Захист даних комп'ютерних мереж корпоративних підприємств

Олександр Ананьєв, Олександр Белей

Кафедра інформаційних систем у менеджменті, Львівська комерційна академія, УКРАЇНА, м.Львів, вул. Туган-Барановського 10, E-mail: oles@lac.lviv.ua

Abstract **– *Directions of defence of komp'yuternikh networks of corporation which going to carry out the activity in the network of Internet are examined in this research. Technologies of enciphering and code as base technologies of protection of data are examined in the modern automated informative systems. The special attention is spared technology of Java, which is basic in development of Internet-networks and electronic shops..***

Ключові слова – protection of data, komp'yuterni networks, the informative system is automated, transmission information, enciphering of information, confidentiality, access, cryptographic defence, key of enciphering, is unauthorized.

I. Вступ

Стрімкий розвиток засобів обчислювальної техніки та відкритих мереж передачі даних сприяв їх ширшому використанню в повсякденному житті. Значні обчислювальні можливості і оперативність передачі інформації в комп'ютерних мережах вплинули не тільки на зміну принципів ведення традиційного бізнесу, але й спричинили виникнення та розвиток нових напрямів бізнесової діяльності.

В галузі використання засобів обчислювальної техніки і передачі даних, яка інтенсивно розвивається і розширюється, регулярно з'являються нові проблеми щодо зберігання конфіденційності та цілісності інформації, захисту її від посягань злочинців, що озброєні найсучаснішими методами для проникнення в мережу обміну даними.

Конкурентні переваги корпоративних підприємств багато в чому залежать від конфіденційності його облікової інформації. Перехід до комп'ютерної обробки даних створив досить специфічні проблеми, одною з яких є захист інформації від несанкціонованого доступу. В умовах розповсюдження глобальних комп'ютерних мереж проблема захисту інформації стала досить важливою, оскільки тепер "дистанційна крадіжка" секретної інформації стала досить поширеним явищем.

II. Постановка проблеми, мета статті

У зв'язку з переходом до комп'ютерної обробки даних з'явилася необхідність у забезпеченні інформаційної безпеки діяльності корпоративних підприємств у сучасному технократичному та інфокомунікаційному суспільстві. Інформаційна безпека – це стан захищеності обробки, збереження і передачі даних в інформаційно-технологічних системах від незаконного доступу до них, а також стану захищеності інформаційних ресурсів від дій, направлених на порушення їх роботи.

III. Виклад основного матеріалу

Засоби захисту інформації можна поділити на внутрішні і зовнішні. Зовнішні побудовані на технологіях, які вбудовані безпосередньо в прикладні програмні системи. До них відносяться ключі захисту програм і спеціалізоване програмне забезпечення, що дозволяє "приховувати" файли і цілі логічні диски. Внутрішні засоби – це технології захисту інформації, інтегровані в саму програмну систему. Сюди відносяться засоби обмеження доступу користувачів до даних і можливість їх обробки, різні механізми шифрування в базах даних. Взагалі, засоби забезпечення захисту комп'ютерних систем можна поділити на: правові, морально-етичні, технічні, адміністративні, фізичні. Згідно проведених досліджень, найбільша питома вага захисту інформації припадають на правові засоби – 60%, на криптографічні – 20%, програмні – 14%, апаратні та фізичні - 2%, 2% - на організаційні.

Сьогодні сформувались два основних способи реалізації механізмів захисту. Перший спосіб захисту реалізує лише частину механізмів захисту в програмному і апаратному забезпеченні комп'ютерних систем, яка необхідна для забезпечення роботи всієї комп'ютерної системи. Захист інформації при зберіганні, обробці або передачі забезпечується додатковими програмними чи апаратними засобами, що не входять до складу самої комп'ютерної системи. При цьому засоби захисту підтримуються внутрішніми засобами комп'ютерної системи. Такий спосіб дістав назву додаткового (add-on) захисту, оскільки засоби захисту є доповненням до основних програмних і апаратних засобів комп'ютерної системи. Другий спосіб носить назву вмонтованого (built-in), при якому механізм захисту є невід'ємною частиною комп'ютерної системи, що розроблена і реалізована з врахуванням певних вимог безпеки. Механізми захисту можуть бути реалізовані у вигляді окремих компонент комп'ютерної системи, тобто в деякій компоненті комп'ютерної системи є частина, яка відповідає за її захист. При цьому засоби захисту формують єдиний механізм, що відповідає за забезпечення безпеки всієї комп'ютерної системи.

Є два основні напрями захисту, але справжній захист даних в комп'ютерних мережах не можливий без шифрування і криптографування. Тому особливо актуальною на сьогодні постає проблема використання криптографічних методів в інформаційних системах. Це пов'язано, в першу чергу, із розширенням використання комп'ютерних мереж, через які передаються великі обсяги державної, військової, комерційної і приватної інформації.

В новому тисячолітті, яке вже без сумніву всі називають ерою інформаційного суспільства, передача, обробка та зберігання даних є неможлива без забезпечення їх комплексного захисту від нового типу злочинців – інформаційних.

Локальну мережу, що захищається, ми пропонуємо поділити на сегменти за принципом вимог до інформаційної безпеки того чи іншого сегменту. Можна припустити, що в цій мережі буде відкритий сегмент, в якому може знаходитися рекламна, довідкова чи інша загальнодоступна інформація. Додатково в ній можуть бути організовані сегменти з різним ступенем захищеності або відкриті для доступу різних груп користувачів.

В мережі шляхом встановлення правил фільтрації пакетів ми пропонуємо виробляти параметри системи безпеки для доступу до сегментів мережі ззовні і для обмінів між різними сегментами.

Далі, на нашу думку, може бути встановлено криптозахист вихідного трафіку у зовнішній мережі. Криптозахист трафіку, що виходить у зовнішню мережу, забезпечується на основі протоколу SKIP. Однак використання цього протоколу в Screen-системах надає ряд додаткових можливостей.

Розглянемо з'єднання двох локальних мереж, що з'єднані за допомогою канального провайдера і захищені Screen-пристроями. У цьому випадку Screen-пристрою можуть інкапсулювати весь трафік між цими мережами в SKIP, яке називається SKIP-тунелювання. При цьому вихідні IP-пакети можуть міститися в блоках даних SKIP-пакетів, а всі мережеві адреси всіх вузлів внутрішніх мереж можуть бути замінені на деякі віртуальні адреси, що відповідають Screen-пристроям у зовнішній мережі (адресна векторізація). В результаті весь трафік між цими локальними мережами може виглядати ззовні тільки як цілком шифрований трафік між двома вузлами. В цьому випадку зовнішньому користувачу може бути доступна така інформація, як тимчасова динаміка й оцінка інтенсивності трафіку, яка може маскуватися шляхом використання архіву даних і видачі "порожнього" трафіку. Програмна реалізація SKIP допускає паралельну роботу в режимі шифрування та в режимі відкритого трафіку, проте залишаэться выдкритим питання про безпеку системи, що працює в такому змішаному режимі. З повною відповідальністю можна гарантувати безпеку систем, які вимагають як відкритого, так і конфіденційного обміну тільки при використанні Screen-пристроїв. На основі даних технологій компанією ЕЛВІС+ було розроблено комплекс рішень, що включають в себе продукти призначені для використання в різних місцях корпоративної мережі, яка використовує як транспортне середовище глобальні мережі. Пристрій SKIP-Bridge, що може розміщатися між відкритим і SKIP-захищеним сегментом локальної мережі і використовуватися для кодування чи декодування трафіку. Він орієнтований на великі підприємства і використовується замість SunScreen, вартість якого є дуже висока. SKIP-Bridge базується на відносно недорогій платформі Sparc або Intel і допускає використання адаптера для високошвидкісної виділеної лінії замість одного з адаптерів Ethernet. Це дозволяє підключати SKIP-Bridge безпосередньо до комунікаційного провайдера і заощаджувати на роутері, який необхідний в конфігурації з SunScreen. Як одна з модифікацій даного рішення пристрій SKIP-Server призначений для використання безпосередньо в локальній мережі підприємства. Інша модифікація - пристрій SKIP-Proxy – призначена для спільного використання разом зі стандартними FireWall-рішеннями. Вже сьогодні є досить очевидним, що мова йде про виникнення нового напрямку, який за масштабами виходить далеко за межі окремого протоколу технічної ідеї, покладе край розробці розрізнених технічних рішень в області безпеки та дає початок єдиній технології побудови захищених комунікацій.

Як нову філософію інформаційної безпеки можна розглядати Java, яка на сьогодні є не тільки новою мовою для програмування, але й принципово новим підходом до організації мережних обрахунків на підприємстві. Це призвело до побудови мереж Internet і Intranet. Технологія і мова Java настільки змінили мислення фахівців в області інформаційних технологій, що в 1995 році більшість кваліфікованих програмістів все більше і більше звертати увагу на вирішення поточних задач, які пов’язані з адаптуванням додатків з однієї платформи на іншу. При цьому, нововедення в будь-який програмний додаток вимагають титанічних зусиль по приведенню всіх версій для будь-яких платформ і операційних систем до єдиної основи. Крім того, назріли і ряд об'єктивних проблем:

- глобальність – організація доставки визначеного програмного забезпечення одночасно мільйону клієнтів в заданий час;
- керування – остання версія виконується на хостах локальної мережі;
- безпека – ідентифікація прикладного програмного забезпечення.

Поява Java дозволило відповісти на цілий ряд проблем розробників нових інформаційних, що виникають як в розробників, так і в користувачів цих технологій. Поява Java стало цілком усвідомленим і природним явищем після появи цілого ряду технологій: клієнт-серверу, клієнт-брокер-сервер, Web, Java, Network Applets. Java включає в себе:

- універсальний мережевий інструмент для створення мережевих застосувань;
- мережеві додатки, що виконуються на будь-якій платформі без модифікацій;
- додатки складаються з applets, які завантажуються з будь-якої точки мережі;
- можливість створення мільйонів персоналізованих applets і застосувань.

Процес створення і використання програмного забезпечення, яке базується на технології Java, стає не національним, а інтернаціональним завданням в рамках світових обчислювальних мереж. Спроба "введення" обмежень на ці технології безсумнівно може призвести до ізоляції українських інформаційних технологій від світових і до непередбаченого відставання. Технологія Java орієнтована на розподілене створення і використання програмного забезпечення, тому суттєва роль відводиться питанню авторизації. Причому питання зводиться не стільки до захисту авторських прав, скільки до захисті від підробок програмного забезпечення. Одним зі спо-

собів підтвердження авторства є внесення підпису в байтний код. При цьому, такий підпис буде мати подвійне призначення: підтверджувати цілісність і незмінність коду, однозначно визначати автора.

Захист даних в комп'ютерних мережах від несанкціонованого доступу здійснюють шляхом попередньої чи періодичньої аутентифікації користувача програмного забезпечення (ПЗ). При цьому захист можна здійснювати кількома способами: 1) системи парольного захисту ПЗ, 2) системи "прив'язки" ПЗ до комп'ютера користувача, 3) системи з "ключовими дисками", 4) апаратно-програмні системи з електронними ключами.

Розглянемо далі більш детально основні принципи функціонування шифрувальної файлової системи (Encrypting file system - EFS) в роботі операційної системи мережевого типу, якою є ОС Windows'2000, Windows'2003 та Windows'XP.

Шифрувальна файлова система (EFS) поміщена в ядрі Windows'XP та тісно інтегрована з NTFS службою. Її основним призначенням є захист даних, що зберігаються на диску, від несанкціонованого доступу шляхом їх шифрування. Існуючі файлові системи типу Windows не забезпечують необхідного захисту даних від несанкціонованого доступу.

Система EFS була розроблена з ціллю подолання недоліків, що притаманні операційній системі (ОС) сімейства Windows. Далі ми розглядаємо більш детально технології шифрування, взаємодії EFS з користувачем і способи відновлення даних та приклад шифрування каталогу за допомогою EFS.

В основі EFS використовується архітектура Windows CryptoAPI та технологія шифрування з відкритим ключем. Для шифрування кожного файлу випадковим чином генерується ключ шифрування на основі будь-якого симетричного алгоритму шифрування. На сьогодні в EFS найчастіше використовується один алгоритм (DESX), що є спеціальною модифікацією стандарту DES. Ключі шифрування EFS зберігаються в резидентному пулі пам'яті (сама EFS розташована в ядрі Windows'XP), що виключає несанкціонований доступ до них через файл підкачки.

За замовчуванням EFS конфігурована таким чином, що користувач може відразу почати використовувати шифрування файлів. Операція шифрування і дешифрування підтримуються для файлів і каталогів. У випадку шифрування каталогу, автоматично шифруються всі файли і підкаталоги цього каталогу. Необхідно відзначити, що при переміщенні зашифрованого файлу або перейменуванні із зашифрованого каталогу в незашифрований, каталог все одно залишається зашифрованим.

EFS здійснює шифрування даних, використовуючи схему із загальним ключем. Дані шифруються швидким симетричним алгоритмом за допомогою ключа шифрування файла FEK (file encryption key). FEK шифрується одним або декількома загальними ключами шифрування, внаслідок чого можна отримати список зашифрованих ключів FEK. Список зашифрованих ключів FEK зберігається в спеціальному атрибуті EFS, який називається DDF (data decryption field - поле дешифрування даних). Інформація, за допомогою якої виробляється шифрування даних, тісно пов'язана з цим файлом.

Список зашифрованих ключів FEK зберігається разом з файлом в спеціальній області EFS, яка називається DRF (data recovery field - поле відновлення даних) (рис.1.).

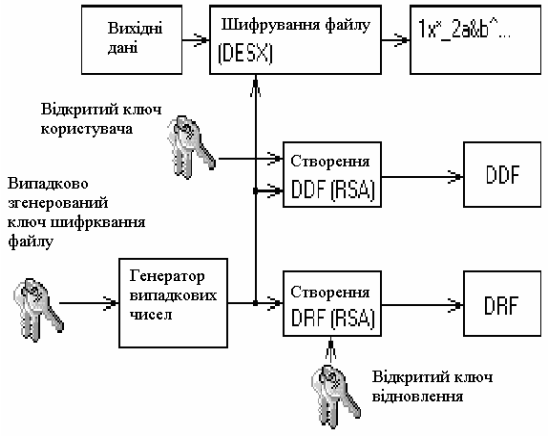

Рис. 1. Процес шифрування даних з допомогою EFS в середовищі Windows`XP

Для шифрування списку FEK в DRF використовується тільки загальна частина кожної пари ключів. Для нормального здійснення файлових операцій необхідно тільки загальні ключі відновлення. Агенти відновлення можуть берегти свої особисті ключі в безпечному місці поза системою (наприклад, на смарт-картах).

Незашифрований файл користувача шифрується за допомогою випадково згенерованого ключа FEK. Цей ключ записується разом з файлом, файл дешифрується за допомогою загального ключа користувача (записаного в DDF), а також за допомогою загального ключа агента відновлення (записаного в DRF).

В процесі дешифрування використовується особистий ключ користувача для дешифрування FEK (версія FEK, яка зберігається в DDF). Розшифрований FEK використовується для поблочного дешифрування файла. Якщо у великому файлі блоки прочитуються не послідовно, то дешифруються тільки блоки, що читаються. Файл при цьому залишається зашифрованим рис. 2.

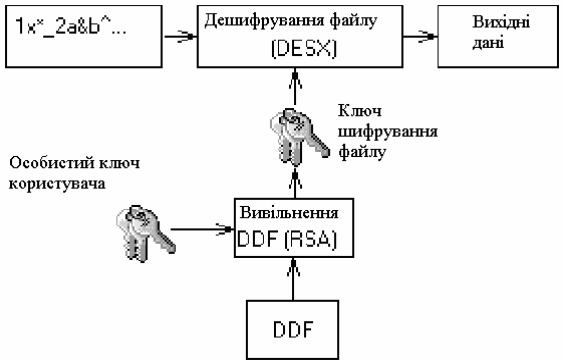

Рис. 2. Процес дешифрування даних з допомогою EFS в середовищі Windows'XP

Процес відновлення аналогічний дешифруванню з тією відмінністю, що для дешифрування FEK використовується особистий ключ агента відновлення, а зашифрована версія FEK береться з DRF (рис. 3).

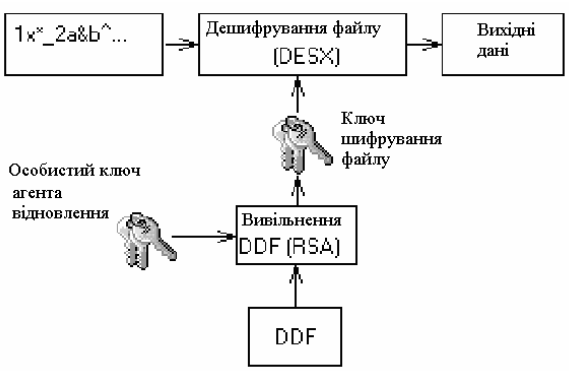

Рис. 3. Процес відновлення даних з допомогою EFS в середовищі Windows'XP

EFS (рис. 4) в ОС Windows'XP складається з наступних компонентів:

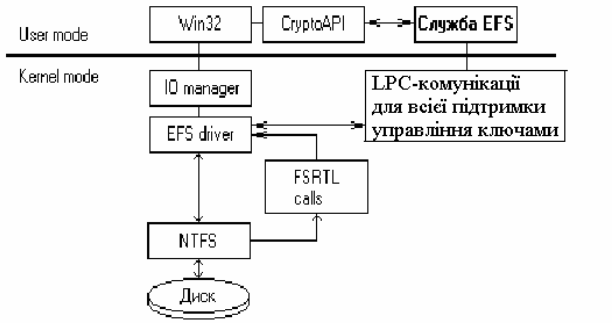

Рис. 4. Архітектура EFS в ОС Windows'XP

1) драйвер EFS розташований логічно на вершині NTFS. Він взаємодіє з сервісом EFS, одержує ключі шифрування файлів, поля DDF, DRF та інші дані управління ключами;

2) бібліотека часу виконання EFS (FSRTL) - це модуль усередині драйвера EFS, який здійснює зовнішні виклики NTFS для виконання різних операцій файлової системи, таких як читання, запис, відкриття зашифрованих файлів і каталогів, а також операцій шифрування, дешифрування, відновлення даних при записі на диск і читанні з диска;

3) служба EFS використовує існуючий порт зв'язку LPC між LSA (Local security authority, локальні засоби захисту) і працює з kernel-mode монітором безпеки для зв'язку з драйвером EFS;

4) Win32 API забезпечує інтерфейс програмування для шифрування відкритих файлів, дешифрування і відновлення закритих файлів, прийому і передачі закритих файлів без їх попередньої розшифровки. Він реалізований у вигляді стандартної системної бібліотеки advapi32.dll.

Таким чином, система EFS в Windows'XP надає користувачам можливість зашифровувати каталоги NTFS, використовуючи стійку, засновану на загальних ключах криптографічну схему, при цьому всі файли в закритих каталогах будуть зашифровані. Шифрування окремих файлів підтримується, але не рекомендується через непередбачувану поведінку застосувань. Вона підтримує шифрування файлів на інших комп'ютерах, доступ до яких здійснюється як до спільно використовуваних ресурсів. Система EFS надає встановити політику відновлення даних таким чином, що зашифровані дані можуть бути відновлені за допомогою EFS.

Висновок

Існують технології безпеки і вони готові для використання Internet з метою ведення сучасного бізнесу. Ми говоримо про технологію "клієнт-сервер", як про вершину досягнень в області змін інформаційної системи світових корпорацій. На їх базі вже тестується більше 1500 Java-застосувань тільки в області фінансів. В нашій державі мережа X.25 є стандартом для побудови корпоративних обчислювальних мереж тоді, як у світі настала нова ера Internet-бізнесу - "digital money". Вони впроваджують нові стандарти і на практиці досліджують такі нові задачі, як: "private money" і " digital money and world currency". У всьому світі основним двигуном створення нових технологій є розвиток бізнесу. Тому всі питання зводяться до готовності національного бізнесу та нормативної бази, бо технології вже існують і готові.

В наступних дослідженнях особливу увагу буде приділено економічній безпеці корпоративного підприємства.