Лекція 3

Засоби й методи обмеження доступу до файлів та захист від несанкціонованого копіювання

Несанкціонований доступ до інформації (НСД) — доступ до інформації з порушенням посадових повноважень співробітника, доступ до закритої для публічного доступу інформації з боку осіб, що не мають дозволу на доступ до цієї інформації. Також іноді несанкціонованим доступом називають одержання доступу до інформації особою, яка має право на доступ до цієї інформації в обсязі, що перевищує необхідний для виконання службових обов'язків.

Причини несанкціонованого доступу до інформації:

- Наявність помилок конфігурації (прав доступу, брандмауерів, обмежень на масовість запитів до баз даних);
- слабка захищеність засобів авторизації (викрадання паролів, смарт-карт; фізичний доступ до устаткування, що погано охороняється; доступ до незаблокованих робочих місць співробітників під час відсутності співробітників);
- наявність помилок у програмному забезпеченні;
- зловживання службовими повноваженнями (викрадання резервних копій, копіювання інформації на зовнішні носії при праві доступу до інформації);
- прослуховування каналів зв'язку при використанні незахищених з'єднань всередині локальної мережі;
- використання клавіатурних шпигунів, вірусів і троянів на комп'ютерах співробітників.

До основних способів НСД належать:

- безпосереднє звернення до об'єктів з метою одержання певного виду доступу;
- створення програмно-апаратних засобів, що виконують звертання до об'єктів в обхід засобів захисту;
- модифікація засобів захисту, що дозволяє здійснити НСД;
- впровадження в АС програмних або апаратних механізмів, що порушують структуру і функції АС і дають можливість здійснити НСД.

Можна виділити такі узагальнені категорії методів захисту від НСД:

• технологічні;

• правові.

Захист від несанкціонованого доступу до інформації

Для здійснення несанкціонованого доступу до інформації зловмисник не застосовує жодних апаратних або програмних засобів, що не входять до складу КС.

Для захисту інформації від несанкціонованого доступу створюється система розмежування доступу до інформації. Завданням системи розмежування доступу є управління доступом користувачів до внутрішніх інформаційних ресурсів КС.

Система має у своєму складі блоки ідентифікації і автентифікації процесів, активованих певними користувачами; базу даних повноважень користувачів і керуючий блок.

При необхідності виконання певних дій в ІС користувач активує програму. Операційна система запускає процеси виконання програми, яким присвоюється ознака користувача. При зверненні процесів до ресурсів інформаційної системи (програм, файлів, пристроїв) система розмежування доступу визначає, в інтересах якого користувача ініційований процес, що вимагає звернення до ресурсів. Після автентифікації процесу система розмежування доступу вибирає з бази даних відомості про повноваження користувача і порівнює їх з вимогами до повноважень, які визначені для ресурсу. Якщо повноваження користувача не менше потрібних, то відповідному процесу дозволяється виконати запитані дії по відношенню до ресурсу. Інакше йде відмова у виконанні операції і факт спроби порушення встановлених правил запам'ятовується в спеціальному журналі.

Для посилення стійкості ІС до спроб несанкціонованого доступу до інформації використовується шифрування інформації на зовнішніх носіях, а також видаляються тимчасові файли після завершення інформаційних процесів.

Захист від електромагнітних випромінювань і наведень

Всі методи захисту від електромагнітних випромінювань і наведень можна розділити на пасивні і активні.

Пасивні методи забезпечують зменшення амплітуди випромінюваного сигналу до безпечного рівня. Основним методом пасивного захисту від

випромінювань служить екранування апаратних засобів. Екран вибирається відповідно до характеристиками випромінювання. Це може бути струмопровідний матеріал у вигляді суцільного екрана, наприклад з листової сталі товщиною до 2 мм або тонкої фольги, а також у вигляді сітки з певною величиною осередки.

Активні методи засновані на використанні генераторів шумів, які видають в навколишній простір сигнали з амплітудою і частотою, відповідними побічним випромінюваним сигналам. У результаті накладення сигналів побічні випромінювання неможливо виділити і використовувати.

Наведення усуваються за рахунок екранування електричних кабелів і використання оптичних кабелів, які не роблять електричного впливу на провідники струму, що знаходяться поблизу.

Механізми захисту від несанкціонованих змін технічної структури в процесі експлуатації інформаційної системи

На етапі експлуатації ІС зловмисники можуть призвести наступні несанкціоновані дії по зміні технічної (апаратної) структури: підключення нештатних блоків, пристроїв або комп'ютерів; зміна зв'язків ІС; заміна штатних блоків, пристроїв або комп'ютерів на відповідні структурні компоненти зі зміненими характеристиками; зміна режимів роботи пристроїв.

Несанкціонований доступ до апаратних і програмних засобів може бути виключений або суттєво ускладнений при виконанні наступного комплексу заходів:

• охорона приміщень, в яких знаходяться апаратні засоби КС;

• протидія несанкціонованому входу в систему;

• протидія несанкціонованому підключенню обладнання;

• захист внутрішнього монтажу, засобів управління і комутації від несанкціонованого втручання.

Організація охорони приміщень

У загальному випадку контрольований вхід в систему передбачає виконання таких дій:

• включення апаратних засобів захисту;

• завантаження програмних засобів системи захисту інформації;

• ідентифікацію та автентифікацію суб'єкта доступу;

• завантаження операційної системи;

• реєстрацію суб'єкта доступу;

• розблокування КС.

Для протидії несанкціонованому включенню апаратних засобів КС можуть застосовуватися такі методи:

• використання замків в блоках живлення;

• дистанційне керування подачею живлення;

• блокування органів управління подачею живлення.

У захищених системах до завантаження штатної ОС може здійснюватися завантаження програмного блоку, який контролює процес ідентифікації і автентифікації, а також процес завантаження ОС. За рахунок відносної простоти і захищеності від несанкціонованого зміни блок дозволяє здійснити ідентифікацію, автентифікацію і довірене завантаження ОС. Ідентифікація та автентифікація суб'єктів доступу можуть проводитися і засобами ОС після завершення її завантаження.

Комплекс заходів та засобів управління доступом до пристроїв повинен виконувати і функцію автоматичної реєстрації дій суб'єкта доступу. Журнал реєстрації подій може вестися як на автономної ЕОМ, так і в мережі. Періодично або при фіксації порушень протоколів доступу адміністратор переглядає журнал реєстрації з метою контролю дій суб'єктів доступу.

Завершується контрольований вхід в систему розблокуванням доступу і активуванням системи розмежування доступу для забезпечення авторизованого доступу до ресурсів системи.

Для запобігання загрози неконтрольованого підключення пристроїв використовуються наступні методи:

• перевірка особливостей пристроїв;

• використання ідентифікаторів пристроїв.

Контроль підключення пристроїв може здійснюватися за рахунок порівняння інформації про влаштування, що підключається та відомостей про пристрої КС (типи пристроїв (блоків) та їх характеристики, кількість і особливості підключення зовнішніх пристроїв, режими роботи і інша інформація).

Ще більш надійним і оперативним методом контролю є використання спеціального коду-ідентифікатора пристрою. Цей код може генеруватися апаратними засобами, а може зберігатися в спеціальному запам'ятовуючому пристрої. Генератор може ініціювати видачу в контролюючий пристрій (в обчислювальній мережі це може бути робоче місце адміністратора) унікального номера пристрою.

Для захисту від несанкціонованих дій щодо зміни монтажу, заміні елементів, переключенню комутуючих пристроїв необхідна наявність таких засобів:

• блокування доступу до внутрішнього монтажу, до органів управління і комутації пристроями. що мають замок двері, кришки, захисні екрани і т.п .;

• автоматизованого контролю доступу до апаратури.

Поняття ідентифікації та автентифікації

Ідентифікацію й автентифікацію можна вважати основою програмно-технічних засобів безпеки, оскільки інші сервіси розраховані на обслуговування іменованих суб'єктів. Ідентифікація й автентифікація – це перша лінія оборони, "прохідна" інформаційного простору організації.

Ідентифікація дозволяє суб'єктові (користувачеві, процесу, що діє від імені певного користувача, або іншому апаратно-програмному компоненту) назвати себе (повідомити своє ім'я, тобто дати можливість себе розпізнати). За допомогою автентифікації друга сторона переконується, що суб'єкт дійсно той, за кого він себе видає. Як синонім слова "автентифікація" іноді використовують словосполучення "перевірка дійсності".

У відкритому мережевому середовищі між сторонами ідентифікації/автентифікації не існує довіреного маршруту; це значить, що в загальному випадку дані, передані суб'єктом, можуть не збігатися з даними, отриманими й використаними для перевірки дійсності. Необхідно забезпечити захист від пасивного й активного прослуховування мережі, тобто від перехоплення, зміни й/або відтворення даних. Передача паролів у відкритому вигляді, мабуть, незадовільна; не рятує положення й шифрування паролів, тому що воно не захищає від відтворення. Потрібні більш складні протоколи автентифікації.

Надійна ідентифікація й автентифікація ускладнена не тільки через мережеві загрози, але й з цілого ряду причин. По-перше, майже всі автентифікаційні сутності можна довідатися, украсти або підробити. По-друге, є протиріччя між надійністю автентифікації, з одного боку, і зручностями користувача й системного адміністратора з іншогої. Так, з міркувань безпеки необхідно з певною частотою просити користувача повторно вводити автентифікаційну інформацію (адже на його місце могла сісти інша людина), а це не тільки клопітно, але й підвищує ймовірність того,

що хтось може підглянути за уведенням даних. По-третє, чим надійніший засіб захисту, тим він дорожчий.

Сучасні засоби ідентифікації/автентифікації повинні підтримувати концепцію єдиного входу в мережу. Єдиний вхід у мережу - це, у першу чергу, вимога зручності для користувачів. Якщо в корпоративній мережі багато інформаційних сервісів, що допускають незалежний обіг, то багаторазова ідентифікація/автентифікація стає занадто обтяжною. На жаль, поки не можна сказати, що єдиний вхід у мережу став нормою, що домінантні рішення поки не сформувалися.

Таким чином, необхідно шукати компроміс між надійністю, доступністю за ціною й зручністю використання й адміністрування засобів ідентифікації й автентифікації.

Цікаво відзначити, що сервіс ідентифікації/автентифікації може стати об'єктом атак на доступність. Якщо система зконфігурована так, що після певного числа невдалих спроб пристрій уведення ідентифікаційної інформації (таке, наприклад, як термінал) блокується, то зловмисник може припинити роботу легального користувача буквально декількома натисканнями клавіш.

Методи автентифікації

В інформаційних технологіях використовуються такі методи автентифікації:

- *однобічна автентифікація*, коли клієнт системи для доступу до інформації доводить свою автентичність;
- *двобічна автентифікація*, коли, крім клієнта, свою автентичність повинна підтверджувати і система (наприклад, банк);
- *трибічна автентифікація*, коли використовується так звана нотаріальна служба автентифікації для підтвердження достовірності кожного з партнерів в обміні інформацією.

Методи автентифікації також умовно можна поділити на ***однофакторні*** та ***двофакторні.***

Однофакторні методи діляться на:

- *логічні* (паролі, ключові фрази, які вводяться з клавіатури комп'ютера чи клавіатури спеціалізованого пристрою);
- *ідентифікаційні* (носієм ключової інформації є фізичні об'єкти: дискета, магнітна карта, смарт-карта, штрих-кодова

карта тощо. Недоліки: для зчитування інформації з фізичного об’єкта (носія) необхідний спеціальний рідер; носій можна загубити, випадково пошкодити, його можуть викрасти або зробити копію).

- *біометричні* (в їх основі – аналіз унікальних характеристик людини, наприклад: відбитки пальців, малюнок райдужної оболонки ока, голос, обличчя. Недоліки: біометричні методи дорогі і складні в обслуговуванні; чутливі до зміни параметрів носія інформації; володіють низькою достовірністю; призначені тільки для автентифікації людей, а не програм або інших ресурсів).

*Автентифікація за відбитками пальців***.** Переваги засобів доступу по відбитку пальця - простота використання, зручність і надійність. Весь процес ідентифікації здійснюється досить швидко і не вимагає особливих зусиль від користувачів. Вірогідність помилки при ідентифікації користувача набагато менша порівняно з іншими біометричними методами.

Використання геометрії долоні. Переваги ідентифікації по геометрії долоні в питаннях надійності дорівнює автентифікації по відбитку пальця, хоча пристрій для прочитування відбитків долонь займає більше місця. Найбільш досконалий пристрій, Handkey, сканує як внутрішню, так і бічну сторону руки.

Автентифікація за райдужною оболонкою ока. Перевага сканування райдужної оболонки полягає в тому, що зразок плям на оболонці знаходиться на поверхні ока, і від користувача не вимагається спеціальних зусиль. Фактично відеозображення ока може бути відсканована на відстані метра, що робить можливим використання таких сканерів в банкоматах та в системах доступу. Ідентифікуючі параметри можуть скануватися і кодуватися, зокрема, і у людей з ослабленим зором, але непошкодженою райдужною оболонкою.

Автентифікація за сітківкою ока. Сканування сітківки відбувається з використанням інфрачервоного світла низької інтенсивності, направленого через зіницю до кровоносних судин на задній стінці ока. Сканери для сітківки ока набули великого

поширення в надсекретних системах контролю доступу, оскільки ці засоби автентифікації характеризуються одним з найнижчих відсотків відмови в доступі зареєстрованим користувачам і майже нульовим відсотком помилкового доступу.

Автентифікація за рисами особи (за геометрією особи) - один з напрямів, що швидко розвиваються, в біометричній індустрії. Розвиток цього напряму пов'язаний з швидким зростанням мультимедійних відео-технологій. Проте більшість розробників поки зазнають труднощі в досягненні високого рівня виконання таких пристроїв. Проте можна чекати появу в найближчому майбутньому спеціальних пристроїв ідентифікації особи за рисами обличчя в залах аеропортів для захисту від терористів і т. ін.

Двофакторні методи **автентифікації** отримують в результаті комбінації двох різних однофакторних методів, частіше всього ідентифікаційного та логічного. Наприклад: «пароль + дискета», «магнітна карта + PIN».

Кожен клас методів має свої переваги і недоліки. Майже всі методи автентифікації страждають на один недолік - вони, насправді, автентифікують не конкретного суб'єкта, а лише фіксують той факт, що автентифікатор суб'єкта відповідає його ідентифікатору. Тобто всі відомі методи не захищені від компрометації автентифікатора.

Апаратна ідентифікація

Цей принцип ідентифікації ґрунтується на визначенні особистості користувача за певним предметом, ключем, що перебуває в його ексклюзивному користуванні. Мова йде про спеціальні електронні ключі. На даний момент найбільше поширення одержали два типи пристроїв. До першого ставляться всілякі ***карти.*** Їх досить багато, і працюють вони за різними принципами. Так, наприклад, досить зручні у використанні безконтактні карти (їх ще називають проксіміті-карти), які дозволяють користувачам проходити ідентифікацію як у комп'ютерних системах, так й у системах доступу в приміщення. Найбільш надійними вважаються смарт-карти - аналоги звичних багатьом людям банківських карт. Крім того, є й більш дешеві, але менш стійкі до злому карти: магнітні, зі штрих-

кодом і т.д.

Іншим типом ключів, які можуть використатися для апаратної ідентифікації, є так звані ***токени.*** Ці пристрої мають власну захищену пам'ять і підключаються безпосередньо до одного з портів комп'ютера (USB, LPT).

Головною *перевагою* застосування апаратної ідентифікації є досить висока надійність. У пам'яті токенів можуть зберігатися ключі, підібрати які хакерам не вдасться. Крім того, у них реалізовано чимало різних захисних механізмів. А вбудований мікропроцесор дозволяє електронному ключу не тільки брати участь у процесі ідентифікації користувача, але й виконувати деякі інші корисні функції.

Недоліком апаратної ідентифікації є висока 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 майнової ідентифікації однаково будуть потрібні деякі вкладення. Все-таки кожного зареєстрованого користувача потрібно забезпечити персональними токенами. Крім того, згодом деякі типи ключів можуть зношуватися або можуть бути загублені користувачами.

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 в переважній більшості випадків використовується тільки одна пара: парольний захист і токен. У цьому випадку користувач може не боятися підбору 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 використовуються паролі, токени й біометричні характеристики людини.

Біометрична ідентифікація

Біометрія – це ідентифікація людини за унікальними, властивими тільки їй біологічними ознаками. 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. Так що користувачам, що вирішили використати біометричну ідентифікацію, є із чого вибрати.

Головною *перевагою* біометричних технологій є найвища надійність. І дійсно, усі знають, що двох людей з однаковими відбитками пальців у природі просто не існує. Правда, сьогодні вже відомо кілька способів обману дактилоскопічних сканерів. Наприклад, потрібні відбитки пальців можуть бути перенесені на плівку або до пристрою може бути прикладена велика фотографія пальця зареєстрованого користувача. Втім, треба зізнатися, що сучасні пристрої вже не попадаються на такі прості виверти. Так що зловмисникам доводиться видумувати все нові й нові способи обману біометричних сканерів.

Основним *недоліком* біометричної ідентифікації є вартість устаткування. Адже для кожного комп'ютера, що входять до цієї системи, необхідно придбати власний сканер. Варто також 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, який пристрій придбати – дорожчий й кращий або дешевший й гірший.

Парольна ідентифікація

Ще не дуже давно ***парольна ідентифікація*** була чи ледве не єдиним способом визначення особистості користувача. Справа в тому, що парольна ідентифікація найбільш проста як у реалізації, так й у використанні. Суть її зводиться до наступного. Кожен зареєстрований користувач системи одержує набір персональних реквізитів (звичайно використаються пари: логін-пароль). Далі при кожній спробі входу людина повинна вказати свою інформацію. Оскільки вона унікальна для кожного користувача, то на підставі її система й робить висновок про особистість та ідентифікує.

Недоліком парольної ідентифікації є значна залежність

надійності ідентифікації від користувачів, точніше від обраних ними паролів. Справа в тому, що більшість людей використовують ненадійні ключові слова, які легко підбираються. Фахівці в області інформаційної безпеки радять використати довгі паролі, що складаються з безладного сполучення букв, цифр і різних символів.