НПО «Мир и семья — 95» ООО «Интерлайн», 1998.

Поступила 11.09.2010р.